



Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet

Et tillegg til Kommunedirektørens internkontroll – Orden i eget hus



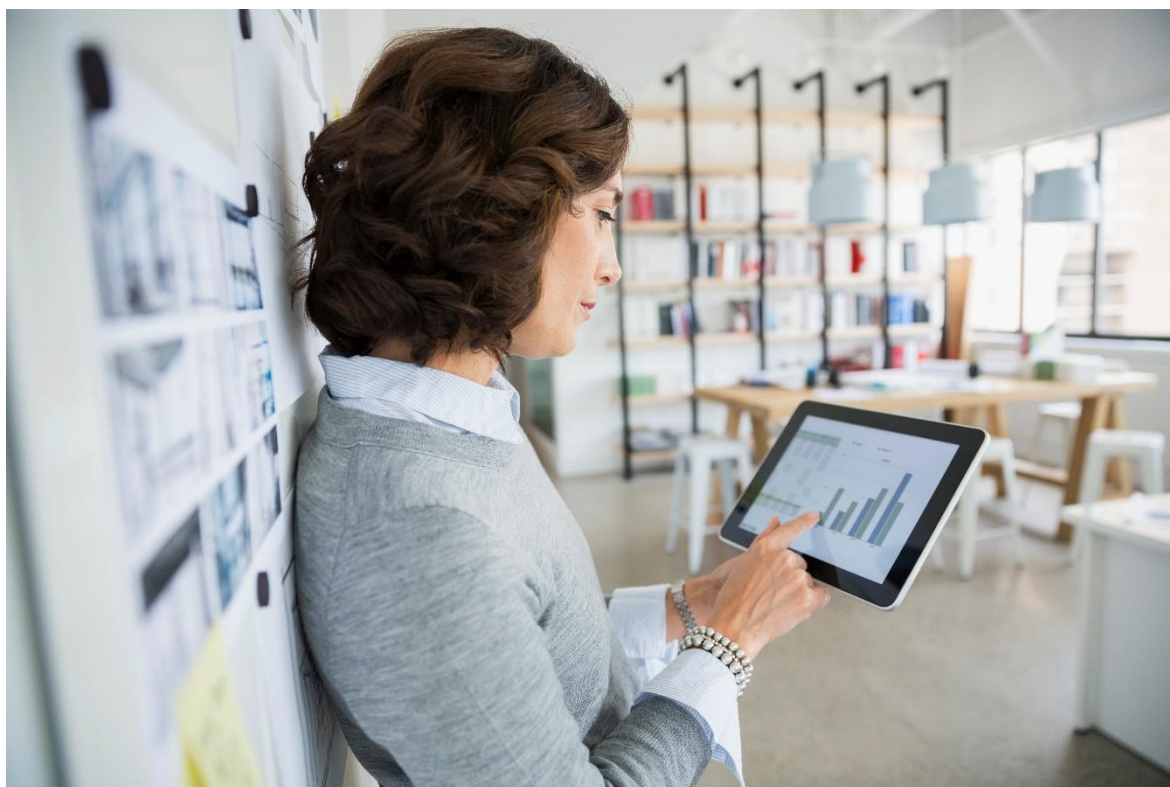
Innledning	3
1. Hvordan bruker du verktøykassen?	4
2. Sikkerhetsstyring som integrert del av virksomhetsstyringen	5
2.1 Risikoforståelse og sikkerhetsstyring	5
3. Om informasjonssikkerhet og personvern	6
3.1 Hva er informasjonssikkerhet?	6
3.2 Grunnprinsipper for sikkerhetsstyring	7
3.3 Hva er personvern?	8
3.4 Personvernprinsippene	8
3.5 Informasjon som verdi	9
3.6 Informasjonssikkerhet og personopplysningssikkerhet ivaretas gjennom sikkerhetstiltak	12
3.7 Personvern ivaretas gjennom involvering, medbestemmelse, åpenhet og forutsigbarhet	12
3.8 Ledelse av arbeid med informasjonssikkerhet og personvern	13
4. Hvordan oppnå etterlevelse og organisere arbeidet?	18
4.1 Planlegge	19
4.2 Utføre	20
Digitaliseringsprosjekter	20
4.3 Kontrollere	21
4.4 Korrigere	22
Avvik (Forbedringsprosess)	22
4.5 Roller og ansvar	23
Informasjonssikkerhetsansvarlig	23
Personvernombud	24
4.6 Sikkerhetskultur	24
VEDLEGG	27
Vedlegg 1 Regelverket	27
Vedlegg 2 Grunnprinsipper for sikkerhetsstyring	27
Vedlegg 4 Tjenesteutsetting	27
Vedlegg 5 Sjekkklister	27
Vedlegg 6 Definisjoner og nasjonale ressurser personvern og informasjonssikkerhet	27
Vedlegg 7 Kunstig intelligens	27
Vedlegg 8 Mal Nødplakat (fylles ut/ferdigstilles av den enkelte kommune)	27

Innledning

I en stadig mer digitalisert verden, er det viktig at toppledere har kunnskap om digital risiko, muligheten for å redusere risiko og regelverk. For å nå mål og ønsket effekt av digitaliseringen, er det viktig å ta hensyn til personvern og informasjonssikkerhet allerede fra start.

Digitale angrep og hendelser kan få alvorlige konsekvenser for kommunens tjenesteproduksjon, lede til driftsavbrudd, tap av kritisk informasjon og økonomiske tap. Enkeltpersoners grunnleggende rettigheter knyttet til selvbestemmelse og autonomi kan også stå på spill dersom kommunen ikke etterlever prinsippene om lovlig, åpen og rettferdig behandling av personopplysninger. Evnen til å forstå og håndtere risikoer som den digitale infrastrukturen innebærer er viktig for sikre god informasjonssikkerhet og godt personvern. På denne måten kan lover og regler følges og tjenester leveres med god kvalitet.

Kommuner behandler store mengder informasjon om innbyggere og ansatte, og mye av denne informasjonen er av privat karakter. I tillegg har kommuner en rekke samfunnskritiske oppgaver hvor det å ivareta informasjonsbehov og -beskyttelse har stor betydning. Økt digitalisering innebærer økt avhengighet av teknologiske løsninger. Teknologien må fungere for at kommunen skal kunne levere tjenester til innbyggerne. Leverandørkjedene blir også stadig mer komplekse. Det stiller krav til gode rutiner for oppfølging og kontroll.



1. Hvordan bruker du verktøykassen?

Denne verktøykassen skal gjøre det enklere for deg som kommunedirektør å forstå risiko og forsikre deg om at internkontroll på området personvern og informasjonssikkerhet gjennomføres på en god måte.

Verktøykassen tar utgangspunkt i [Orden i eget hus – Kommunedirektørens internkontroll](#), og er ment som et tillegg til denne. I likhet med *Orden i eget hus* bruker vi i fortsettelsen «kommune» for omtale av både kommuner og fylkeskommuner.

Verktøykassen er utarbeidet for at du som kommunedirektør skal forstå hva personvern og informasjonssikkerhet er, og kjenne ansvaret ditt knyttet til regelverk som angår personvern og informasjonssikkerhet. Videre skