

# IT i praksis 2026



# Innholdsfortegnelse

|           |                                              |        |
|-----------|----------------------------------------------|--------|
| <b>01</b> | Forord, årets funn og om <i>IT i praksis</i> | ... 3  |
| <b>02</b> | Temarapport 1<br>Kunstig intelligens         | ... 5  |
|           | Utbredelse og modenhet                       | ... 9  |
|           | Gevinster                                    | ... 12 |
|           | Barrierer                                    | ... 15 |
|           | Innbyggernes tillit                          | ... 17 |
|           | Veiledning og veien videre                   | ... 20 |
| <b>03</b> | Temarapport 2<br>Sikkerhet og beredskap      | ... 26 |
|           | Sikkerhetsarbeidet                           | ... 30 |
|           | Kompetanse og beredskap                      | ... 33 |
|           | Styring og støtte                            | ... 36 |
|           | Innbyggernes tillit                          | ... 39 |
|           | Veien videre                                 | ... 42 |
| <b>04</b> | Fra ambisjoner til praksis som virker        | ... 44 |

# Forord

## Årets hovedfunn

Offentlig sektor er godt i gang med både bruk av KI og sikkerhetsplanverk, men praksisen henger etter. KI brukes stadig mer, men mest til enkle oppgaver, og gevinstene tas i liten grad ut i organisasjonen. På sikkerhetsområdet er planverket på plass, men beredskapen er svakest der den skal virke i en faktisk hendelse. Kompetanse er en flaskehals på begge områdene, og på sikkerhetsområdet faller den samtidig som kravene skjerpes. Støtten fra nasjonale myndigheter holder heller ikke tritt. På KI-området mangler både retning og støtte, mens virksomhetene på sikkerhetsområdet kjenner kravene, men trenger hjelp til å gjennomføre dem.

Samtidig kan ikke innbyggernes tillit tas for gitt. Tilliten til forvaltningen av opplysninger er stabil, men overføres ikke automatisk til bruk av data i KI. KI og sikkerhet må derfor ses i sammenheng. Usikkerhet om risiko bremser bruken av KI, og KI kan gjøre angrep raskere og enklere. Felles for funnene er at utfordringen handler mindre om å etablere noe nytt, og mer om å få det som finnes til å virke i praksis.

## Formål og målgruppe

Rapporten gir et empirisk grunnlag for å prioritere innsatsen på begge områdene. Den er skrevet for beslutningstakere i departementer, direktorater, kommuner og fylkeskommuner, og for nasjonale fagmiljøer som skal støtte dem.

## Slik er rapporten bygget opp

Hver temarapport har fire hovedfunn. Begge bygger på hovedundersøkelsen til statlige virksomheter, kommuner og fylkeskommuner og på innbyggerundersøkelsen. Temarapporten om KI er utarbeidet i samarbeid med KI Norge og bruker i tillegg en ny undersøkelse blant små og mellomstore private virksomheter. Spørsmålene om cybersikkerhet er nye i år. Årets hovedfunn løfter fram det som går igjen på tvers av de to delene.

## To temaer som henger sammen

IT i praksis fyller 20 år, og årets utgave går i dybden på to temaer som preger offentlig sektor. Det ene er kunstig intelligens, det andre er sikkerhet og beredskap. Temaene kan virke ulike, men de henger tett sammen. KI gir muligheter for bedre og mer effektive tjenester, men endrer også trusselbildet og stiller nye krav til personvern, åpenhet og kontroll. Samtidig har digitalsikkerhetsloven skjerpet kravene til digital sikkerhet, og Totalforsvarsåret 2026 retter oppmerksomheten mot om planverket virker når samfunnet settes under press.

Begge temaene handler dermed om det samme spørsmålet: Klarer offentlig sektor å omsette ambisjoner, planer og krav til en praksis som virker, og som innbyggerne har tillit til?

## Utvalgte nøkkeltall

- 66 prosent av offentlige virksomheter bruker KI, mot 54 prosent i 2025 og 14 prosent i 2021, mens bare 15 prosent opplever god nasjonal støtte. Utviklingen av bruken øker raskere enn støtteapparatet.
- 83 prosent får raskere oppgaveløsning med KI, men bare 37 prosent reduserte kostnader. Forskjellen kan tyde på at gevinstene merkes hos den enkelte, men ennå ikke tas systematisk ut i organisasjonen.
- 42 prosent opplever manglende kompetanse som en stor KI-barriere, mens sikkerhetskompetanse og ressurser har falt fra 65 til 60 prosent. Det opplevde kompetansegapet kan bremse både utvikling og beskyttelse.
- Bare 57 prosent oppgir at ledelsen gir tydelige føringer for informasjonssikkerheten. Dette kan peke mot et behov for sterkere ledelsesforankring for å tydeliggjøre ansvar og prioriteringer.
- 76 prosent har prosedyrer for cyberangrep, men bare 42 prosent øver regelmessig. Planverk alene ikke er tilstrekkelig til å vite om beredskapen virker under press.
- 76 prosent opplever sikkerhetssignalene som tydelige og 80 prosent som forpliktende, men bare 51 prosent får god nasjonal støtte. Funnene peker på at hovedutfordringen ligger i gjennomføring snarere enn i flere krav.
- 31 prosent aksepterer at egne data brukes til å utvikle KI, ned fra 41 prosent, og bare 4 prosent mener det offentlige er godt beskyttet mot cyberangrep. Undersøkelsen viser et tillitsgap som kan begrense handlingsrommet.

# Om IT i praksis

*IT i praksis* er den mest omfattende undersøkelsen om digitalisering i offentlig sektor og gir et praksisnært kunnskapsgrunnlag om utvikling, erfaringer og behov hos virksomheter og innbyggere. Årets undersøkelse samler 20 års erfaring med digitalisering, og retter blikket mot to områder som blir avgjørende for offentlig sektor: kunstig intelligens og sikkerhet og beredskap.

## Om IT i praksis

*IT i praksis* er den mest omfattende undersøkelsen om digitalisering i offentlig sektor. Undersøkelsen gjennomføres av Rambøll i samarbeid med Digdir, KS, TEK Norge og NTNU, og prosjektet er i 2026 inne i sitt 20. år. Gjennom systematisk innhenting av erfaringer, vurderinger og prioriteringer fra virksomhetene selv gir undersøkelsen et helhetlig og praksisnært bilde av status og utvikling for digitaliseringsarbeidet.

Også årets undersøkelse er utformet med utgangspunkt i den nasjonale digitaliseringsstrategien *Fremtidens digitale Norge* (2024–2030), og gir slik et grunnlag for å måle utviklingen mot strategiens mål og innsatsområder. *IT i praksis* har etablert seg som et kjent kunnskapsgrunnlag for beslutningstakere i offentlig sektor, og tidligere utgaver har blant annet bidratt i strategiarbeid i departementene. Rambøll har det overordnede ansvaret for utforming, gjennomføring og de samlede vurderingene i undersøkelsen.

## Hovedundersøkelsen

*IT i praksis* 2026 ble gjennomført i perioden februar til april 2026, og dekker alle statlige virksomheter samt landets kommuner og fylkeskommuner. Respondentene er digitaliseringsansvarlige, kommunedirektører eller personer med direkte kjennskap til hvordan virksomheten arbeider med digitalisering. Spørreskjemaene er utviklet med innspill fra samtlige samarbeidspartnere bak undersøkelsen.

Den samlede svarprosenten i 2026 var på 54 prosent, fordelt på 28 prosent for statlige virksomheter og 72 prosent for kommuner og fylkeskommuner. Totalt 269 virksomheter har besvart undersøkelsen, hvorav 74 er statlige og 195 er kommunale eller fylkeskommunale. Kommunene er videre inndelt etter størrelse: store kommuner med over 40 000 innbyggere, mellomstore med 20 000–40 000 innbyggere og små kommuner med under 20 000 innbyggere. Statlige virksomheter er inndelt etter virksomhetsstørrelse, med små virksomheter fra 1–99, mellomstore fra 100 til 249 og store virksomheter over 250.

## Innbyggerundersøkelsen

Som en integrert del av *IT i praksis* gjennomfører Ipsos hvert år en innbyggerundersøkelse som belyser befolkningens oppfatninger av og erfaringer med offentlige digitale tjenester. Undersøkelsen er gjennomført blant et representativt utvalg av den norske befolkningen over 16 år, med om lag 1 000 telefonintervjuer. Rekrutteringen skjer via tilfeldig uttrekk fra telefonabonnementsregistre, og panelet har god representativitet med hensyn til kjønn, alder, inntektsnivå og region.

I årets undersøkelse deler innbyggerne sine erfaringer med offentlige digitale tjenester og vurderer blant annet tillit, informasjonssikkerhet, personvern og bruk av kunstig intelligens. Svarene gir et felles innbyggerperspektiv på temaene i begge temarapportene. De viser hvilke forventninger offentlig sektor må møte for å bevare tilliten når nye digitale løsninger utvikles og tas i bruk.

## Nye perspektiver i 2026

*IT i praksis* 2026 er utvidet med nye temaer og datakilder som styrker kunnskapsgrunnlaget for de to temarapportene. Utvidelsene belyser både hvordan offentlige virksomheter arbeider med cybersikkerhet, og hvordan private virksomheter møter mulighetene og utfordringene knyttet til kunstig intelligens. Samlet gir dette et bredere bilde av digitaliseringen i Norge.

Spørsmålene om cybersikkerhet kartlegger virksomhetenes prosedyrer for rapportering og håndtering av cyberangrep, beredskap for gjenoppretting av systemer og data, tilgang på relevant kompetanse og gjennomføring av regelmessige øvelser. Siden spørsmålene er nye, etablerer resultatene et utgangspunkt for senere målinger.

Den nye undersøkelsen gjennomført av Ipsos blant rundt 160 små og mellomstore private virksomheter belyser samtidig modenhet, barrierer og behov for offentlig veiledning om kunstig intelligens. Datagrunnlaget gjør det mulig å sammenligne offentlig og privat sektor og vurdere hvilke utfordringer som går på tvers av norsk arbeidsliv.





• Temarapport 1:2026

# Kunstig intelligens

Hva trenger Norge for å lykkes med bruk av KI?

# Oppsummering

Norge har tatt et stort steg. Bruken av kunstig intelligens har skutt fart de siste årene, og et stort flertall av virksomhetene rapporterer at de er i gang. Det er en betydelig endring fra tidligere år, men å ta i bruk KI er ikke det samme som å lykkes med KI.

Tallene fra *IT i praksis 2026* viser at Norge befinner seg i overgangen mellom to faser. Den første fasen, som handler om å tørre å starte, å teste og å bygge de første erfaringene, er i stor grad tilbakelagt. Den andre fasen er vanskeligere, hvor virksomhetene må gå fra pilot til drift, fra enkeltinitiativ til systematisk bruk, fra teknologiutprøving til reell verdiskaping i kjerneoppgavene. Det er i denne overgangen de største utfordringene viser seg.

Gevinstene er reelle, men de er ikke jevnt fordelt og potensialet er langt fra realisert. Stadig flere virksomheter rapporterer om raskere oppgaveløsning, men gevinstene realiseres i stor grad på individnivå. Men for å hente ut de store gevinstene er ikke løsningene primært teknologiske, men organisatoriske. Bare halvparten har en tydelig strategisk forankring av digitaliseringsarbeidet, og skal gevinstene tas ut i organisasjonen, må virksomhetene investere i strategi, kompetanse og styring.

De største barrierene nå er usikkerhet og forutsetninger. Vi ser at barrierene som holder virksomhetene tilbake har endret karakter, og det handler ikke lenger primært om teknologi eller økonomi, men om usikkerhet og risikovurderinger knyttet til hvordan de skal ta i bruk kunstig intelligens. Funnene indikerer at flere virksomheter nå er kommet langt nok i sin bruk til å møte de reelle dilemmaene KI reiser.

Samtidig øker skepsisen til bruk av KI i offentlig sektor i befolkningen, særlig blant de yngre. Bruk av KI i offentlig sektor handler ikke bare om teknologi og effektivitet, men også om legitimitet, tillit og opplevd verdi for innbyggerne. Dette fordrer et offentlig Norge som aktivt tar ansvar for å bygge og opprettholde tilliten.

Det overordnede bildet viser at disse utfordringene ikke kan overlates til enkeltvirksomheter selv å løse. Det krever en felles innsats. Samtidig opplever virksomheter at de ikke får nok støtte fra nasjonale myndigheter, og et flertall opplever de politiske styringssignalene innen KI som verken tydelige eller forpliktende. Virksomhetene ønsker veiledning på flere ulike områder slik tidligere *IT i praksis* har vist, og etterspør i år konkret og praktisk veiledning, særlig på regulatoriske og juridiske spørsmål knyttet til KI.

*IT i praksis 2026* peker på fire hovedutfordringer som til sammen beskriver gapet mellom der vi er og dit vi vil. De fire utfordringene er ikke uavhengige av hverandre. De forsterker hverandre, og peker alle i retning av det samme behovet av mer moden KI-bruk, tydeligere nasjonal koordinering og retning, bedre veiledning og sterkere støttestrukturer for virksomheter som vil, men ikke vet hvordan.



# Fremtidens digitale Norge

Kunstig intelligens er i ferd med å bli en avgjørende og grunnleggende del av hvordan både offentlige og private virksomheter utvikler og leverer tjenester, organiserer arbeid og skaper verdi. Det er utvilsomt viktig at offentlige myndigheter finner sin rolle i å drive dette arbeidet framover på en trygg, ansvarlig og formålstjenlig måte.

## Potensialet i kunstig intelligens

KI kommer til å bli en avgjørende og grunnleggende del av hvordan både offentlige og private virksomheter utvikler og leverer tjenester, organiserer arbeid og skaper verdi. KI påvirker ikke bare effektivitet, men også beslutningsprosesser, kompetansebehov, ansvarsforhold og samspillet mellom mennesker, organisasjon, teknologi og samfunn.

Teknologien har et betydelig potensial for økt produktivitet, bedre tjenester og mer bærekraftig ressursbruk. Den kan støtte mer treffsikre beslutninger, automatisere tidkrevende oppgaver og frigjøre kapasitet der behovene er størst. Dette gjør KI særlig relevant for å møte sentrale samfunnsutfordringer i Norge, som demografiske endringer, press på arbeidskraft og økonomi og økende forventninger fra innbyggere og brukere av offentlige tjenester.

Samtidig griper bruk av KI direkte inn i kjerneoppgaver som tjenesteleveranse, myndighetsutøvelse og forvaltning av fellesskapets ressurser. Hvordan teknologien tas i bruk, har direkte betydning for rettsikkerhet, legitimitet og tillit. Det er nettopp derfor offentlige myndigheter må ta en aktiv rolle som tilrettelegger og regulator, for å sikre trygg og ansvarlig bruk av KI for alle, og for å ivareta digital suverenitet og kontroll over egen data og infrastruktur. Behovet for en slik aktiv rolle er reelt. Manglende kompetanse og usikkerhet om risiko har blitt de to raskest voksende barrierene for trygg og ansvarlig bruk av KI.

Funnene blant innbyggerne er at befolkningens tillit til bruk av KI fortsatt er noe lav, særlig når teknologien tas i bruk i offentlige tjenester. Dette understreker behovet for åpenhet, tydelig kommunikasjon og ansvarlig innføring for å sikre legitimitet og trygghet i befolkningen.

## Strategiske ambisjoner og behovet for handling

Digitaliseringsstrategien *Fremtidens digitale Norge* (2024–2030) legger til grunn at Norge har gode forutsetninger for å lykkes med kunstig intelligens: høy digital modenhet, sterke fagmiljøer, god tilgang på data og et samfunn preget av høy tillit. Regjeringens mål er store: innen 2030 skal Norge være verdens mest digitaliserte land. Funn fra *IT i praksis* 2026 viser imidlertid at det er en vei igjen å gå de neste årene:

- 3 av 10 virksomheter i offentlig og privat sektor **bruker ikke KI** i dag.
- 9 av 10 offentlige virksomheter oppgir at de i noen, stor eller svært stor grad opplever **usikkerhet om risiko** som en barriere for at de kan bruke KI på en trygg og ansvarlig måte.
- 9 av 10 offentlige virksomheter oppgir at de i noen, stor eller svært stor grad opplever **manglende kompetanse** i egen virksomhet som en barriere for å bruke KI på en trygg og ansvarlig måte.

- 1 av 7 offentlige virksomheter opplever at de i stor eller svært stor grad får **god støtte** fra nasjonale myndigheter på spørsmål om KI.
- Omtrent 7 av 10 offentlige virksomheter oppgir at de i noen, liten eller svært liten grad opplever styringssignalene på KI-området som **tydelige og forpliktende**.
- 4 av 10 i befolkningen, og halvparten av 16–24-åringene, er **skeptiske til bruk av KI** i offentlige tjenester.

## KI Norge – et nytt virkemiddel

KI Norge er etablert som en nasjonal arena og spissmiljø for ansvarlig, innovativ og trygg utvikling og bruk av kunstig intelligens i offentlig og privat sektor. Organisasjonen er lagt til Digdir og skal samarbeide tett med Nkom og Datatilsynet for å drive en regulatorisk sandkasse for trygg og ansvarlig utvikling av KI, samt samarbeide om veiledning. Den nye tjenesten skal bidra til erfarings- og kunnskapsdeling mellom næringsliv, academia og forskningsmiljøer, og være et samlende kompetansemiljø i skjæringspunktet mellom forvaltning, teknologi og samfunn.

Etableringen er et direkte svar på et klart identifisert behov. Mange virksomheter har vilje og interesse for å ta i bruk KI, men de mangler retning og kapabiliteter til å få dette til. KI Norge skal bidra til å fylle dette gapet.

## KI Norge og IT i praksis

*IT i praksis* har målt bruken av KI i offentlig sektor over flere år, og tallene viser en tydelig positiv utvikling. I 2025 registrerte vi at 54 prosent av offentlige virksomheter hadde tatt i bruk KI. I 2026 er andelen økt til nærmere 70 prosent.

Når flertallet av respondentene opplever de politiske styringssignalene som verken forpliktende eller klare, og i tillegg gir uttrykk for et stort behov for veiledning, korresponderer funnene godt med regjeringens uttalte ambisjoner om å styrke veiledningsarbeidet og sikre ansvarlig utvikling og bruk av KI i offentlig sektor. I år har *IT i praksis* hatt et ekstra fokus på nettopp veiledningsbehov og ønsker i forbindelse med bruk av KI. Funnene understreker at etterspørselen etter konkret, praktisk støtte er betydelig.

Samlet tegner tallene et bilde av en offentlig sektor i bevegelse: Ambisjonsnivået er høyt, og viljen er til stede. Det som mangler er ikke bare retning, men verktøy, kompetanse og trygghet nok til å handle. Det er i nettopp dette rommet KI Norge er tenkt å virke.

**Rambøll, TEK Norge, KS, NTNU og Digitaliseringsdirektoratet**



# Funn fra *IT i praksis*: Fire hovedutfordringer

Resultatene peker på fire hovedutfordringer som til sammen beskriver gapet mellom der vi er og dit vi vil. I dette kapittelet ser vi på hvordan bruken utvikler seg, hvilke gevinster som realiseres, hvilke barrierer som vokser og hvordan innbyggerne forholder seg til bruken av KI i offentlig sektor. Utfordringene er ikke uavhengige av hverandre, men forsterker hverandre og peker mot et felles behov for tydeligere retning og bedre støtte.



## Utbredelsen øker, men modenheten henger etter

Bruken av kunstig intelligens er ikke lenger et randfenomen i norske virksomheter. Andelen som rapporterer at de tar teknologien i bruk, har økt over flere år, og for mange er KI i ferd med å bli en integrert del av hvordan oppgaver løses i det daglige. Samtidig er bruken fortsatt i hovedsak knyttet til relativt enkle og avgrensede anvendelser, som tekstutkast, oppsummeringer og chatboter. Mer avansert og integrert bruk, som for eksempel KI i fagsystemer, prediksjon eller analyse av komplekse datasett, er foreløpig forbeholdt et mindretall. Likevel ser mange potensialet i mer gjennomgripende løsninger. Veien videre handler om å utvikle bruken, både i bredde og i dybde.



# Bruken av KI fortsetter å øke både i offentlig og privat sektor

Flertallet av virksomhetene både i offentlig og privat sektor er nå i gang med KI. Det markerer et taktskiftet vi så i fjor holder frem. KI er ikke lenger et randfenomen i offentlig sektor, når nær syv av ti virksomheter i stat og kommune oppgir at de bruker teknologien.

## Høye ambisjoner for bruk av KI

Norge har satt seg ambisiøse mål for digitalisering av offentlig sektor. Ambisjonene er klare: KI skal være et sentralt verktøy for å effektivisere offentlige prosesser, frigjøre ressurser og levere bedre tjenester til innbyggere og næringsliv. Dette skal bidra til at Norge blir det mest digitaliserte landet i verden innen 2030.

Tidligere utgaver av *IT i praksis* har imidlertid dokumentert et betydelig gap mellom ambisjon og realitet på KI-bruk. I perioden 2021–2024 rapporterte kun én av tre virksomheter at de hadde erfaring med KI, og blant kommunene var andelen enda lavere, med bare 15 prosent. I 2025 så vi en markant økning i bruk hvor over halvparten av virksomhetene rapporterte om bruk av KI.

## Fortsatt økning i bruk av KI

Funnene fra årets undersøkelse viser at denne utviklingen fortsetter. I 2026 rapporterte 66 prosent av offentlige virksomheter at de brukte KI. Veksten er betydelig, selv om den prosentvise økningen fra 2025 til 2026 på 12 prosentpoeng er mindre enn utviklingen fra 2024 til 2025, som var på 34 prosentpoeng.

Utviklingen peker mot økt bruk av KI i hele feltet. Gjennomsnittlig rapportert KI-bruk blant alle respondentene har økt fra 2,39 til 2,65 på en skala fra 1 til 5. Andelen som svarer i svært liten grad faller fra 16 prosent til 7 prosent, og andelen som svarer i liten grad fra 30 prosent til 26 prosent. Samlet sett peker tallene mot en sektor der færre virksomheter står helt utenfor utviklingen, og hvor terskelen for å ta KI i bruk er tydelig senket.

Samtidig viser også tallene at den høyeste andelen svarer i noen grad, med 62 prosent. Hvorvidt dette er et tall som bør øke er et spørsmål som vil være viktig fremover. Det er ikke nødvendigvis et formål i seg selv at alle skal bruke KI i utstrakt grad, men at det er hvordan de bruker det som blir det viktige i årene som kommer.

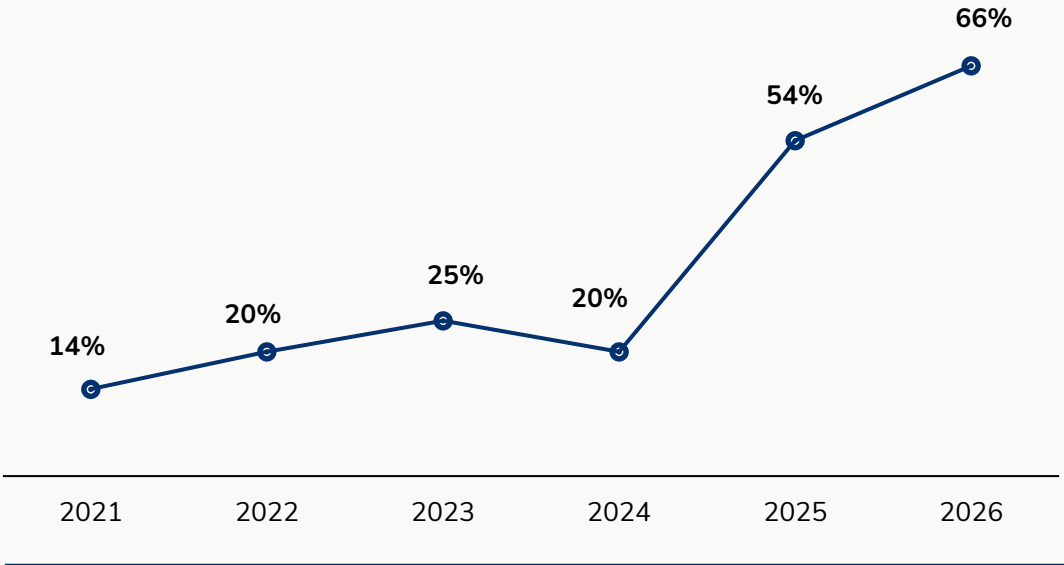
Vel så interessant er det derfor å se på dybden i bruken. Syv av ti offentlige virksomheter oppgir at de enten tester, bruker eller utvikler KI-løsninger, mens seks av ti private oppgir det samme. Dette indikerer at KI ikke lenger er forbeholdt enkeltprosjekter eller pilotforsøk, men at teknologien er i ferd med å bli en integrert del av hvordan offentlig sektor løser sine oppgaver.

## Fortsatt gjenstående arbeid

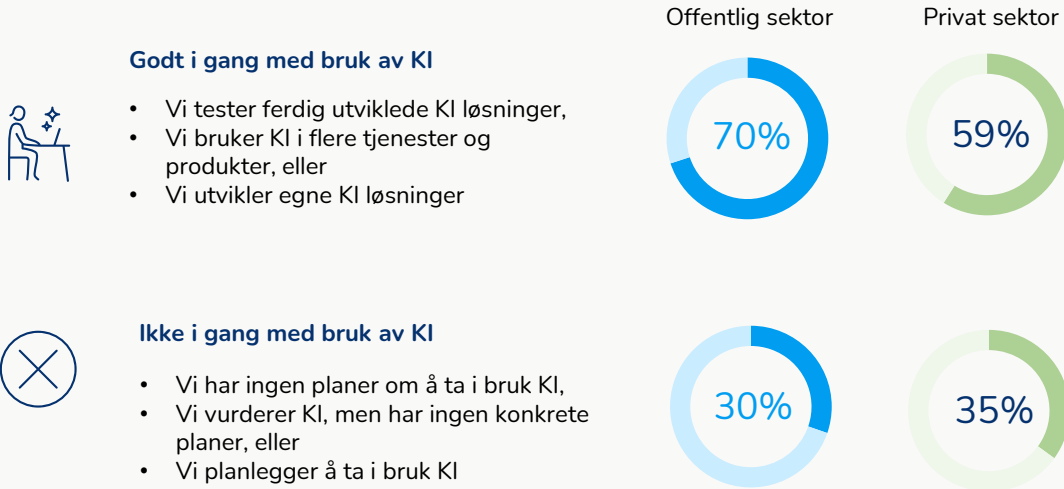
Det gjenstående arbeidet handler i mindre grad om å få flest mulig i gang, og i større grad om å sikre at virksomheter som allerede bruker eller skal ta i bruk KI, gjør det på en god og ansvarlig måte. Det innebærer å bygge kompetanse, etablere tydelige rammer for styring og risikohåndtering og sørge for at teknologien brukes der den faktisk gir verdi. Samtidig må man ikke glemme de resterende tre av ti innen både offentlig og privat sektor som ikke er i gang, og sørge for at KI-løsninger er lett tilgjengelig for alle.

Tallene viser altså at det fortsatt finnes et betydelig potensial for å ta KI videre i bruk i både offentlig og privat sektor, og i begge sektorer gjenstår det arbeid for å ta teknologien i bruk i større bredde og dybde. Det vil være avgjørende for å realisere mer av verdien som KI kan gi i årene fremover.

Andelen virksomheter som i **noen, stor eller svært stor grad** har tatt i bruk kunstig intelligens i interne prosesser og tjenesteleveranser



Hvordan vil du beskrive virksomhetens **modenhet** når det gjelder bruk av KI?



# Bruken av KI er ofte enkel, men flere ser potensialet i mer gjennomgripende løsninger

KI er på full vei inn i offentlige og private virksomheter, men bruken er fortsatt i stor grad avgrenset til enkle oppgaver og støtte rundt eksisterende arbeidsmåter. Mer avanserte og integrerte anvendelser er foreløpig mindre vanlige i dag, selv om mange ser et tydelig potensial for videre utvikling.

## Løsningene offentlig sektor bruker i dag er enkle

Bruken av KI i offentlig sektor er i stor grad preget av avgrensede og relativt enkel bruk. KI tas primært i bruk som et støtteverktøy rundt eksisterende arbeidsmåter, hvor teknologien hjelper ansatte med konkrete deloppgaver som tekstutkast, oppsummeringer, informasjonssøk og dokument- og saksarbeid. Å analysere dokumenter og lage utkast er den mest utbredte bruken, der 59 prosent oppgir at dette er i daglig drift. Informasjonsassistenter som chatboter er også godt etablert, med 43 prosent i daglig bruk. Dette er løsninger som kan innføres uten store endringer i organisering eller arbeidsprosesser, og som derfor ofte blir virksomhetenes og de ansattes første møte med KI i praksis.

## Flere ser potensialet i mer avanserte løsninger

Samtidig peker funnene på et tydelig ambisjonsnivå utover denne første fasen. Mange virksomheter ser potensialet i mer integrert og gjennomgripende bruk, der KI i større grad blir en del av kjerneprosessene gjennom tettere kobling til fagsystemer, mer helhetlig bruk av virksomhetsdata, eller løsninger som påvirker hvordan tjenester utvikles og leveres.

De mest komplekse bruksområdene er foreløpig lite utbredt i daglig drift. KI-funksjonalitet integrert i fagsystemer som beslutningsstøtte benyttes daglig av kun 17 prosent, analyse av komplekse datasett kun av 11 prosent, og predikerende løsninger, som å forutse vedlikeholdsbehov eller skolefravær, brukes bare av 5 prosent.

Dette peker mot at det antakelig er store språkmodeller som er i bruk blant virksomhetene, og ikke prediktive eller analytiske KI-modeller.

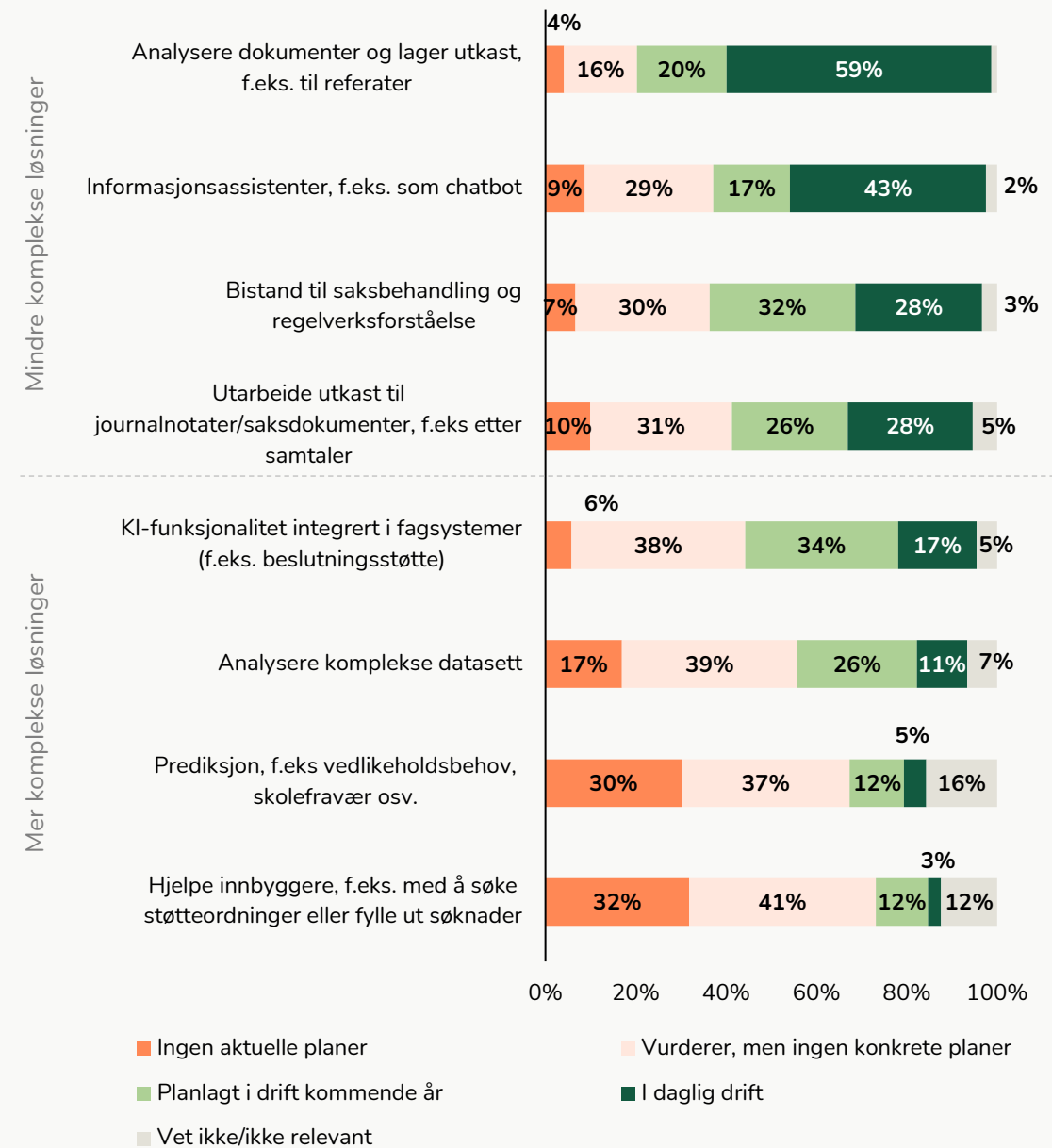
Likevel rapporterer mellom 37 og 41 prosent at de vurderer slike løsninger, og mellom 12 og 34 prosent planlegger innføring i løpet av kommende år. Skiftet fra enkeltstående verktøybruk til strategisk anvendelse er med andre ord noe mange ønsker å bevege seg mot, selv om det for de fleste fortsatt beskrives som et neste steg.

## Virksomhetene vil utvikle bruken og trenger støtte til å realisere planene

Spenningsfeltet mellom dagens avgrensede bruk og ambisjonen om mer integrerte løsninger kan forstås som et uttrykk for en tidlig modningsfase. Mange virksomheter er fortsatt i en utforskende fase, der KI først og fremst prøves ut i enkeltstående bruksområder som gir erfaring med teknologiens muligheter og begrensninger. Virksomhetene er slik på vei fra tidligfase og enkel bruk til moden og mer gjennomgripende KI-anvendelse.

Samtidig tyder funnene angående veiledning og støtte, som vi vil komme tilbake til, på at overgangen til mer integrert bruk ikke først og fremst handler om vilje. Behovet framstår ikke bare som teknologisk, men også som organisatorisk. Skal KI tas i bruk på en mer strategisk og bærekraftig måte, krever det tydelige strukturer, sterk kompetanse og målrettet støtte i virksomhetene. Dette vil bidra til mer gjennomgripende KI-løsninger, som også vil bidra til at virksomhetene i større grad kan realisere gevinster fra bruken.

I hvilken grad tar din virksomhet i bruk KI på følgende oppgaveområder?





## Gevinster realiseres, men ikke på organisatorisk nivå

Undersøkelsen viser at KI gir resultater. Andelen virksomheter som rapporterer om gevinster har økt på alle målte områder, og særlig knyttet til raskere oppgaveløsning og bedre kvalitet i tjenester og prosesser. Samtidig viser årets undersøkelse at gevinstene i stor grad realiseres på individnivå, mens få virksomheter klarer å ta dem ut strukturelt. Forskjellene henger tett sammen med organisatoriske forutsetninger som data, kompetanse, styring og strategisk forankring. Gevinster oppstår ikke av seg selv, for det er virksomhetene som har gjort organisatoriske grep som høster mest.



# Stadig flere virksomheter realiserer gevinster

Andelen som rapporterer reelle gevinster har økt på alle målte områder fra 2025 til 2026. Funnene tegner et bilde av en sektor som ikke bare er i gang med bruk av KI, men at bruken gir resultater og virksomhetene begynner å høste konkrete gevinster.

## KI gir reelle gevinster, særlig i tempo og kvalitet

Andelen som rapporterer at de i noen, stor eller svært stor grad har realisert gevinster, har økt markant fra 2025 til 2026 på tvers av alle målte områder.

Den mest utbredte gevinsten er raskere oppgaveløsning, der 83 prosent, en økning på 22 prosentpoeng fra 2025, oppgir at de i noen, stor eller svært stor grad har opplevd dette, fulgt av bedre kvalitet i prosesser og tjenester, som 63 prosent nå rapporterer, mot 57 prosent året før. Dette er gevinster som i stor grad samsvarer med de enkle bruksområdene som vi ser blant virksomhetene i dag. Når ansatte bruker KI til å utarbeide utkast, søke i informasjon eller håndtere saksarbeid, blir oppgavene løst raskere og med høyere kvalitet.

Reduserte kostnader er også i vekst, med 37 prosent i 2026 mot 25 prosent i 2025. Redusert bemanning er derimot den gevinsten færrest rapporterer. Dette reflekterer trolig at dagens bruk primært støtter og effektiviserer eksisterende arbeid, heller enn å erstatte stillinger eller endre store arbeidsprosesser i virksomhetene.

Gevinstbildet peker dermed i en tydelig retning: KI brukes i dag som et produktivitetstverktøy som frigjør tid og løfter kvaliteten på arbeidet som utføres, men gjør ikke store endringer i organisasjonen. Det er naturlig å forvente at gevinstene vil øke ytterligere etter hvert som virksomhetene beveger seg fra enkel verktøybruk mot mer integrerte og strategiske anvendelser. Dette kan på sikt også ha større påvirkning på kostnader og ressurser enn det vi ser tendensen til i dag.

## Gevinstene er drevet av atferdsendring, ikke systemendring

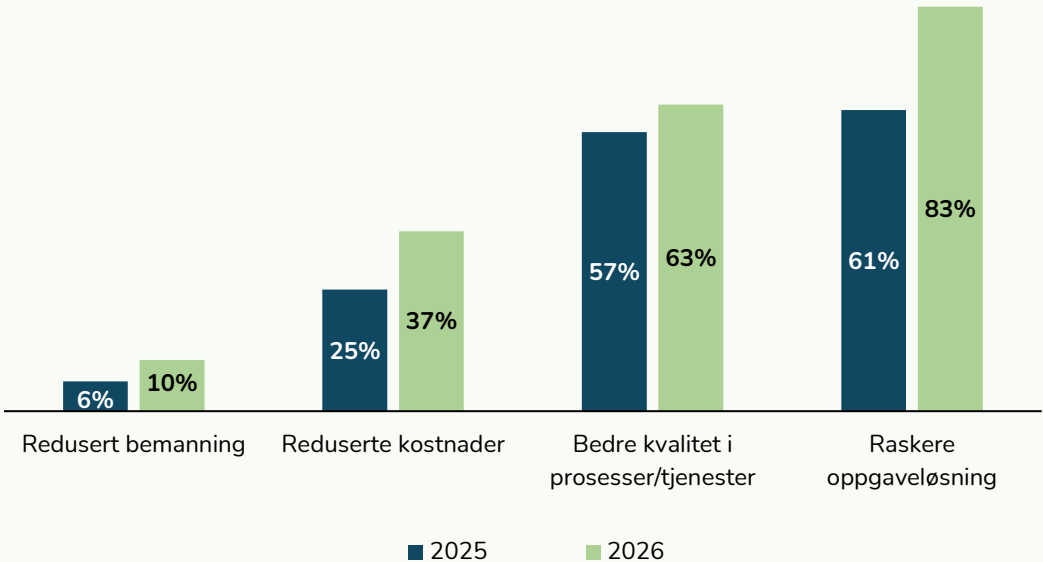
Når 83 prosent opplever raskere oppgaveløsning, men bare 37 prosent rapporterer reduserte kostnader, tyder det på at gevinstene foreløpig realiseres på individnivå og ikke på organisasjonsnivå. Ansatte opplever å jobbe raskere og bedre, men virksomhetene har i liten grad tatt ut gevinstene strukturelt gjennom reduserte kostnader eller omorganisering.

Frigjort tid omdisponeres ikke systematisk til nye oppgaver eller besparelser, men forsvinner inn i eksisterende arbeidsflyt. Det samme mønsteret finner vi igjen i forskning på KI og produktivitet: Produktivitetsgevinstene i oppstartsfasen er reelle, men de «absorberes» av den enkelte fremfor å synliggjøres i driften som helhet.<sup>1</sup>

### Bygger momentum for neste fase

Våre funn kan være typiske trekk ved en tidlig fase. Når nye og generelle teknologier som KI introduseres, går det vanligvis en periode med læring, utprøving og kompetansebygging før gevinstene blir synlige på organisasjonsnivå. Først når virksomhetene har bygget kompetanse, etablert tydelige rammer for bruk og har koblet KI tettere til kjerneprosesser og fagsystemer, vil de være godt rigget for å ta ut gevinstene strukturelt gjennom omorganisering, nye arbeidsmåter og reelle endringer i hvordan tjenester utvikles og leveres. Det vi observerer nå, kan med andre ord være forarbeidet til den mer gjennomgripende verdiskapingen som først kommer til syne i neste fase.

Andelen som svarer at de i **noen, stor eller svært stor grad** har realisert følgende gevinster gjennom bruk av KI



# Gevinstene realiseres ikke av seg selv

Funnene om gevinster er lovende. De forteller imidlertid også at det ikke er nok bare å ta i bruk KI. Skall teknologien gi reelle og varige gevinster, må en rekke organisatoriske forutsetninger på plass. Et strategisk forhold til digitaliseringsarbeidet i virksomheten er avgjørende.

## Strategisk forankring er fortsatt mangelvare

Et sentralt funn er at mange virksomheter ennå ikke har forankret sitt arbeid med digitalisering i virksomhetens strategiarbeid. Kun 27 prosent oppgir at de har integrert digitalisering i sitt overordnede strategiarbeid, og 23 prosent at de har en strategi de følger systematisk. Til sammen betyr det at knapt halvparten av virksomhetene har en tydelig strategisk ramme rundt sitt digitaliseringsarbeid, og slik også rundt KI-arbeidet. Nær en av ti jobber fortsatt ad hoc, uten forankring i strategi. Dette er bekymringsfullt, fordi strategisk forankring ikke bare handler om formelle dokumenter, men om å tydeliggjøre hvilke gevinster man ønsker, hvem som har ansvar og hvordan teknologien kobles til virksomhetens mål, oppgaveløsning og tjenesteleveranser.

## Færre som opererer systematisk og etter en strategi

Andelen virksomheter med en tydelig strategisk forankring, enten gjennom integrasjon i det overordnede strategiarbeidet eller systematisk oppfølging av en etablert strategi, har gått noe ned, fra 54 prosent i 2025 til 50 prosent i 2026. I den andre enden av skalaen faller andelen som jobber ad hoc eller som har en strategi de ikke følger systematisk, fra 34 prosent til 28 prosent. Endringen skjer dermed i mellomstadiet, hvor funnene viser at andelen virksomheter som jobber systematisk med digitalisering, men uten en overordnet strategi, har nesten doblet seg fra 11 prosent i 2025 til 21 prosent i 2026.

Funnene peker på at flere virksomheter arbeider mer systematisk med digitalisering, men uten en tydelig overordnet strategisk ramme. Mangel på en strategisk tilnærming kan føre til manglende eierskap blant de

ansatte<sup>2</sup>, noe som igjen påvirker KI-arbeidet og gjør både prioritering og realisering av gevinster mer krevende.

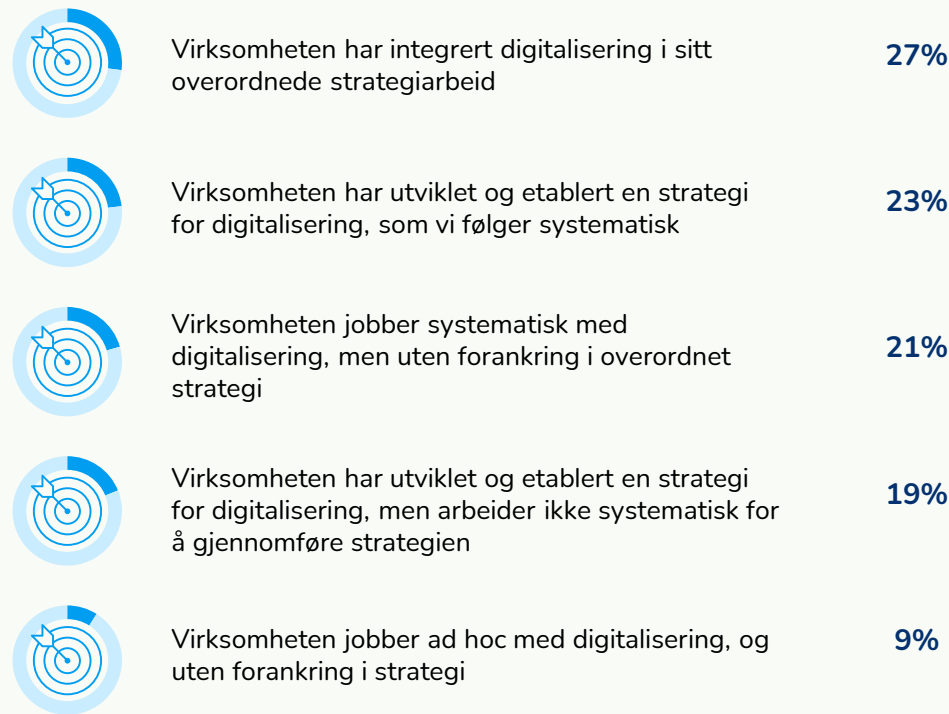
## Hvordan bør virksomhetene arbeide med gevinstrealisering?

Dette bildet gjenkjennes fra tidligere erfaring og praksis på digitalisering i offentlig sektor. Rambølls kunnskapsgrunnlag om generativ KI i statlige virksomheter, utarbeidet på oppdrag fra Digitaliserings- og forvaltningsdepartementet, peker på at svært få statlige virksomheter har formulert konkrete effektmål eller gevinster for sin KI-bruk.<sup>3</sup> Kun én av ti virksomheter oppgir at de har satt slike mål. Uten definerte mål er det vanskelig å måle om gevinstene faktisk tas ut. Rapporten understreker at gevinstene som oppstår i tidlig fase ofte er subjektive og individuelle. De ansatte opplever at de jobber raskere eller bedre, men virksomheten har ikke systemene eller strukturene på plass til å omsette dette til dokumenterte resultater på organisasjonsnivå.

## Sammenhengen mellom forutsetninger og realiserte gevinster

Gevinster oppstår ikke tilfeldig. De er resultatet av at virksomheten har gjort de riktige grepene i forkant. Dette understreker at veien til gevinstrealisering ikke primært er teknologisk. Veien til gevinstrealisering ved bruk av KI er organisatorisk. Virksomheter som ønsker å gå fra enkle produktivitetsforbedringer på individnivå til strukturelle gevinster på virksomhetsnivå, må investere parallelt i strategi, kompetanse og styring. Uten denne investeringen risikerer man at KI-bruken forblir ujevnt fordelt, vanskelig å måle og at gevinstene absorberes i den daglige arbeidsflyten uten å gi varige effekter.

Hvilken påstand beskriver best din virksomhets strategiske tilnærming til digitalisering?



<sup>2</sup> og <sup>3</sup> Rambøll. 2025. Generativ KI i statlige virksomheter: <https://www.regjeringen.no/no/dokumenter/generativ-ki-i-statlige-virksomheter/id3109999/>

1% har svart «vet ikke/ikke relevant»

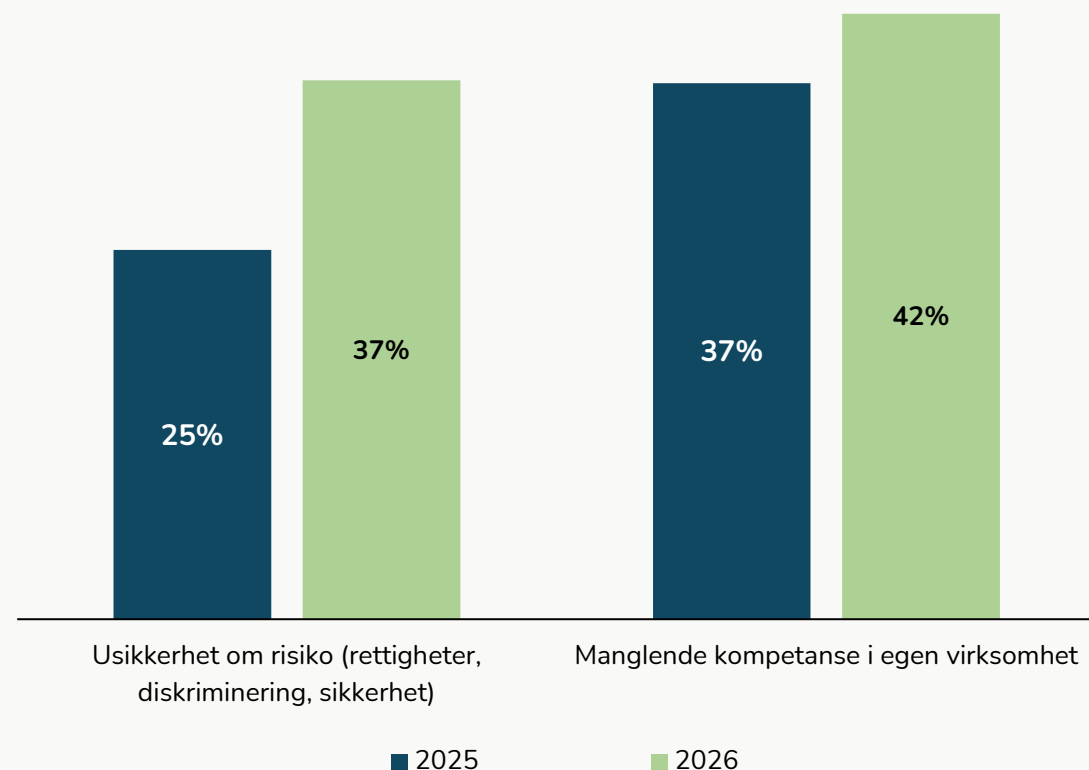


## Barrierene handler i økende grad om usikkerhet og forutsetninger

Selv om bruken av KI øker og flere virksomheter realiserer konkrete gevinster, forsvinner ikke barrierene, men de endrer karakter. Manglende kompetanse og usikkerhet om risiko er nå de to dominerende hindrene, og begge har vokst fra 2025 til 2026. Det viser at de viktigste utfordringene ikke primært handler om økonomi, ledelsesforankring eller endringsmotstand, men om kunnskap og trygghet. Møtes ikke disse barrierene, kan bruk og gevinster i møte med KI stagnere. At de største barrierene vokser i en periode der bruken øker, er et viktig signal, og peker mot et tydelig behov for kompetansebygging, veiledning og tydelige rammeverk.



Andelen virksomheter som i **stor eller svært stor grad** opplever følgende barrierer for å ta i bruk KI på en trygg og ansvarlig måte.



# Barrierene endrer seg i takt med høyere ambisjoner til bruk av KI

Selv om bruken av KI øker, viser funnene at barrierene ikke forsvinner. De to største hindrene for å ta i bruk KI i interne prosesser og tjenesteleveranser har begge økt fra 2025 til 2026, og tegner et bilde av en sektor som møter nye utfordringer etter hvert som ambisjonsnivået stiger.

## Hva hindrer trygg og ansvarlig bruk av KI i dag?

Størst vekst finner vi i usikkerhet knyttet til risiko om eksempelvis rettigheter, diskriminering og sikkerhet. Her ser vi en økning på 12 prosentpoeng fra i fjor til i år. Det er kun 1 av 10 som oppgir at de i liten eller svært liten grad opplever usikkerhet om risiko som en barriere. Det vil si hele 9 av 10 opplever risiko som minimum en barriere i noen grad. Tilnærmet 4 av 10 opplever det i stor til svært stor grad.

En naturlig tolkning er at dette ikke er et tegn på at risikobildet har forverret seg, men snarere at flere virksomheter nå er kommet langt nok i sin bruk av KI til å møte de juridiske og etiske dilemmaene som faktisk bruk reiser. Jo mer konkret og integrert bruken blir eller har mål om å bli, desto mer påtrengende blir spørsmålene om personvern, diskriminering og ansvar.

Manglende kompetanse i egen virksomhet er den største barrieren. Funnet henger sammen med det vi så i kapitlet om gevinster, som peker mot at kompetanse ikke bare er en forutsetning for å ta i bruk KI, men også for å ta ut gevinstene i organisasjonen. Også her finner vi at 1 av 10 oppgir barrieren som i liten eller svært liten grad.

At nær halvparten av virksomhetene fortsatt opplever dette som en stor eller svært stor barriere, understreker at tilgang på kompetanse eller kompetansebygging må prioriteres høyere og mer systematisk enn det som er tilfellet i dag.

## Barrierene er store på tvers av undergrupper

Bildet av barrierene nyanseres ytterligere når vi skiller mellom ulike typer virksomheter. På de fleste barrierene er stat og kommune relativt likestilte. Men

på én faktor skiller kommunene seg markant ut: For høye investeringskostnader oppleves som en stor eller svært stor barriere av hele 47 prosent av kommunene (23 prosent i staten).

Dette peker på at stramme budsjetter og begrenset handlingsrom i kommunene gjør det vanskeligere å prioritere KI-investeringer, selv når viljen er til stede.

Funnet bør tas på alvor i utformingen av nasjonale støtteordninger og finansieringsmekanismer. For små og mellomstore virksomheter er bildet enda tydeligere. Manglende kompetanse i egen virksomhet toppe listen for begge grupper, og skiller seg klart fra alle andre målte barrierer.

## Kompetanse og risiko hindrer bruk av KI

For virksomhetene som ennå ikke har tatt i bruk KI, er det de samme to barrierene som dominerer: manglende kompetanse og usikkerhet om risiko. Dette viser at de viktigste hindrene handler om kunnskap og trygghet. Virksomhetene som står på sidelinjen eller avventer bruk av KI gjør det i stor grad fordi de ikke vet nok om teknologien eller anvendelsen av den, og fordi de er usikre på hvilke juridiske, etiske og sikkerhetsmessige risikoer som følger med. Dette er også grunnleggende utfordringer for virksomhetene i møte med KI, og som krever tilgang på kompetanse og statlig koordinering av målrettede tiltak i form av kompetansebygging, veiledning og tydelige nasjonale rammeverk som gir virksomhetene den tryggheten de trenger for å ta steget.

At disse to barrierene vokser i en periode der bruken øker, er et viktig signal. Det indikerer at offentlig sektor i stor grad er overlatt til seg selv i møte med utfordringer som i sin natur er sektorovergripende.

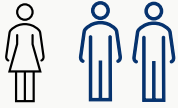


## For mange innbyggere er skeptiske til bruk av KI i offentlig sektor

Mens offentlig sektor satser på KI, viser funnene at befolkningens holdninger til teknologien beveger seg i en annen retning. Skepsisen har økt på flere områder, særlig knyttet til bruk av KI i beslutninger som vedrører en selv og bruk av egne data til å utvikle KI-tjenester. Samtidig er en relativt stor andel positiv til bruk av KI der det kan gi bedre tjenester. Funnene peker på at bruk av KI i offentlig sektor ikke bare handler om teknologi og effektivitet, men også i høy grad om tillit, legitimitet og opplevd verdi for innbyggerne.



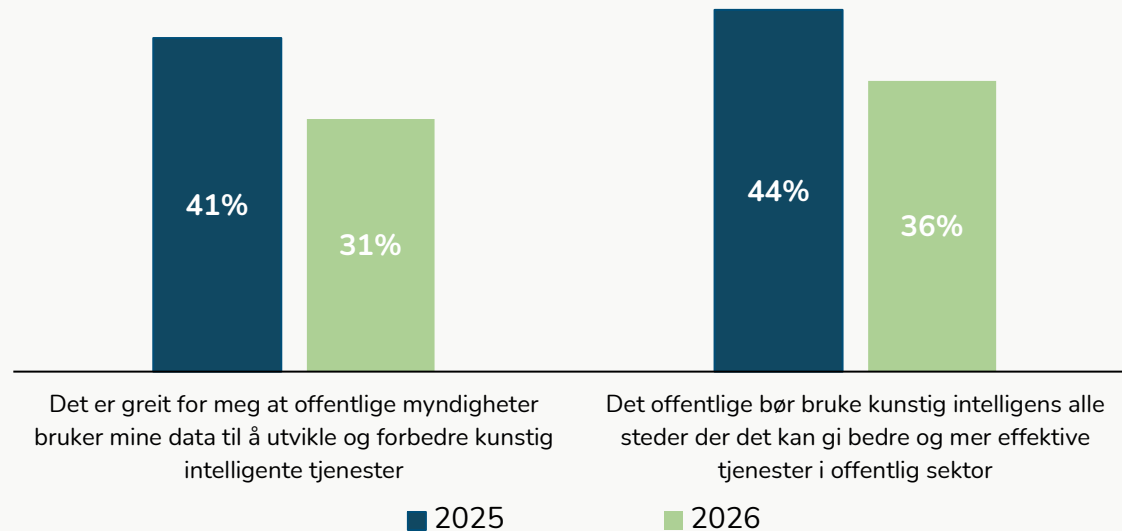
Andel av innbyggere som er **uenig eller helt uenig** i at



Det er greit at offentlig sektor benytter KI som støtte til å fatte beslutninger om meg

39%

Andelen som svarer at de er **enig eller helt enig** i følgende påstander



Spørsmålet «det offentlige bør bruke kunstig intelligens alle steder der det kan gi bedre og mer effektive tjenester i offentlig sektor» ble i 2025 stilt som «bruk av kunstig intelligens er et riktig grep for å sikre bedre og mer effektive tjenester i offentlig sektor».

# Innbyggerne har blitt mer tilbakeholdne med bruk av deres egne data i offentlige tjenester

Mens offentlig sektor skal satse på kunstig intelligens, viser funnene fra innbyggerundersøkelsen at befolkningens holdninger til teknologien beveger seg i motsatt retning. Skepsisen øker og tegner et bilde av et tillitsgap som kan bli en betydelig utfordring dersom det ikke tas på alvor.

## Bruk av KI i offentlig sektor krever tillit

Bruk av kunstig intelligens i offentlig sektor handler ikke bare om teknologi, effektivitet og interne gevinster. Det er avgjørende for tjenesteleverandørene at de oppleves som legitime, at innbyggerne har tillit til dem og at tjenesteutviklingen gir opplevd verdi for innbyggerne. Offentlige tjenester forvalter store mengder data og treffer beslutninger som direkte påvirker enkeltpersoner. Hvordan offentlige virksomheter tar i bruk KI og hvordan dette oppleves av innbyggerne er derfor avgjørende for om løsningene får bred aksept og faktisk kan tas i bruk i praksis.

Innbyggerperspektivet gir innsikt i hvor det er støtte og skepsis til bruk av KI, hvilke bruksområder som oppleves som akseptable, og hvilke hensyn som er viktige for å bevare tillit til offentlige tjenester. Dette perspektivet er sentralt for å forstå handlingsrommet for videre KI-bruk i offentlig sektor, og understreker behovet for demokratisk dialog rundt temaet.

## Motstand mot KI i beslutninger som angår dem selv

Innbyggerne er i liten grad komfortable med at KI brukes til å fatte beslutninger om dem, hvor 39 prosent er uenig eller helt uenige. Dette illustrerer en tydelig spenning mellom effektivisering og forventningen om menneskelig skjønn. Skepsisen er enda sterkere når det gjelder bruk av egne data. Andelen som er positive til at persondata brukes til å utvikle KI-tjenester har i snitt sunket 10 prosentpoeng på ett år.

Samlet sett i 2026 er innbyggerne altså mer positive til bruk av deres data til å forbedre KI-tjenester og gjøre

dem mer effektive enn til at KI skal brukes til å fatte beslutninger om en selv.

## Skepsis blant de unge

Blant de unge, som i større grad vil være påvirket av KI-bruk i offentlig sektor på sikt, ser vi at det er en urovekkende skepsis til at offentlige tjenester bruker KI som støtte til å fatte beslutninger om dem. Blant de som er mellom 16 og 24 finner vi at halvparten er enten uenig eller helt uenig i denne bruken av KI i offentlige virksomheter. Dette er 9 til 12 prosentpoeng høyere enn blant de andre aldersgruppene.

Funnet gjelder ikke bare for bruk av KI som støtte til å fatte beslutninger, men også på spørsmål om bruk av deres data for å forbedre KI-tjenestene. Halvparten av de unge er uenig eller helt uenig i at offentlige myndigheter kan bruke deres data for å utvikle og forbedre KI-tjenester.

## Et tillitsgap som krever aktiv håndtering

Funnene peker på en utfordring offentlig sektor må ta på alvor. At skepsisen øker samtidig som bruken vokser, er også et tydelig signal.

Tillit krever åpenhet om hvordan og hvorfor KI brukes, tydelighet i forhold til hva teknologien gjør og hva mennesker avgjør, reell involvering og medvirkning, muligheter for innsyn og en offentlig sektor som tar bevisste valg om når KI skal brukes og ikke brukes, for å nevne noe. Dette må skje fra starten av, og ikke som ettertanke.

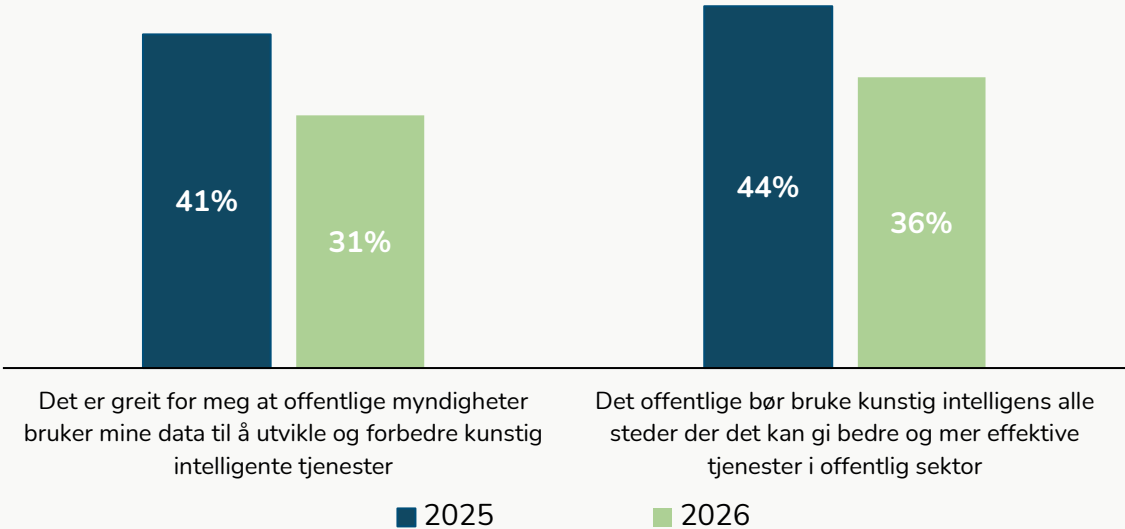
Andel av innbyggere som er uenig eller helt uenig i at



Det er greit at offentlig sektor benytter KI som støtte til å fatte beslutninger om meg

39%

Andelen som svarer at de er **enig eller helt enig** i følgende påstander



Spørsmålet «det offentlige bør bruke kunstig intelligens alle steder der det kan gi bedre og mer effektive tjenester i offentlig sektor» ble i 2025 stilt som «Bruk av kunstig intelligens er et riktig grep for å sikre bedre og mer effektive tjenester i offentlig sektor».

<sup>4</sup>: OECD. (2024). *OECD Survey on Drivers of Trust in Public Institutions 2024 Results: Country note—Norway*. [https://www.oecd.org/en/publications/oecd-survey-on-drivers-of-trust-in-public-institutions-2024-results-country-notes\\_a8004759-en/norway\\_d9a67b9b-en.html](https://www.oecd.org/en/publications/oecd-survey-on-drivers-of-trust-in-public-institutions-2024-results-country-notes_a8004759-en/norway_d9a67b9b-en.html)

<sup>5</sup>: Broomfield, H. (2025). *The data-driven public sector: A critical assessment of its framing and implementation* [Doktoravhandling, Universitetet i Oslo].

# Tillit er viktig av flere grunner

**Funnene viser at offentlig sektors handlingsrom for å bruke KI ikke avgjøres av teknologi og regelverk alene. Når innbyggerne blir mer skeptiske til bruk av egne data og KI-baserte beslutninger, blir tillit avgjørende for legitimitet, aksept og offentlig verdi.**

Debatten om kunstig intelligens har så langt i stor grad handlet om juss, teknologi og effektivisering. Men etter hvert som teknologien tas i bruk i stadig flere tjenester og beslutningsprosesser, blir et annet spørsmål minst like viktig: Hvorfor skal vi bruke KI, og på hvilke områder ønsker vi egentlig at teknologien skal få innflytelse?

Våre tall viser at befolkningen blir mer skeptisk til bruk av KI. Samtidig viser internasjonale undersøkelser som OECDs Trust Survey at vi fortsatt har høy sosial og institusjonell tillit i Norge.<sup>4</sup> Dette er et godt utgangspunkt, men tilliten kan ikke tas for gitt, og våre tall peker på et viktig skille: Selv om mange har høy tillit til offentlige institusjoner generelt, er ikke denne tilliten automatisk overførbart til digitale løsninger eller bruk av KI. Særlig spørsmål knyttet til personvern, automatiserte beslutninger og bruk av data skaper usikkerhet. Dette gjør tillit og legitimitet til et strategisk spørsmål for videre bruk av KI i offentlig sektor, og ikke kun et juridisk/teknisk spørsmål.

Diskusjonen om KI må derfor handle om mer enn hva som er mulig eller lovlig. Den må også handle om hvilke samfunns mål teknologien skal bidra til, hvilke avveininger vi må gjøre, og hvordan offentlig sektor kan bruke KI på en måte som både er og oppleves som trygg, forståelig og legitim. I sin doktoravhandling peker Heather Broomfield blant annet på at en datadreven forvaltning også stiller demokratiske spørsmål.<sup>5</sup> Når teknologi får større betydning for beslutninger som påvirker innbyggernes liv, øker behovet for åpenhet, ansvarlighet og involvering. Utover å fungere teknisk, må løsningene også ha tillit hos både ansatte og innbyggere.

Dette blir særlig tydelig i møte med konkrete eksempler som allerede preger den offentlige samtalen om KI. Debatten om bruk av KI i forbindelse med skolenedleggelse i Tromsø har vist hvordan teknologi raskt kan bli knyttet til spørsmål om politisk ansvar og legitimitet, og i DFDs rapport om KI i statlige virksomheter, trakk ansatte frem amerikanske teknologiselskapers rolle som teknologileverandør i Israels krigføring i Gaza, samtidig som de er en leverandør av viktige arbeidsverktøy her i Norge. Samtidig har diskusjoner om innsyn i prompts og KI-systemers beslutningsgrunnlag synliggjort nye spørsmål om transparens og etterprøvnbarhet i forvaltningen.

Slike saker påvirker ikke bare hvordan teknologien vurderes, men også hvordan ansatte og innbyggere oppfatter offentlig sektors bruk av KI. Mange ansatte etterspør derfor tydeligere svar på formålet med KI-bruken: Hva er problemet som skal løses? Hvilken verdi skal teknologien skape? Og hvilke hensyn skal veie tyngst når effektivisering må balanseres mot personvern, rettsikkerhet og demokratisk kontroll?

For å bygge og opprettholde tillit må offentlig sektor kombinere teknologisk utvikling med tydelig styring, åpenhet og dialog. Vi må forstå hvorfor KI brukes, hvordan beslutninger tas, og hvilke mekanismer som sikrer kontroll og ansvarlighet.

Samtidig må de organisatoriske og tekniske utfordringene som *IT i praksis* identifiserer fortsatt løses. Men dersom offentlig sektor skal lykkes med KI over tid, er ikke teknisk implementering alene tilstrekkelig. Teknologien må også oppleves som legitim, ansvarlig og samfunnsmessig forankret. Først da kan KI bidra til reell offentlig verdi.

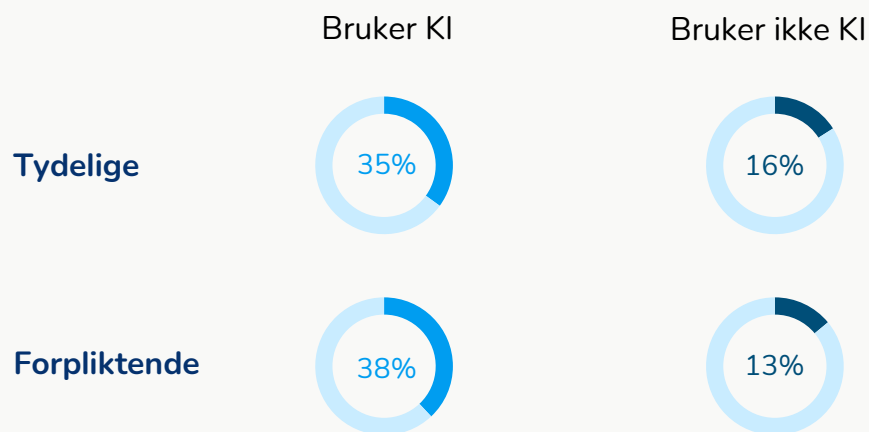


# Veiledningsbehov og opplevd støtte

Funnene viser at det er tydelig at mange virksomheter har et betydelig behov for veiledning. Behovet gjelder både for å komme i gang med KI i praksis og for å håndtere utfordringer som oppstår når bruken skal videreutvikles og forankres over tid. I dette kapitlet undersøker vi hvilke støttebehov virksomhetene selv peker på, hvordan de opplever dagens veiledning og støtte, og hvordan de ønsker at framtidig veiledning skal utformes og formidles.

**15 %** av offentlige virksomheter oppgir at de i stor eller svært stor grad får god støtte fra nasjonale myndigheter (for eksempel veiledning, rådgivning, støtteordninger) innen kunstig intelligens.

Virksomheter som **i stor eller svært stor grad** opplever styringssignalene innen kunstig intelligens som



«Bruker KI» og «bruker ikke KI» er en indeks basert på flere av KI-spørsmålene i undersøkelsen, og viser om en virksomhet bruker KI over eller under gjennomsnittet av KI-bruk på tvers av virksomhetene.

Ramboll

## Et kritisk gap: Opplevd nasjonal støtte innen kunstig intelligens er lav

Norge har høye mål for KI i offentlig sektor, men ambisjonene alene sikrer ikke trygg og ansvarlig bruk. Funnene viser at mange virksomheter verken opplever styringssignalene som tydelige og forpliktende, eller får nok støtte til å omsette ambisjonene i praksis.

### Nasjonale styringssignaler når ikke frem

Til tross for høye politiske ambisjoner, opplever et klart flertall av offentlige virksomheter at de nasjonale styringssignalene innen KI verken er tydelige eller forpliktende. Bare drøyt en tredjedel av virksomhetene som bruker KI opplever signalene som klare. Blant dem som ikke bruker KI er andelen enda lavere. Det er liten forskjell mellom stat og kommune, og heller ikke mellom virksomheter som realiserer gevinster og de som ikke gjør det.

Mest bekymringsfullt er det at virksomhetene som ennå ikke har tatt i bruk KI, og som derfor har størst behov for tydelig retning utenfra, også er de som i minst grad opplever at styringssignalene er forpliktende for dem. Det kan være med på å forklare hvorfor en betydelig andel fortsatt står på sidelinjen. I tillegg er tilfredsheten med styringssignalene enda lavere blant virksomheter som opplever mange og sterke barrierer. Dette peker på en klar sammenheng: uklare signaler fra nasjonale myndigheter gjør det vanskeligere å navigere, og barrierene vokser som følge.

### Støtten fra nasjonale myndigheter oppleves som fraværende

Bildet forsterkes når virksomhetene vurderer den konkrete støtten de mottar fra nasjonale myndigheter innen området KI. Bare 15 prosent oppgir at de i stor eller svært stor grad får god støtte fra nasjonale myndigheter, i form av veiledning, rådgivning eller støtteordninger. Det betyr at åtte av ti virksomheter i realiteten navigerer på egenhånd i et landskap som er både teknologisk komplekst og regulatorisk uavklart.

Blant statlige virksomheter er det de små som i størst grad opplever at de får god støtte. På en skala fra 1 til 5 er gjennomsnittet 2,5 for små virksomheter, mot 2,2 for de store. Det er et tankekors, fordi det ofte er de store virksomhetene som har størst mulighet til å hente ut de store gevinstene ved mer omfattende bruk av KI. Når de samtidig opplever mindre støtte, kan det bremse utviklingen der potensialet er størst.

### Et gap med konsekvenser for trygg og ansvarlig bruk

Dette er ikke bare et spørsmål om tempo og dekningsgrad, men et spørsmål om modenheten på den KI-bruken som faktisk skjer. Når styringssignalene er uklare og støtten er begrenset, øker risikoen for at KI tas i bruk på måter som ikke er tilstrekkelig utredet, etisk forankret eller juridisk avklart. Trygg og ansvarlig bruk forutsetter at virksomhetene vet hva de kan gjøre, hva de ikke bør gjøre, og hvordan de skal håndtere dilemmaene som oppstår. Denne kunnskapen kan ikke forventes å vokse frem i hver enkelt virksomhet, men må tilrettelegges, kommuniseres og forankres nasjonalt. Så lenge flertallet opplever at denne støtten mangler, er risikoen stor for at utviklingen går raskere enn ansvarligheten.

Det er heller ikke bare et spørsmål om at støtten uteblir. Det er et spørsmål om hva fraværet av nasjonal støtte faktisk koster. Dersom virksomhetene ikke er trygge på KI-bruk, vil heller ikke bruken bli moden, og man vil ikke kunne hente ut de store gevinstene av en gjennomgripende bruk.

# Veiledning fra KI Norge: hvor er behovene?

Virksomheter fra både offentlig og privat sektor er spurt om hva slags veiledning på KI de har behov for og hvordan de ønsker at veiledning skal leveres. Svarene viser et bredt spekter av preferanser, men tegner samtidig et bilde av hva som etterspørres mest og hvor behovene skiller seg mellom ulike virksomhetstyper.

## Regulatorisk trygghet er viktigst for virksomhetene

En stor andel av virksomhetene ønsker veiledning på regulatorisk og juridisk tema - etterspurt av hele 71 prosent av kommunene og 74 prosent av statlige virksomheter. Rundt 20 prosent av private virksomheter ønsker også dette. Funnet henger direkte sammen med at usikkerhet om risiko er den raskest voksende barrieren i sektoren. Virksomhetene vil bruke KI, men de trenger klarhet i hva de faktisk har lov til, og hvilke risikoer de må håndtere. Uten denne tryggheten stopper mange opp.

## Behov for veiledning i bruk av data

Etter veiledning på regulatorisk og juridisk tema, ønsker 52 prosent av statlige virksomheter og 66 prosent av kommunene å få veiledning i tilrettelegging og bruk av data for KI-løsninger. Dette funnet peker tilbake på hvordan virksomhetene er på vei til å bli modne brukere av KI, og går fra enkelt tekstarbeid og over til mer integrert bruk av egne data i KI-løsninger.

## Offentlige virksomheter vil ha lavterskel veiledning

Blant offentlige virksomheter er det veiledere og sjekklister, webinarer og informasjonsmøter, og erfaringsdeling og nettverk som dominerer. Dette er lavterskel og praktisk orientert veiledning som gir mulighet for læring på tvers av virksomheter. Fire av ti ønsker veiledning som en regulatorisk sandkasse eller maler og dokumentasjonsstøtte.

Forskjellene mellom stat og kommune er små, men på to punkter skiller de seg tydelig. Kommunene etterspør webinarer og informasjonsmøter i større grad enn staten, henholdsvis 78 mot 61 prosent. Når det gjelder

maler og dokumentasjonsstøtte, er andelen blant kommunene nær dobbelt så høy som blant statlige virksomheter, 49 mot 27 prosent. En mulig forklaring på dette kan være at kommunene i større grad har behov for ferdig tilrettelagt støtte de kan ta i bruk direkte, fordi de har færre interne ressurser enn statlige virksomheter.

## Private virksomheter er mer tilbakeholdne

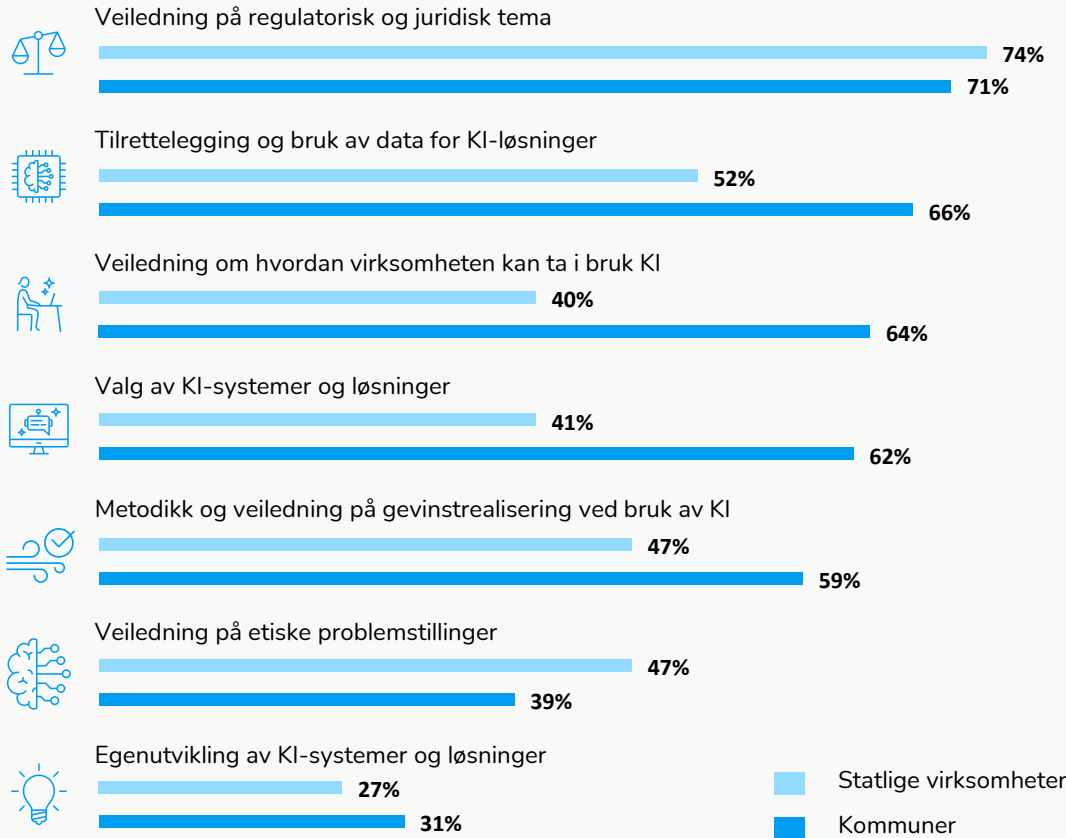
Blant små og mellomstore private bedrifter er andelen som etterspør veiledning gjennomgående lavere enn i offentlig sektor. Webinarer og informasjonsmøter er det mest etterspurte formatet, og det er færrest som etterspør maler og dokumentasjonsstøtte.

Forskjellene mellom små og mellomstore bedrifter er ikke dramatiske. Likevel er det dobbelt så mange mellomstore som små bedrifter som ønsker veiledning i en regulatorisk sandkasse, og noen flere mellomstore bedrifter som ønsker maler og dokumentasjonsstøtte og erfaringsdeling. Små bedrifter på sin side etterspør i noe større grad veiledere, sjekklister og webinarer, de mest tilgjengelige og lavterskelpregede formatene.

## Store behov og konkrete veiledningsformer

Funnene viser at behovene er store, men også ganske tydelige. Virksomhetene etterspør først og fremst støtte som gjør det tryggere og enklere å ta KI i bruk i praksis, særlig på regulatoriske spørsmål og bruk av data, og de ønsker konkrete lavterskeltilbud. Dataene peker også på at særlig kommuner ønsker konkret veiledning i bruk og valg av KI-løsninger. Behovene varierer mellom sektorer og virksomhetstyper, noe som understreker at veiledningen må være både relevant, praktisk og tilpasset de ulike forutsetningene for både offentlige og private virksomheter.

Hvilken **type veiledning** på KI er viktigst for virksomheten akkurat nå? (Flere svar mulig)



7 av 10 virksomheter ønsker at veiledningen på KI skal leveres i form av **veiledere og sjekklister, webinarer og informasjonsmøter og erfaringsdeling og nettverk.**

4 av 10 virksomheter ønsker at veiledningen på KI skal leveres som en **regulatorisk sandkasse og som maler og dokumentasjonsstøtte.**



# Veien videre: Refleksjoner fra KI Norge

Funnene fra *IT i praksis* viser at Norge er godt i gang med KI, men at potensialet er langt fra realisert. Utfordringene med usikkerhet, manglende støtte og synkende tillit kan ikke løses av virksomhetene alene. I dette kapittelet løfter vi blikket fra status til handling, og deler KI Norges refleksjoner om hva som skal til for å lykkes med innovativ og ansvarlig bruk av KI. Veien videre handler om å bygge tillit, sette tydeligere retning og gi bedre støtte, og om å ta fatt i de vanskelige spørsmålene i fellesskap.

# Refleksjoner fra KI Norge: En balansekunst

KI Norge vil bidra til å finne og holde balansen mellom innovativ og ansvarlig bruk av kunstig intelligens. Veiledning, kompetansebygging og erfaringsutveksling skal stimulere til både innovasjon og ansvarlighet på KI-området. Eksempler på innsatsfaktorer for å stimulere innovativ KI er tilgang til regnekraft, bedre datadeling og finansiering. KI-forordningen og bruk av den regulatoriske sandkassen er eksempler på viktige rammer for å sikre ansvarlig KI-bruk. Samtidig handler ansvarlig bruk også om andre hensyn, som miljø, digital suverenitet, arbeidsliv og innbyggernes tillit. For å lykkes må vi lytte til og involvere hele samfunnet. Gjennom behovskartlegging og innspill fra offentlig sektor, næringsliv, academia og innbyggerne vil KI Norge legge ulike perspektiver i vektskålene og fylle dem med konkrete tiltak for Norges langsiktige KI-utvikling.

## Retning og støtte

Funnene i *IT i praksis* viser at potensialet i KI ikke realiseres fullt ut og at en stor andel etterspør tydeligere retning. Usikkerhet og umoden bruk gjør at gevinster ofte tas ut på individnivå, ikke på organisasjonsnivå. Først når usikkerheten reduseres og vi får til transformasjon på virksomhets- og samfunnsnivå, kan potensialet realiseres. Dette krever at vi anerkjenner kompleksiteten, håndterer vanskelige dilemmaer og etablerer en felles forståelse for hvor vi vil og hvor langt vi skal gå. KI Norge vil bidra til dette gjennom å gi mer støtte og tydeligere retning, på både kort og lang sikt.



## Tillit

Tillit er en grunnleggende forutsetning for bruk av KI. Årets *IT i praksis* viser en økende skepsis til KI i offentlig sektor, særlig blant unge. Internasjonale undersøkelser, blant annet fra Stanford, viser samme trend i andre land. Dette er bekymrende. Norge er et av verdens mest tillitsbaserte samfunn. KI Norge vil, på tvers av sektorene og sammen med innbyggerne, jobbe for at KI anvendes i Norge på måter som understøtter denne tilliten, heller enn å svekke den.



## Samarbeid og inkludering

KI Norge skal bidra til å bygge tillit, sette retning og gi støtte gjennom å koble offentlig og privat sektor, sivilsamfunn og academia tettere sammen, og skape arenaer der behov, erfaringer og bekymringer deles tidlig. Inkludering handler også om at innbyggerne får reell mulighet til å forstå, påvirke og delta i utviklingen. KI Norge vil derfor legge til rette for bred medvirkning, felles læring og konkrete samarbeid som gjør at KI tas i bruk på en måte som skaper verdi for hele samfunnet.





# Fra KI til digital beredskap

Temarapporten om KI viser at virksomhetene vil ta KI videre, men at usikkerhet om risiko er den raskest voksende barrieren. Samtidig blir innbyggerne mer tilbakeholdne med at dataene deres brukes til å utvikle KI.

Trygg bruk av KI forutsetter derfor at data og systemer er godt beskyttet. KI endrer også trusselbildet, fordi angrep kan gjennomføres raskere og enklere. Temarapporten om sikkerhet og beredskap undersøker om sikkerhetsarbeidet i offentlig sektor virker i praksis, og om virksomhetene er forberedt på det som kommer.

**Trygg KI krever sikkerhet som virker i praksis.**

Temarapport 2:2026

# Sikkerhet og beredskap

Er vi forberedt på det som kommer?



# Oppsummering

Apparatet er bygget. Nesten ni av ti offentlige virksomheter har en dedikert rolle for informasjonssikkerhet og personvern, og tre av fire gjennomfører regelmessige risikovurderinger. De fleste oppgir også å ha god oversikt over egne informasjonsverdier og systemer. Likevel er det stor avstand mellom å ha et sikkerhetsapparat og å få det til å fungere når det gjelder.

Årets undersøkelse viser en offentlig sektor som har kommet lenger med strukturer og prosedyrer, enn med ledelsesforankring, kompetanse og daglig etterlevelse. 78 prosent oppgir å ha god oversikt over informasjonssikkerheten, mens 57 prosent mener ledelsen gir tydelige føringer, og 46 prosent oppgir at ansatte forstår, etterlever og tar ansvar for informasjonssikkerheten i det daglige arbeidet. Det samme mønsteret går igjen når det gjelder cybersikkerhet: 76 prosent har klare prosedyrer for å håndtere angrep, mens kun 42 prosent øver regelmessig, og 44 prosent opplever kompetansen som tilstrekkelig. Jo nærmere spørsmålene kommer en faktisk hendelse, desto svakere blir resultatene.

Samtidig har framgangen stoppet opp. Opplevd kompetanse og ressurser steg fra 37 prosent i 2021 til 65 prosent i 2025, men faller til 60 prosent i år. Opplevd sikkerhetsoversikt har falt fra 87 prosent i 2023 til 78 prosent i 2026. At begge seriene nå peker nedover, kan skyldes at virksomhetene vurderer seg selv mot en strengere målestokk etter at digitalsikkerhetsloven trådte i kraft. Det kan være uttrykk for større realisme, men også et varsel om at avstanden til et forsvarlig nivå er større enn tidligere antatt. Nasjonal sikkerhetsmyndighet (NSM) viser dessuten til anslag om at Norge vil mangle 4 000 personer med cybersikkerhetskompetanse i 2030. Utfordringen er derfor ikke bare å møte skjerpede krav, men å sikre kompetansen og kapasiteten som trengs for å omsette kravene i praksis.

Virksomhetene mangler ikke retning. 76 prosent opplever styringssignalene innen informasjonssikkerhet som tydelige og 80 prosent som forpliktende. Samtidig opplever bare omtrent halvparten god støtte fra nasjonale myndigheter. Behovet er derfor ikke først og fremst flere signaler, men mer konkret og tilpasset hjelp til gjennomføring. Forutsetningene varierer: Kommuner og fylkeskommuner ligger lavere enn staten på dokumentert etterlevelse av personvernreglene, 52 mot 82 prosent, og cybersikkerhetskompetanse, 39 mot 56 prosent. Samtidig opplever staten svakere støtte fra nasjonale myndigheter enn kommunesektoren, 44 mot 54 prosent innen informasjonssikkerhet, med samme mønster innen personvern og cybersikkerhet. Resultatene viser dermed ulike utfordringer i sektorene og understreker behovet for støtte som er tilpasset virksomhetenes forutsetninger.

Innbyggernes vurderinger speiler flere av svakhetene virksomhetene selv rapporterer. Tilliten til at offentlige digitale løsninger ivaretar personopplysninger, ligger stabilt rundt 51 prosent, men bare 4 prosent er helt enig i at det offentlige er godt beskyttet mot cyberangrep. Hele 18 prosent er helt uenige. Innbyggerne er positive til datadeling når nytten er tydelig, men opplever langt mindre innsikt i og kontroll over hvordan opplysningene brukes. Når data deles mer og tas i bruk i KI-løsninger, blir åpenhet om datagrunnlag, vurderinger og menneskelig ansvar enda viktigere.

Kunstig intelligens bidrar samtidig til å endre trusselbildet. Angrep kan gjennomføres raskere, mer målrettet og i større skala enn tidligere. Det øker betydningen av de områdene hvor virksomhetene allerede scorer lavest: kompetanse, øvelser og evnen til å omsette planverk til handling.

Det neste steget er derfor å få de etablerte strukturene til å virke bedre. Sikkerhetsarbeidet må forankres tydeligere i ledelsen, beredskapen må øves og etterleves, og støtten må bli mer konkret. Samtidig kan KI gjøre angrep raskere og enklere å gjennomføre, mens bruk av KI i offentlige beslutninger øker behovet for innsyn og etterprøvbarehet. Videre framgang må komme i praksislaget: i kompetansen, den øvde responsen, gjennomføringsevnen og tilliten som følger når sikkerhetstiltakene faktisk virker.



# Totalforsvarsåret 2026

Totalforsvarsåret 2026 skal styrke Norges evne til å forebygge og håndtere sikkerhetspolitiske kriser og krig. Denne temarapporten undersøker en avgjørende del av denne evnen, nemlig om offentlig sektors digitale sikkerhetsarbeid fungerer i praksis når samfunnet settes under press.

## Fra planverk til øvd samvirke

Totalforsvarsåret 2026 er det første i sitt slag. Direktoratet for samfunnssikkerhet og beredskap (DSB) og Forsvaret leder arbeidet, som samler sivile myndigheter, Forsvaret, næringslivet, frivilligheten og befolkningen om tverrsektorielle aktiviteter og øvelser.

*Cold Response*, *Øvelse Totalforsvar 2026* og *Norge øver* skal blant annet teste planverk, rolleforståelse, beslutninger og samhandling. Målet er å beskytte befolkningen, opprettholde kritiske samfunnsfunksjoner og styrke den sivile støtten til Forsvaret og allierte. Oppmerksomheten flyttes dermed fra om planene finnes, til om de kan brukes.

## Kravene og forventningene er skjerpet

Digitalsikkerhetsloven trådte i kraft 1. oktober 2025 og skjerper kravene til blant annet styringssystemer, risikovurderinger, beredskap og hendelseshåndtering. Virksomhetene vurderer seg derfor både mot en strengere målestokk og et mer krevende sikkerhetspolitisk bakteppe.

Dette gjør temarapportens funn særlig relevante. Totalforsvaret er avhengig av at digitale tjenester, kommunikasjonsløsninger og styringssystemer tåler press. Når resultatene er svakere for ledelsesforankring, kompetanse, øvelser og daglig etterlevelse enn for formelle strukturer, peker de på områdene Totalforsvarsåret er ment å teste og styrke.

## Fire begreper som brukes gjennomgående

**Informasjonssikkerhet** er det bredeste av begrepene, og handler om å beskytte all informasjon, uavhengig av form, mot uautorisert tilgang, endring eller tap.

**Cybersikkerhet** er en delmengde av informasjonssikkerhet, rettet mot beskyttelse av digitale systemer, nettverk og data mot angrep og uønsket aktivitet i det digitale domenet.

**Personvern** handler om den enkeltes rett til kontroll over egne opplysninger, og stiller krav til hvordan virksomheter samler inn, lagrer og behandler data.

**Risikostyring** er prosessen som hjelper virksomheter å forstå hva de har å beskytte, hvilke trusler de står overfor, og hvilke tiltak som gir best effekt.

## Nøkkeltall

- 89 prosent har en dedikert rolle for informasjonssikkerhet og personvern. Apparatet er på plass.
- 46 prosent mener ansatte forstår, etterlever og tar ansvar for informasjonssikkerhet i det daglige arbeidet.
- 42 prosent øver regelmessig på å håndtere cyberangrep, mot 76 prosent som har prosedyrene på plass.
- 60 prosent opplever tilstrekkelig kompetanse og ressurser innen informasjonssikkerhet, ned fra 65 prosent i 2025.
- 51 prosent opplever god støtte fra nasjonale myndigheter innen informasjonssikkerhet.
- 52 prosent av kommunene sikrer at personvernreglene følges fullt ut, mot 82 prosent i staten.
- 4 prosent av innbyggerne er helt enig i at det offentlige er godt beskyttet mot cyberangrep. 18 prosent er helt uenige.

**Rambøll, TEK Norge, KS, NTNU og Digitaliseringsdirektoratet**

A photograph of a male technician in a server room. He is wearing a yellow hard hat, a yellow safety vest over a plaid shirt, and is holding a tablet. He is looking at the tablet. In the background, there are several black server racks with various cables (blue, orange, green) plugged into them. The scene is dimly lit, with some lights from the server equipment visible.

# Fire hovedfunn om sikkerhet og beredskap

Resultatene peker på fire hovedfunn som til sammen beskriver avstanden mellom det formelle sikkerhetsarbeidet og den praksisen som faktisk beskytter. I dette kapittelet ser vi på hva virksomhetene har etablert, hva de får gjennomført, hvordan utviklingen har snudd, og hvordan innbyggerne vurderer beredskapen. Utfordringene er ikke uavhengige av hverandre, men forsterker hverandre.

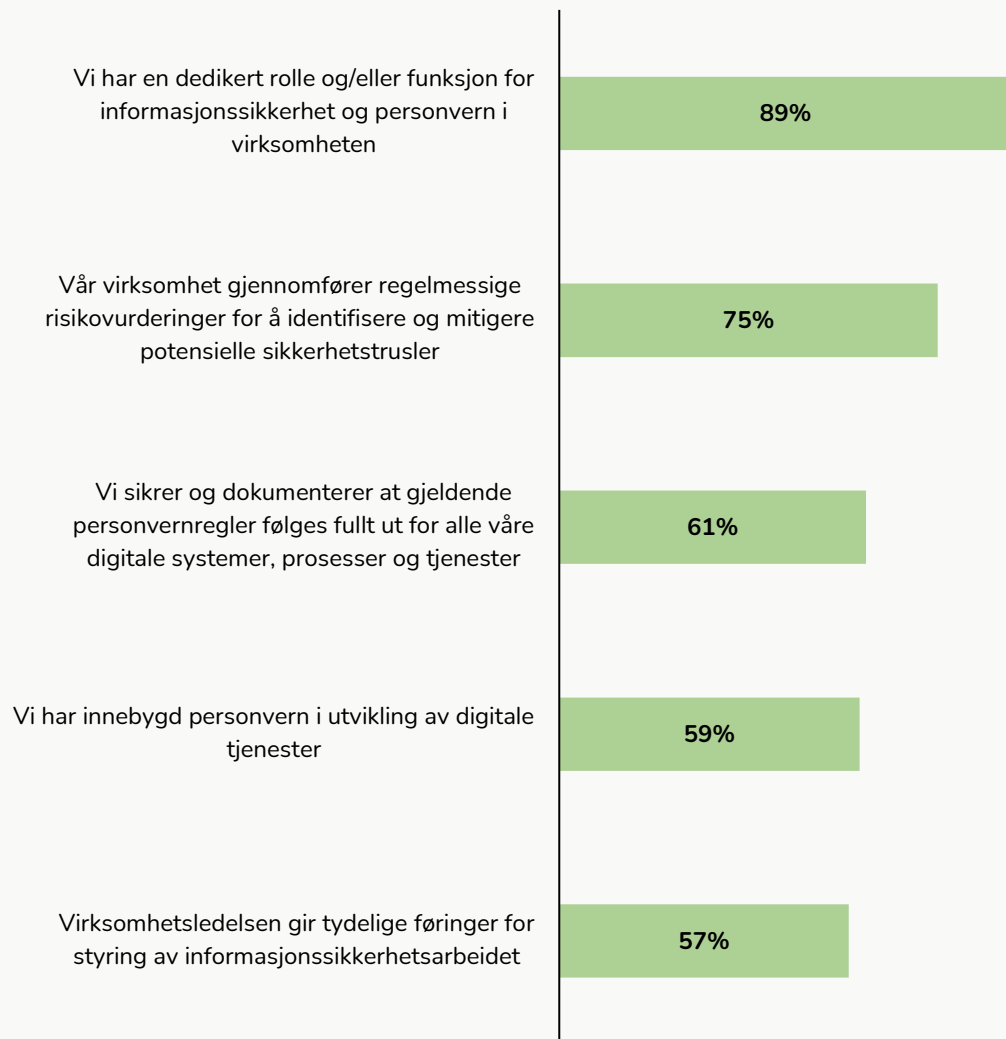


# Sikkerhetsarbeidet er i stor grad etablert

Offentlig sektor har de siste årene bygget opp rollene, rutinene og styringsstrukturene som kreves for et systematisk sikkerhetsarbeid. De fleste virksomheter har dedikerte sikkerhetsfunksjoner, gjennomfører risikovurderinger og oppgir god oversikt over egne verdier og systemer. Samtidig viser resultatene en liten tilbakegang i oversikt og tilstrekkelig kompetanse og ressurser, og at forskjellene blir tydeligere når kravene til styring, integrering og gjennomføring øker.



Andelen som svarer at de er **enig** eller **helt enig** i følgende påstander:



# Sikkerhetsarbeidet i offentlig sektor er i stor grad etablert

Offentlige virksomheter har i stor grad etablert de grunnleggende strukturene for informasjonssikkerhet og personvern. De fleste har dedikerte roller, gjennomfører risikovurderinger og arbeider systematisk med sikkerhet. Resultatene tyder likevel på at offentlig sektor har kommet lenger i etableringen av sikkerhetsarbeidet enn i den videre praktiseringen av det.

## Rollene og rutinene er på plass

Offentlig sektor har i stor grad etablert de organisatoriske forutsetningene for systematisk sikkerhetsarbeid. Nesten alle virksomhetene oppgir at de har dedikerte roller eller funksjoner for informasjonssikkerhet og personvern, og tre av fire virksomheter oppgir at de gjennomfører regelmessige risikovurderinger for å identifisere og mitigere potensielle trusler. De fleste har også rutiner for sikring og dokumentering av personvern, og har personvern innebygd i sine digitale tjenester. Dette peker på at virksomhetene har et godt organisatorisk utgangspunkt for å håndtere informasjonssikkerhet, personvern og stadig mer omfattende regulatoriske krav.

## Styringen er mindre etablert enn strukturene

Etablerte roller og god oversikt er viktige forutsetninger for sikkerhetsarbeidet, men er ikke tilstrekkelige i seg selv. Bare 57 prosent oppgir at ledelsen gir tydelige føringer for styringen av informasjonssikkerhetsarbeidet. Selv om de fleste virksomhetene har etablert organisatoriske strukturer og dedikerte sikkerhetsfunksjoner, er det betydelig færre som opplever at sikkerhetsarbeidet er tydelig forankret i den overordnede virksomhetsstyringen.

Mønsteret peker på en gradvis reduksjon fra etablering av strukturer til aktiv styring. Mens nær ni av ti virksomheter har dedikerte roller for informasjonssikkerhet og personvern, opplever langt færre at ledelsen gir tydelige føringer for arbeidet. Dette

kan indikere at offentlig sektor har kommet lenger i etableringen av sikkerhetsarbeidet enn i den strategiske styringen og videreutviklingen av det.

## Forskjellen blir tydeligere jo høyere kravene er

Funnene peker på at tiltak med lavere krav, som å utpeke dedikerte personer eller gjennomføre risikovurderinger, i større grad er gjennomført, mens tiltak som krever mer samhandling og organisering på tvers og med andre tjenester henger noe etter. Mønsteret peker på at offentlig sektor generelt har kommet lenger i etableringen av sikkerhetsarbeidet enn i arbeidet med å integrere sikkerhet i styring, utvikling og tjenesteleveranse.

## Personvern viser hvor krevende gjennomføringen er

Personvern illustrerer forskjellen mellom etablerte strukturer og mer krevende gjennomføring. 82 prosent av statlige virksomheter oppgir at de sikrer og dokumenterer etterlevelse av personvernregelverket for alle digitale systemer, prosesser og tjenester. Blant kommuner og fylkeskommuner er andelen 52 prosent. Dette peker på ulike forutsetninger for å håndtere stadig mer komplekse krav, hvor statlige virksomheter kan virke til å være bedre rustet for å tilpasse seg nye og komplekse krav enn kommuner og fylkeskommuner.

Selv om grunnstrukturen i stor grad er etablert både i stat og kommune, varierer evnen til å integrere kravene i virksomhetsstyringen og den løpende utviklingen av tjenester.

# Utviklingen peker i en ny retning

Gjennom flere år har offentlige virksomheter rapportert økt kompetanse og bedre forutsetninger for sikkerhetsarbeidet. I år endrer bildet seg. Opplevd kompetanse faller for første gang siden målingene startet, samtidig som opplevd oversikt fortsetter nedover. Kommunesektoren rapporterer lavere nivåer enn staten, særlig når det gjelder kompetanse og ressurser.

## Fem år med jevn framgang

Kompetanse og ressurser innen informasjonssikkerhet har vært blant de områdene som har vist sterkest utvikling i IT i praksis. Andelen virksomheter som oppgir at de har tilstrekkelig kompetanse og ressurser økte fra 37 prosent i 2021 til 65 prosent i 2025. Det tilsvarer en vekst på 28 prosentpoeng over fire år, og framgangen kom gradvis gjennom hele perioden. I 2026 faller kompetansekurven for første gang, med 5 prosentpoeng ned til 60 prosent.

## Oversikten toppet tidligere

Oversikt over informasjonssikkerhet fulgte et annet forløp enn kompetanseutviklingen. Andelen virksomheter som oppgir at de har god oversikt over verdikjeder, informasjonsverdier, utstyr og brukertilganger var høy allerede i 2021, og nådde en topp på 87 prosent i 2023. Siden 2023 har andelen falt hvert år, ned til 78 prosent i 2026.

## Staten ligger foran kommunene

Forskjellen mellom stat og kommune er tydeligst innen kompetanse og ressurser. 70 prosent av de statlige virksomhetene oppgir at de har tilstrekkelig kompetanse og ressurser, mot 56 prosent i kommunesektoren. For sikkerhetsoversikt er forskjellen mindre, med henholdsvis 83 og 76 prosent. Kompetanseutfordringen ser dermed ut til å være noe større i kommunene.

## Timing er verdt å merke seg

Fallet det siste året kan ses i sammenheng med digitalsikkerhetsloven som trådte i kraft 1. oktober 2025. Loven innebærer skjerpede krav til blant annet styringssystemer, risikovurderinger, beredskap og hendelseshåndtering.

En mulig forklaring er derfor at virksomhetene har en annen målestokk enn tidligere, og med det vurderer situasjonen annerledes fordi kravene er blitt mer omfattende.

Dersom dette er en del av forklaringen, er utviklingen ikke nødvendigvis et tegn på svekket sikkerhetsarbeid, men en utvikling mot en mer motstandsdyktig offentlig sektor. Samtidig innebærer det at avstanden mellom dagens situasjon og kravene virksomhetene forventes å oppfylle, kan være større enn tidligere målinger har gitt inntrykk av.

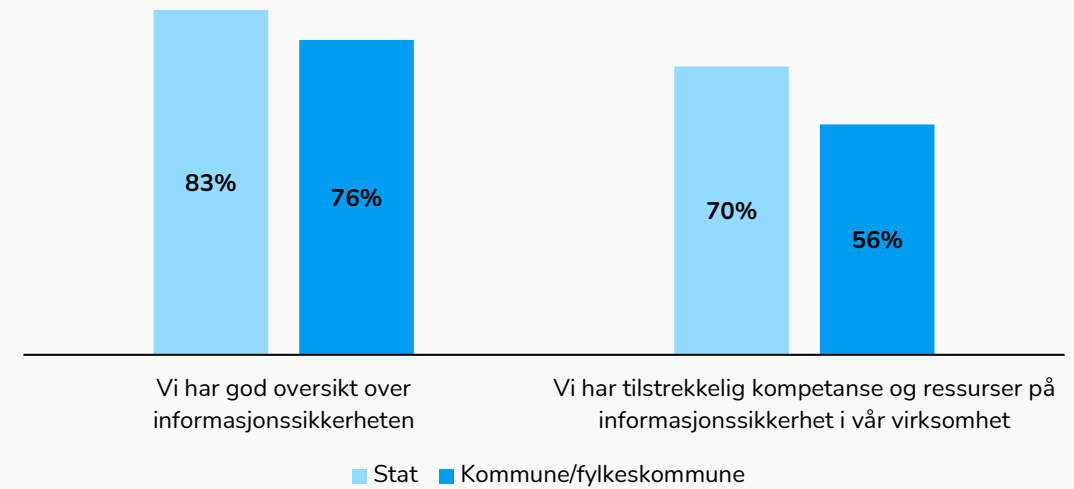
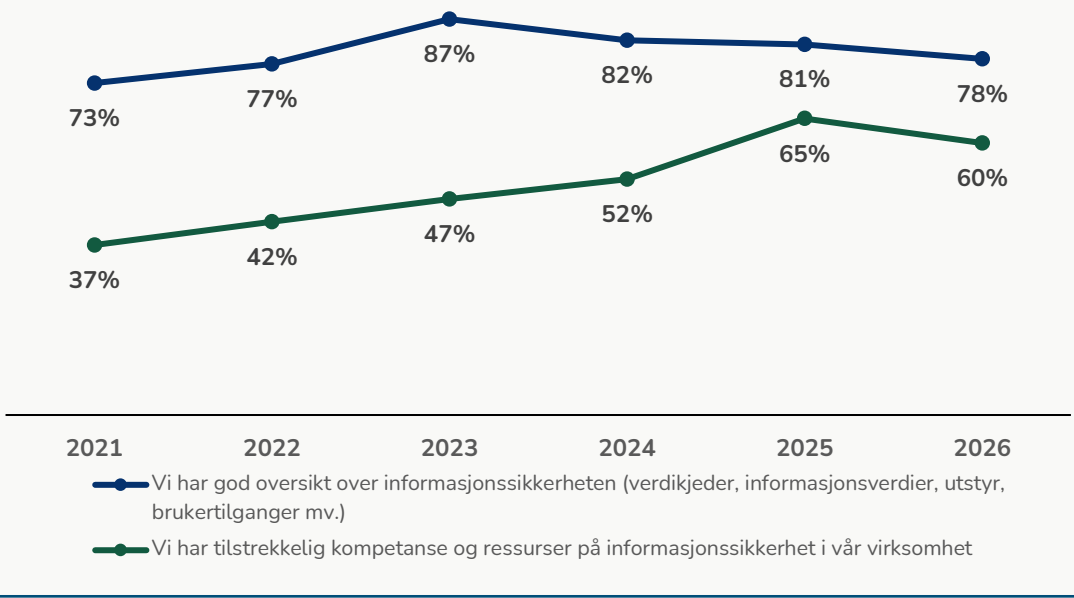
## Kompetansen blir vanskeligere å skaffe

Selv om deler av utviklingen kan forklares med skjerpede krav og økt bevissthet, betyr ikke det at kompetanseutfordringen er mindre reell. Tvert imot skjer fallet i opplevd kompetanse i et arbeidsmarked der tilgangen på sikkerhetskompetanse er under press. NSM viser til framskrivninger fra NIFU som anslår at Norge vil mangle 4 000 personer med cybersikkerhetskompetanse i 2030, og omtaler dette som en alvorlig sårbarhet for norsk sikkerhet.<sup>6</sup>

Det samme bildet tegnes internasjonalt. I ITUs Global Cybersecurity Index for 2024 ligger Norge under medianen for EU-landene på kapasitetsutvikling.<sup>7</sup> Indikatoren omfatter blant annet utdanning, opplæring, bevisstgjøring og forskning. Dette understøtter bildet av en langsiktig utfordring med å utvikle og opprettholde nødvendig cybersikkerhetskompetanse i Norge.

Kompetanse er dermed en utfordring virksomhetene i begrenset grad kan løse alene, og tallene tyder på at behovet er særlig stort i kommunesektoren. Selv virksomheter som har etablert gode styringsstrukturer og tydelige sikkerhetskrav, vil være avhengige av tilgang på kompetanse for å omsette planer, prosedyrer og styringssystemer til praktisk sikkerhetsarbeid.

Andelen som svarer at de er enig eller helt enig i følgende påstander:



<sup>6</sup>: Nasjonal sikkerhetsmyndighet. (2023). Sikkerhetsfaglig råd – Et motstandsdyktig Norge. <https://nsm.no/regelverk-og-hjelp/rapporter/sikkerhetsfaglig-rad-et-motstandsdyktig-norge>

<sup>7</sup>: International Telecommunication Union. (2024). Global Cybersecurity Index 2024 (5th ed.). <https://www.itu.int/hub/publication/d-hdb-gci-01-2024/>



# Planverk er ikke det samme som beredskap

Offentlig sektor har i stor grad etablert prosedyrer og planverk for håndtering av cyberangrep. Men beredskapen blir svakere jo nærmere vi kommer en faktisk hendelse. Færre har tilstrekkelig kompetanse, færre øver regelmessig, og under halvparten oppgir at ansatte etterlever sikkerhetskravene i det daglige arbeidet. Det er den operative kapasiteten, ikke planverket, som avgjør om virksomhetene klarer å håndtere et angrep når det oppstår.



# Fra planverk til beredskap

De fleste offentlige virksomheter har etablert prosedyrer for å håndtere cyberangrep. Resultatene blir imidlertid svakere jo nærmere vi kommer områdene som møter og håndterer en faktisk hendelse. Kompetanse, gjenopprettingsevne og regelmessige øvelser fremstår som de svakeste leddene i beredskapskjeden.

## Cybersikkerhet måles for første gang

Denne delen om cybersikkerhet omtaler virksomhetenes evne til å beskytte digitale systemer, nettverk og data mot angrep og uønsket aktivitet. Spørsmålene om cybersikkerhet er nye i *IT i praksis 2026*. Siden spørsmålene inngår for første gang, gir resultatene først og fremst et situasjonsbilde av dagens beredskap. Samtidig etablerer de et utgangspunkt for å følge utviklingen over tid og vurdere om virksomhetene lykkes med å styrke den operative kapasiteten.

Til forskjell fra det foregående kapitlet, handler disse spørsmålene mer om operativ beredskap. De måler hvor godt rustet virksomhetene er til å håndtere et cyberangrep når sikkerhetsarbeidet settes på prøve.

## Beredskapskjeden blir svakere jo nærmere hendelsen kommer

Det formelle apparatet er i stor grad på plass. Rundt tre av fire virksomheter har klare prosedyrer for å rapportere og håndtere cyberangrep. Dette viser at de fleste virksomheter har etablert et planverk for håndtering av cyberangrep.

Derfra blir resultatene gradvis svakere. Omtrent to av tre virksomheter oppgir at de har beredskap for gjenoppretting av systemer og data etter et cyberangrep. Andelen som oppgir å ha tilstrekkelig kompetanse innen cybersikkerhet er betydelig lavere, og lavest ligger regelmessige øvelser.

Mønsteret er tydelig. Resultatene er høyest på områder som handler om planverk og prosedyrer, og lavest på områder som krever kompetanse, trening og praktisk gjennomføring. Jo nærmere vi kommer en faktisk hendelse, desto svakere blir resultatene.

Planverk er nødvendig, men gir ikke alene trygghet for at virksomheten kan håndtere en alvorlig hendelse. Operativ beredskap forutsetter også at ansvar er tydelig, kompetansen er tilgjengelig og rutinene fungerer under press.

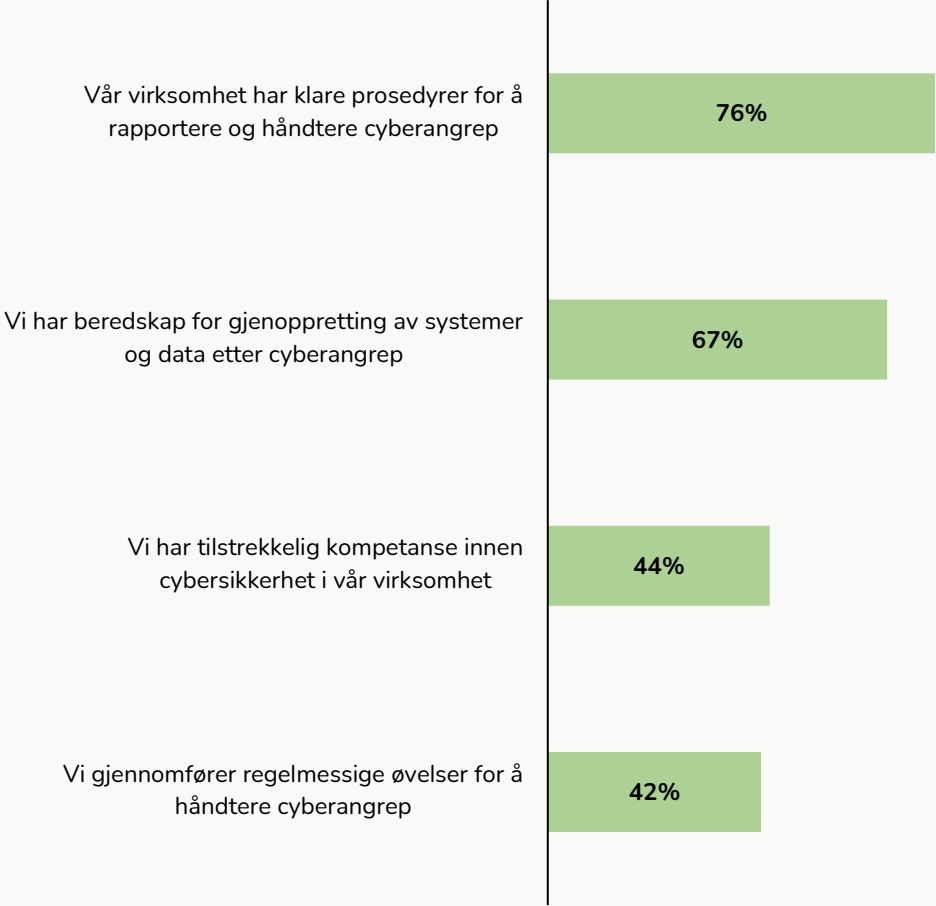
## KI øker kravene til kompetanse og beredskap

Utviklingen innen kunstig intelligens kan forsterke gapet mellom planverk og faktisk beredskap. KI kan brukes til å automatisere kartlegging, phishing og sosial manipulasjon, og reduserer terskelen for å gjennomføre avanserte angrep. Dermed øker betydningen av kompetanse, trening og innøvde roller. Når hendelser utvikler seg raskere, blir avstanden mellom planverk og faktisk beredskap enda viktigere.

## Øvelse viser om beredskapen virker

Regelmessige øvelser er den tydeligste testen på om virksomheten er i stand til å håndtere et cyberangrep. Prosedyrer beskriver hva som skal gjøres, men øvelser viser om organisasjonen faktisk er i stand til å gjøre det når tidspresset øker og konsekvensene blir reelle. At under halvparten av virksomhetene gjennomfører regelmessige øvelser, er derfor et av de mest alvorlige funnene i dette spørsmålsbatteriet.

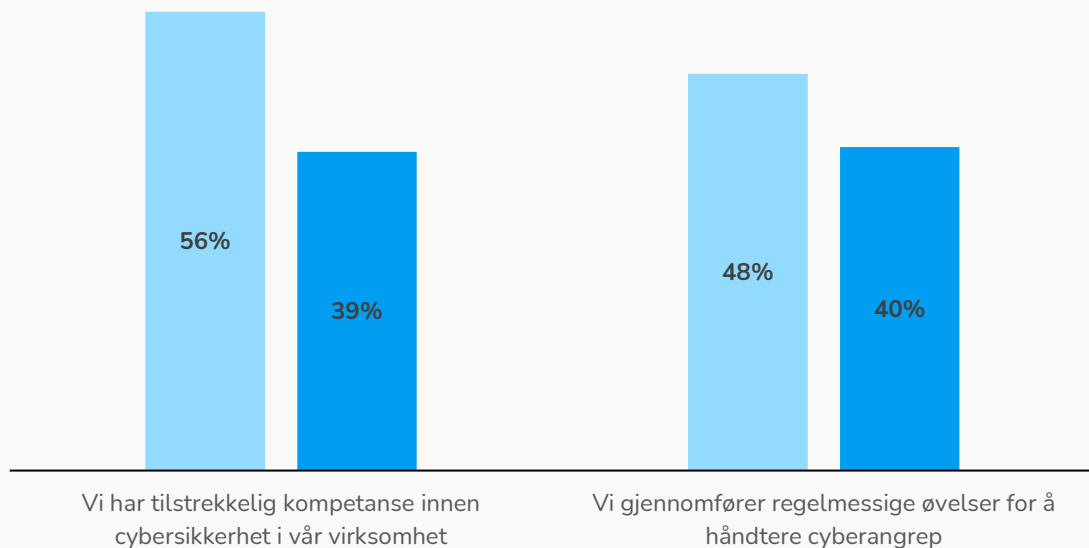
Andelen som svarer at de er enig eller helt enig i følgende påstander:





Ansatte i virksomheten forstår, etterlever og tar ansvar for informasjonssikkerhet i sitt daglige arbeid **46 %**

Andelen som svarer at de er enig eller helt enig i følgende påstander:



■ Stat ■ Kommune/fylkeskommune

## Under halvparten har praksisen som beredskap krever

De svakeste resultatene finner vi på områder som krever kompetanse, øvelser og aktiv deltakelse fra ansatte. Både kompetanse, øvelser og etterlevelse ligger under halvparten av alle respondentene, og resultatene er gjennomgående svakere i kommunesektoren enn i staten. Mønsteret peker mot utfordringer med å omsette strukturer og planer til operativ kapasitet.

### Etterlevelse er det svakeste leddet

Offentlig sektor har i stor grad etablert de organisatoriske strukturene for sikkerhetsarbeidet. Nesten ni av ti virksomheter har dedikerte roller for informasjonssikkerhet og personvern, og et klart flertall gjennomfører risikovurderinger og oppgir god oversikt over egne verdier og systemer. Samtidig oppgir bare 46 prosent at ansatte forstår, etterlever og tar ansvar for informasjonssikkerhet i sitt daglige arbeid.

Forskjellen er betydelig. Etterlevelse framstår dermed som ett av de svakeste områdene i undersøkelsen. Resultatet peker på avstanden mellom formelle strukturer og faktisk praksis. Selv gode styringssystemer forutsetter at ansatte kjenner til kravene, forstår roller og følger etablerte rutiner i hverdagen. Tallene tyder på at dette fortsatt er en betydelig utfordring i mange virksomheter.

### Tre indikatorer peker på det samme problemet

Resultatene for etterlevelse, cybersikkerhetskompetanse og øvelser ligger alle under 50 prosent. Til sammen tegner de et tydelig bilde: Sikkerhetsarbeidet er svakest der det er mest avhengig av kompetente og øvede ansatte som kjenner sitt ansvar og faktisk deltar.

Etterlevelse, kompetanse og øvelser bør derfor ses i sammenheng. Kompetanse gir ansatte forutsetninger for å forstå og håndtere sikkerhetskrav, mens øvelser tester

om roller, rutiner og beredskapsplaner fungerer i praksis. Samlet viser indikatorene hvor krevende det er å omsette sikkerhetsarbeidet til praktisk kapasitet.

Kommunesektoren ligger lavere enn staten på både cybersikkerhetskompetanse og regelmessige øvelser. Kompetansegapet er størst, med 56 prosent i staten mot 39 prosent i kommunesektoren. For øvelser er forskjellen mindre med 48 mot 40 prosent, men nivået er lavt i begge sektorer. Resultatene peker dermed både på ulike forutsetninger og en felles utfordring med praktisk beredskap.

### Den neste utfordringen handler om gjennomføring

Neste steg handler ikke først og fremst om flere styringsdokumenter eller planer, men om å gjøre ansvaret tydelig, håndterbart og operativt i den daglige driften. Medarbeidere må vite hva som forventes, ha kompetansen de trenger og få tid, støtte og handlingsrom til å følge opp sikkerheten i praksis.

Nasjonal sikkerhetsmyndighet beskriver den samme mekanismen i *Risiko 2026*, der de viser til at sikkerhetsansvar altfor ofte plasseres hos medarbeidere som verken er kjent med oppgaven eller er satt i stand til å løse den. Resultatene fra vår undersøkelse peker mot at dette fortsatt er en utfordring for en del av virksomhetene.



## Signalene er tydelige. Gjennomføringen er utfordringen

Virksomhetene vet i stor grad hva som forventes av dem. Et klart flertall opplever styringssignalene innen informasjonssikkerhet, personvern og cybersikkerhet som både tydelige og forpliktende. Samtidig opplever bare halvparten at de får god støtte fra nasjonale myndigheter. Funnene peker mot den samme utfordringen: Virksomhetene mangler ikke retning, men støtte til å omsette kravene til praktisk gjennomføring.



# Forpliktende krav, mangelfull støtte

Virksomhetene vet hva som forventes av dem. Rundt fire av fem opplever styringssignalene innen informasjonssikkerhet som tydelige og forpliktende. Samtidig opplever kun halvparten at de får god støtte til å innfri kravene.

## Kravene er kjent

Virksomhetene som deltar i IT i praksis er ikke i tvil om hva som forventes av dem på sikkerhetsområdet. Rundt fire av fem opplever styringssignalene innen informasjonssikkerhet som både tydelige og forpliktende. Resultatene viser at krav i stor grad er forstått og kjent i virksomhetene.

Mønsteret er viktig i lys av funnene tidligere i temarapporten. Utfordringene knyttet til kompetanse, øvelser og etterlevelse ser ikke ut til å skyldes uklarhet om retning eller manglende forståelse av hvilke krav som gjelder. Virksomhetene opplever i stor grad at forventningene er tydelige. Spørsmålet er derfor ikke *hva* de skal gjøre, men *hvordan* de skal lykkes med å gjøre det.

## Støtten er svakere

Samtidig som kravene til sikkerhet og beredskap blir flere og mer omfattende, opplever mange virksomheter at støtten ikke utvikler seg i samme takt. Kun halvparten mener de får god støtte fra sentrale myndigheter, og mange står igjen med ansvaret for å tolke regelverk, omsette krav til praksis og håndtere et stadig mer komplekse trusselbilde på egen hånd. For virksomheter med små fagmiljøer kan avstanden mellom forventninger og tilgjengelig støtte bli særlig stor.

## Utfordringen handler om gjennomføring, ikke om retning

Tallene tyder ikke på at virksomhetene mangler forståelse for betydningen av sikkerhet og beredskap.

Tvert imot er styringssignalene tydelige, ansvarsforholdene i stor grad etablert og de formelle strukturene på plass. Utfordringen oppstår når kravene skal omsettes til praktisk handling i organisasjonen.

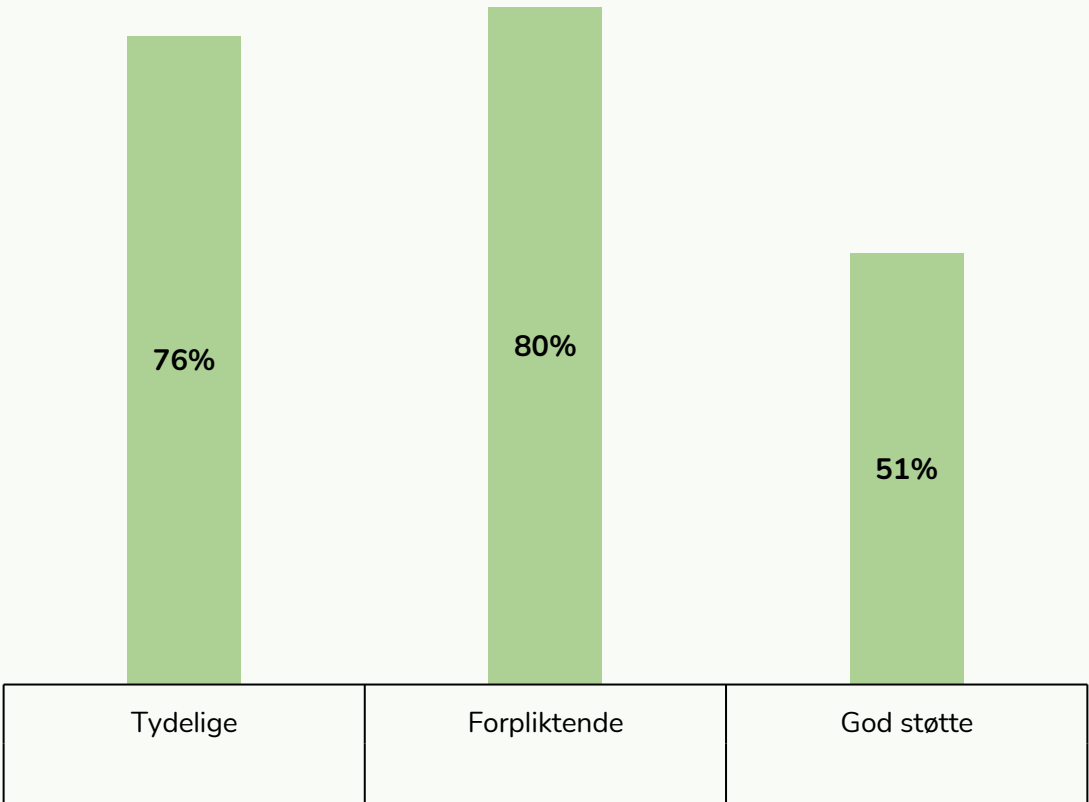
Mange opplever at kompetansen ikke strekker til, at støtten er utilstrekkelig, og at arbeidet i for liten grad følges opp gjennom øvelser, trening og systematisk læring. Samtidig viser andre funn i undersøkelsen at virksomhetene er mer usikre på egen kompetanse og kapasitet enn tidligere. Avstanden mellom ambisjoner og faktisk beredskapsevne blir dermed større enn de formelle strukturene alene skulle tilsi.

Dette peker mot en utfordring som i mindre grad handler om å etablere nye krav, og i større grad om å sikre at eksisterende krav faktisk omsettes til kompetanse, kapasitet og handling i praksis.

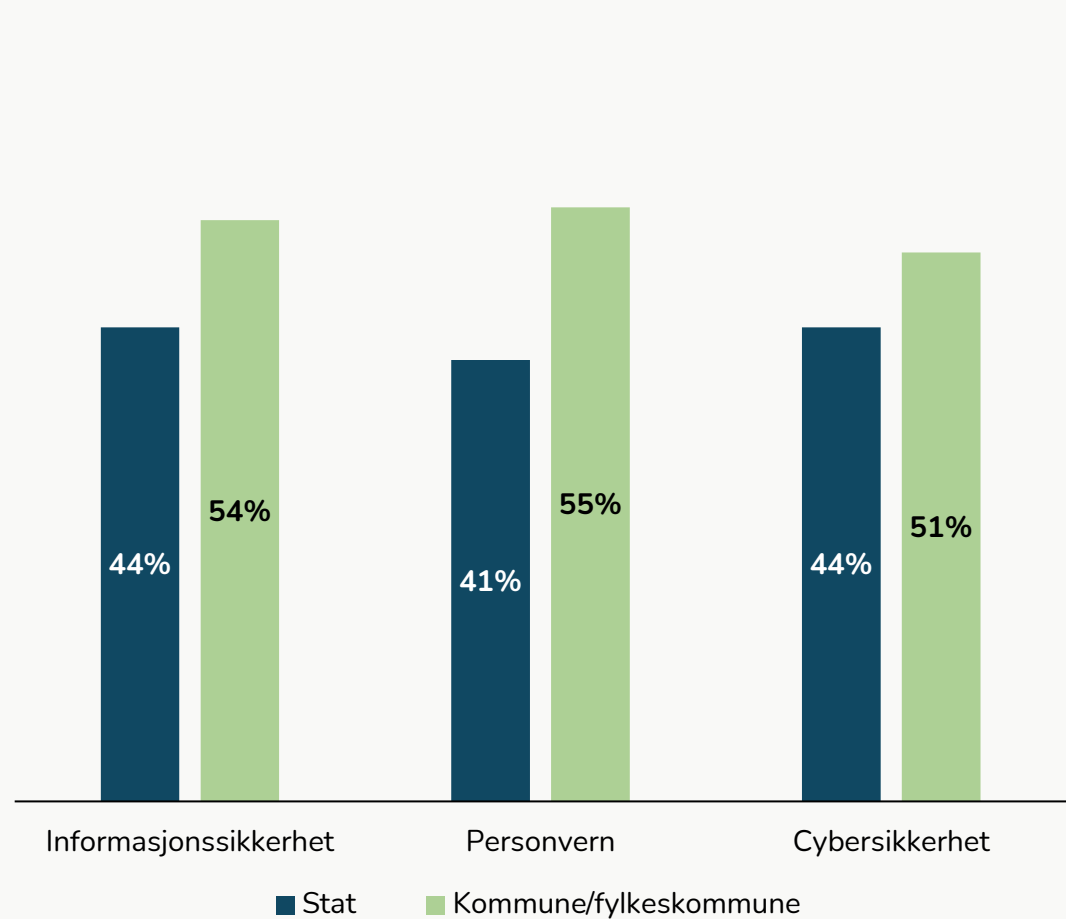
## Konkret støtte kan redusere gapet

Sikkert.no, en nasjonal portal for råd og veiledning om digital sikkerhet, utviklet av NSM i samarbeid med Digitaliseringsdirektoratet, politiet og Datatilsynet, ble lansert i januar 2026. Ved å samle myndighetenes råd, verktøy og kontaktpunkter på ett sted kan Sikkert.no gjøre det enklere å omsette overordnede krav til praktiske tiltak. Portalen kan dermed møte behovet for mer samordnet og konkret gjennomføringsstøtte. Effekten vil avhenge av at tilbudet blir kjent og om det er tilpasset virksomhetenes ulike behov.

Andelen som svarer at de er enig eller helt enig i at styringssignalene er tydelige og forpliktende, og at de får god støtte fra nasjonale myndigheter innen informasjonssikkerhet.



Andelen som svarer at de er **enig** eller **helt enig** i at de får god støtte fra nasjonale myndigheter innen informasjonssikkerhet, personvern og cybersikkerhet



Ramboll

<sup>8</sup>: Riksrevisjonen (2023). Myndighetenes samordning av arbeidet med digital sikkerhet i sivil sektor. Dokument 3:7 (2022–2023).

<sup>9</sup>: Justis- og beredskapsdepartementet & Forsvarsdepartementet. (2025). Nasjonal sikkerhetsmyndighet – oppgaver og styring (G-0460 B).

# Statlige virksomheter opplever mindre støtte enn kommunene

Statlige virksomheter opplever mindre støtte fra nasjonale myndigheter enn kommuner og fylkeskommuner, til tross for at styringssignalene oppleves omtrent like tydelige. Resultatet utfordrer en antakelse om at nærhet til nasjonale myndigheter gir bedre tilgang på veiledning og støtte.

## Staten opplever mindre støtte enn kommunene

Forskjellene mellom statlig og kommunal sektor er tydelige. På alle tre områdene oppgir statlige virksomheter at de får mindre støtte enn kommunene. Innen informasjonssikkerhet opplever 44 prosent av statlige virksomheter god støtte, mot 54 prosent av kommunene. Tilsvarende forskjeller finner vi innen personvern og cybersikkerhet, der kommunene også vurderer støtten høyere enn staten.

Funnet er interessant fordi det bryter med en vanlig antakelse om at kommunene står svakest rustet. Kommunene har ofte mindre fagmiljøer og færre spesialister, men opplever likevel mer støtte enn statlige virksomheter. Resultatene tyder på at utfordringen ikke nødvendigvis handler om størrelsen på virksomhetene, men om hvordan støtteapparatet oppleves av dem som skal etterleve kravene i praksis.

## Forskjellen gjelder støtte, ikke krav

Forskjellen mellom statlig og kommunal sektor handler ikke om hvor tydelige kravene oppleves. Som vist på forrige side vurderer virksomhetene styringssignalene innen informasjonssikkerhet, personvern og cybersikkerhet som både tydelige og forpliktende. Det er først når virksomhetene blir spurt om støtte til å innfri kravene at forskjellene blir tydelige.

Dette gjør funnet særlig interessant. Statlige virksomheter opererer ofte nærmere de nasjonale myndighetene som utvikler regelverkene og utformer styringssignalene. Likevel er det de som i minst grad opplever at de får tilstrekkelig støtte.

Resultatene tyder dermed på at utfordringen ikke først og fremst handler om forståelse av kravene, men om virksomhetenes opplevelse av å få hjelp til å omsette kravene til kompetanse, kapasitet og praktisk gjennomføring.

Dette samsvarer også med funn fra andre rapporter om koordinering av offentlig støtte knyttet til cybersikkerhet. Riksrevisjonen har tidligere pekt på behovet for tydeligere samordning av nasjonal digital sikkerhet i sivil sektor, og at veiledningen må bli mer samordnet og tilgjengelig.<sup>8</sup> Et utvalg som gikk gjennom NSMs oppgaver i 2025, viste også at NSMs oppdrag innen digital sikkerhet har økt, noe som kan ha svekket evnen til å gjennomføre kjerneoppdraget.<sup>9</sup> I digitalsikkerhetsloven er relevante departementer gitt ansvar for tilsyn i egen sektor, men varierende kompetanse og kapasitet kan føre til ulik opplevd støtte.

## Utfordringen gjelder hele offentlig sektor

Resultatene viser at utfordringen ikke kan forklares med at enkelte deler av offentlig sektor henger etter. Tvert imot opplever både statlige og kommunale virksomheter at støtten er svakere enn kravene som stilles. Selv om kommunene vurderer støtten noe høyere enn staten, ligger resultatene i begge sektorer rundt eller under halvparten. Det kan indikere at utfordringen er bredere enn spørsmål om størrelse, organisering eller tilgang på ressurser.

Funnene peker dermed mot en mer generell utfordring i sikkerhetsarbeidet. Virksomhetene vet i stor grad hva som forventes av dem, men mange opplever at de mangler tilstrekkelig støtte til å omsette kravene til kompetanse, kapasitet og praktisk gjennomføring.



## Tillit krever mer enn god forvaltning

Tilliten til at offentlig sektor forvalter personopplysninger står støtt. Samtidig tviler mange på beskyttelsen mot cyberangrep, og de opplever liten innsikt i og kontroll over hvordan data deles og brukes i offentlig sektor. Spesielt når data tas i bruk på nye måter og i KI, blir åpenhet og etterprøvbarehet avgjørende for å bevare tilliten.



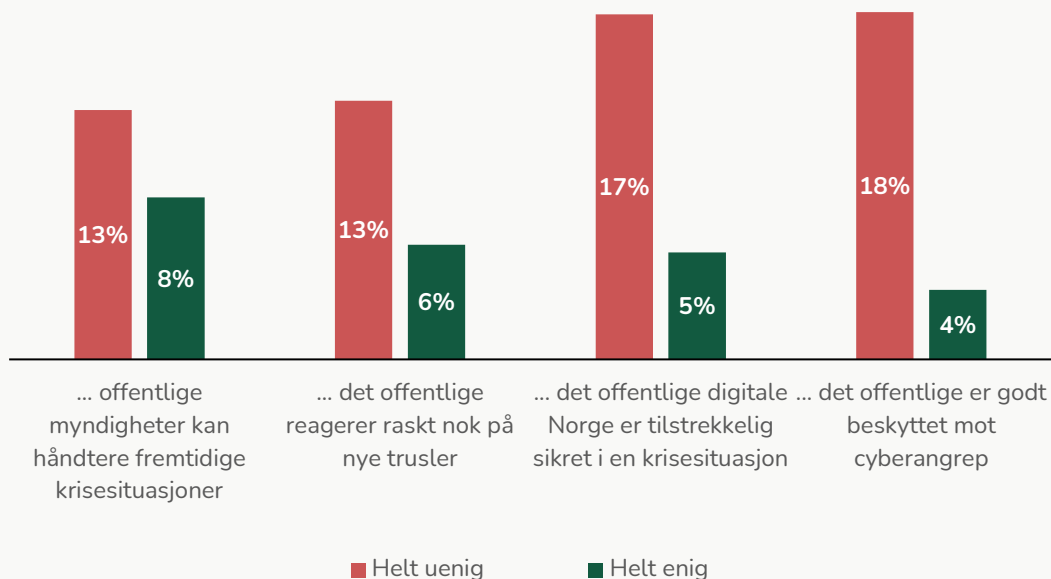
# Innbyggerne skiller mellom forvaltning og beskyttelse

Andel av innbyggerne som i **høy** eller **ganske høy** grad



har tillit til at digitale løsninger fra offentlige myndigheter ivaretar deres opplysninger på en trygg måte – uendret siden 2021 **51 %**

Andelen som har svart helt enig eller helt uenig i at de føler seg trygge på at ...



Tilliten til at offentlige virksomheter håndterer personopplysninger på en god måte har vært stabil over tid. Samtidig er tilliten til at det offentlige er godt beskyttet mot cyberangrep betydelig lavere. Innbyggerne ser ut til å ha tillit til institusjonene, men større tvil om deres evne til å beskytte seg mot digitale trusler.

## Tilliten til forvaltningen av opplysninger står støtt

Innbyggernes tillit til offentlige digitale tjenester har vært stabil over tid. Omtrent halvparten av befolkningen oppgir at de har tillit til at det offentlige ivaretar personopplysningene deres på en god måte. Til tross for økt digitalisering, flere sikkerhetshendelser og økende oppmerksomhet rundt personvern, viser målingene små endringer fra 2021 til 2026. Samtidig vil vi bemerke at undersøkelsen ble gjennomført før hendelsen i Lørenskog kommune og bølgen av tjenestenektangrep mot offentlige tjenester i august, og at slike hendelser kan påvirke befolkningens tillit.

## Men beskyttelsen er noe annet

Spørsmålene om myndighetenes beredskap gir et helt annet bilde. Bare 4 prosent er helt enige i at det offentlige er godt beskyttet mot cyberangrep, mens 18 prosent er helt uenige. Tilsvarende er bare 5 prosent helt enige i at det offentlige digitale Norge er tilstrekkelig sikret i en krisesituasjon, mens 17 prosent er helt uenige. Mønsteret går igjen på de øvrige spørsmålene om beredskap, der andelen som er uenig gjennomgående er større enn andelen som er enig.

Resultatene viser at innbyggerne skiller mellom hvordan opplysninger forvaltes og hvor godt digitale systemer er beskyttet. Tilliten er høyere når spørsmålene handler om myndighetenes generelle håndteringsevne enn når de handler om den konkrete beskyttelsen mot cyberangrep.

## Skillet er verdt å forstå presist

At tilliten til offentlige digitale løsninger ligger stabilt rundt 51 prosent, mens bare 4 prosent er helt enig i at

det offentlige er godt beskyttet mot cyberangrep, viser at tillit ikke er én størrelse. Innbyggerne ser ut til å skille mellom hvordan myndighetene forvalter opplysninger og hvor godt de er i stand til å beskytte systemene som opplysningene lagres i.

## Skepsisen er ikke uinformert

Det er nærliggende å se resultatene i lys av et skjerpet trusselbilde og økt oppmerksomhet om digitale trusler. Samtidig peker flere av funnene i årets rapport i samme retning. Under halvparten av virksomhetene gjennomfører regelmessige øvelser for å håndtere cyberangrep, kun 46 prosent mener ansatte etterlever informasjonssikkerheten i det daglige arbeidet, og under halvparten opplever cybersikkerhetskompetansen som tilstrekkelig.

Innbyggernes vurderinger samsvarer dermed med flere av de utfordringene virksomhetene selv rapporterer. Når så få mener det offentlige er godt beskyttet mot cyberangrep, framstår skepsisen som forståelig snarere enn ubegrunnet.

## Det gjør tillit til et styringsspørsmål

Tillit til offentlig digital beredskap kan ikke bygges gjennom kommunikasjon alene. Innbyggernes vurderinger samsvarer med flere av de målte svakhetene, og da lukkes gapet først når svakhetene lukkes.

Samtidig ligger det en mulighet i at rundt halvparten fortsatt har tillit til hvordan opplysninger forvaltes. Men denne tilliten overføres ikke automatisk til troen på at systemene er tilstrekkelig beskyttet.

# Høy aksept, lav opplevd kontroll

Innbyggerne er langt mer positive til datadeling når nytten er tydelig, enn når det handler om egen innsikt og kontroll. Rundt tre av ti er helt enige i at opplysninger kan deles for å forenkle offentlige tjenester. Bare 4 prosent er helt enige i at de har tilstrekkelig informasjon eller mulighet til å kontrollere hvordan opplysningene deles.

## Innbyggerne er villige til å dele

Innbyggerne avviser ikke datadeling. Aksepten er høy når formålet er konkret, nytten tydelig og delingen skjer i tråd med personvernreglene. 30 prosent er helt enige i at offentlige myndigheter kan dele opplysninger dersom det gir raskere saksbehandling, mens 8 prosent er helt uenige. Når delingen gjør at innbyggerne slipper å oppgi den samme informasjonen flere ganger, er 29 prosent helt enige og 9 prosent helt uenige. Disse resultatene peker på at mange ser verdien av datadeling når den bidrar til enklere og mer sammenhengende tjenester. Det kan forstås som at innbyggerne er mest positive når gevinsten er nær og forståelig.

## Men de opplever ikke å ha oversikt

Når spørsmålene gjelder egen innsikt og kontroll, snur bildet. Bare 4 prosent er helt enige i at de har tilstrekkelig informasjon om hvordan offentlige myndigheter bruker dataene deres, mens 18 prosent er helt uenige. Det samme gjelder muligheten til å kontrollere delingen: 4 prosent er helt enige, mot 18 prosent helt uenige. Forskjellen mellom svarene på spørsmålene om nytte og spørsmålene om oversikt er markant. Innbyggerne kan være positive til resultatet av datadelingen uten å oppleve innsikt i prosessene bak. Det kan gjøre det vanskelig å forstå hvilke opplysninger som brukes, hvem som får tilgang, og hvordan den enkelte kan påvirke bruken.

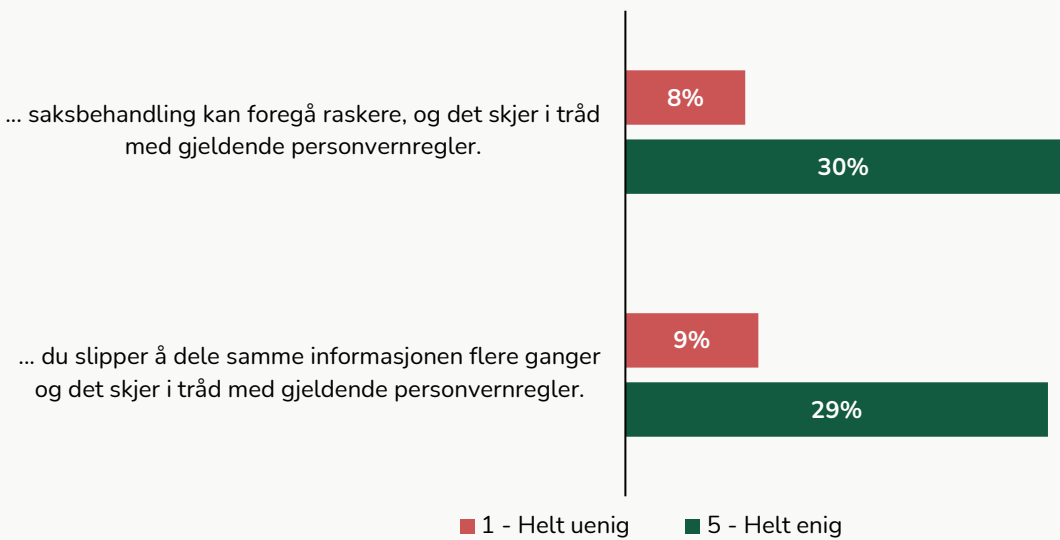
## Aksept er ikke det samme som tillit

Aksept og tillit må forstås som to forskjellige størrelser. Innbyggerne kan godta datadeling fordi de ser nytten, uten samtidig å forstå eller kunne påvirke hvordan opplysningene brukes. Dette blir viktigere når data brukes på nye måter og i KI-løsninger. Som KI-rapporten peker på, overføres ikke tillit vi har til offentlige institusjoner automatisk over til offentlige digitale løsninger. Når KI inngår i beslutninger som berører innbyggerne, må offentlig sektor være åpen og tydelig om hvorfor teknologien brukes, hvilke data som ligger til grunn, hva systemet gjør, hva mennesker avgjør, og hvordan beslutningene kan etterprøves.

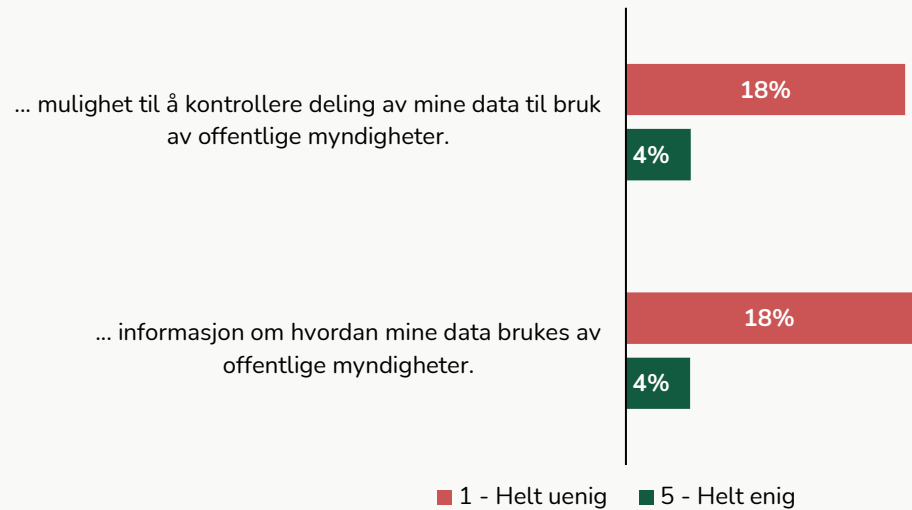
## Innsikt og kontroll må styrkes

Offentlig sektor må gjøre det enklere for innbyggerne å forstå hvilke opplysninger som brukes, hvem de deles med, og hvorfor delingen er nødvendig. Informasjonen bør være tilgjengelig og tilpasset situasjonen der opplysningene brukes. Den bør forklare hvor innbyggerne kan henvende seg dersom noe er uklart eller feil. Tydelig kommunikasjon må kombineres med muligheter for innsyn, korrigering og påvirkning. Innbyggerne bør ikke bare se nytten av datadelingen, men også oppleve oversikt over hvordan den foregår. Slik kan offentlig sektor realisere gevinstene ved datadeling og samtidig styrke opplevelsen av kontroll og tillit.

Du synes det er greit at offentlige myndigheter deler informasjon om deg, dersom ...



Jeg opplever å ha tilstrekkelig ...





# Det som kommer vil teste det som er svakest i dag

Temarapporten viser at offentlig sektor i stor grad har etablert strukturene for sikkerhetsarbeidet. Det som kommer, vil teste om de er godt nok forankret i ledelsen, øvd i organisasjonen og støttet av konkrete virkemidler. Samtidig vil mer datadeling, bruk av KI og angrep som kan gjennomføres raskere, stille større krav til sikkerhet, åpenhet og innbyggernes tillit.

# Strukturene er på plass. Nå må de virke i praksis

Denne rapporten viser at offentlig sektor i stor grad har etablert strukturene for sikkerhetsarbeidet. Det neste steget er å få dem til å virke bedre i praksis – gjennom tydeligere ledelsesforankring, mer trening og etterlevelse, mer konkret støtte og større åpenhet, innsikt og kontroll. Det blir avgjørende både for beredskapen og innbyggernes tillit.

## Styringen må forankres i ledelsen

De grunnleggende strukturene er i stor grad på plass, men bare 57 prosent oppgir at virksomhetsledelsen gir tydelige føringer for informasjonssikkerhetsarbeidet. Framover må sikkerhet i større grad inngå i virksomhetsstyringen og i beslutninger om prioriteringer, ressurser og tjenesteutvikling. Ledelsen må sette retning, avklare ansvar og følge opp om tiltakene gir ønsket effekt. Først når sikkerhetsarbeidet blir en integrert del av den løpende styringen, kan etablerte roller og rutiner omsettes til reell gjennomføringsevne.

## Beredskapen må trenes og etterleves i praksis.

De fleste virksomhetene har prosedyrer for å håndtere cyberangrep, men bare 42 prosent øver regelmessig, og 46 prosent oppgir at ansatte etterlever sikkerhetskravene i det daglige arbeidet. Samtidig kan KI gjøre det enklere å automatisere og gjennomføre angrep raskere og i større omfang. Det reduserer tiden virksomhetene har til å oppdage, vurdere og håndtere hendelser. Planverket må derfor testes gjennom realistiske øvelser, tydelige roller og systematisk læring. Når tempoet øker, blir kompetanse og øvd respons avgjørende for å begrense konsekvensene.

## Støtten må bli mer konkret og tilpasset

Rundt fire av fem virksomheter opplever styringssignalene som tydelige og forpliktende, men bare 51 prosent mener de får god støtte fra nasjonale myndigheter. Utfordringen handler derfor mindre om å formulere nye krav og mer om å hjelpe virksomhetene med å gjennomføre dem. Veiledning, verktøy og kompetansetiltak må bli mer konkrete, samordnede og tilpasset virksomhetenes ulike behov. Slik kan tydelige forventninger omsettes til kompetanse, kapasitet og handling i praksis.

## Tillit må bygges gjennom beskyttelse, innsikt og kontroll

Innbyggerne aksepterer datadeling når nytten er tydelig, men få opplever tilstrekkelig innsikt i eller kontroll over hvordan egne data brukes. Samtidig tviler mange på det offentliges beskyttelse mot cyberangrep. Når data deles mer og brukes i KI-løsninger, må offentlig sektor være åpen om hvilke data og vurderinger som ligger til grunn, hvordan beslutninger tas, og hva mennesker avgjør. Tillit må bygges gjennom reell sikkerhet, forståelig informasjon og muligheter for innsyn, korrigering og etterprøving.

Forholdene som kommer, og funnene som avgjør hvordan vi møter dem



Styringen må forankres. Bare 57 prosent oppgir at ledelsen gir tydelige føringer i dag.

57 %



Beredskap må øves. Under halvparten øver regelmessig på å håndtere cyberangrep.

42 %



Støtten må bli mer konkret. Bare 51 prosent opplever god støtte fra nasjonale myndigheter.

51 %



Tillit må fortjenes. Bare 4 prosent er helt enige i at de har tilstrekkelig informasjon om eller kontroll over datadelingen.

4 %

# Fra ambisjoner til praksis som virker

Årets funn peker på hva som må til for at KI skal gi verdi og sikkerhetsarbeidet skal virke når det gjelder. Arbeidet med KI og sikkerhet må ses i sammenheng, for når KI tas i bruk, må sikkerhet og personvern være med fra starten, og beredskapen må øves på et trusselbilde der angrep går raskere. Ansvaret ligger ikke hos én aktør alene. Virksomhetene, nasjonale myndigheter og fagmiljøene som støtter dem må trekke i samme retning.

## I virksomhetene

Virksomhetene kan med fordel forankre både KI og sikkerhet tydeligere i virksomhetsstyringen, med mål, prioriterte ressurser, avklarte ansvar og jevnlig oppfølging. Et mulig neste steg er å koble KI tettere til kjerneoppgaver og fagsystemer, og undersøke hvordan frigjort tid kan gi gevinster på virksomhetsnivå. Det kan også være nyttig å bygge kompetanse systematisk, vurdere risiko tidlig og støtte etterlevelse i det daglige. Realistiske øvelser, tydelige roller og læring etter hendelser kan bidra til at planverket fungerer bedre under press.



## Nasjonalt

Det er behov for tydeligere retning for KI og mer praktisk gjennomføringsstøtte innen både bruk av KI og innen sikkerhet og beredskap. Virksomhetene trenger hjelp med regelverk, etikk, risikovurdering, valg av løsninger og bruk av data, og ønsker det for eksempel gjennom sjekklister, maler, nettverk og sandkasser. KI Norge og Sikkert.no kan spille en samlende rolle dersom tilbudene blir godt kjent, koordinert og tilpasset ulike forutsetninger i stat og kommune. Nasjonale myndigheter kan også vurdere flere tiltak for kompetansebygging og erfaringsdeling, slik at virksomhetene lettere kan lære av hverandre.



## Overfor innbyggerne

Funnene kan tyde på at tilliten til nye digitale løsninger ikke kan tas for gitt. For å styrke den kan offentlig sektor være tydelig på hvorfor KI brukes, hvilke data som inngår, hva systemene gjør, hva mennesker avgjør og hvordan beslutninger kan etterprøves. Det kan også være hensiktsmessig å gi innbyggerne gode muligheter til innsyn, korrigering, kontroll og medvirkning. Samtidig kan virksomhetene synliggjøre hvordan data og tjenester beskyttes, og hvordan beredskapen øves. Slik kan forståelig nytte, håndtert risiko og tydelig ansvar bidra til økt tillit.



# Menneskene bak *IT i praksis*

Redaksjonsgruppen for *IT i praksis* 2026 består av:

**Mathias Sikveland Wee**, Manager

Prosjektleder og kontaktperson for *IT i praksis*

[mwee@ramboll.com](mailto:mwee@ramboll.com)

**Henrik Stener Pedersen**, Direktør

Ansvarlig for *IT i praksis*

[heks@ramboll.com](mailto:heks@ramboll.com)

**Thomas Nortvedt**, Manager

[thno@ramboll.com](mailto:thno@ramboll.com)

**Gunder Fyllingen Nordgården**, Konsulent

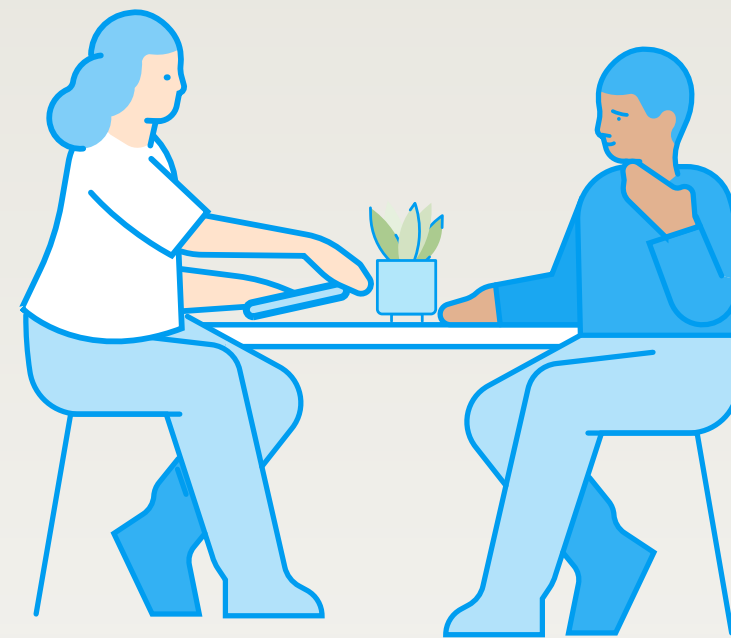
[guno@ramboll.com](mailto:guno@ramboll.com)

**Katrine Rummelhoff**, Lead Consultant

**Rikke Munkvold**, Konsulent

**Kristina Heldal**, Prosjektassistent

**Live Amalie Krogsrud**, Prosjektassistent



Bright  
ideas.  
Sustainable  
change.

RAMBOLL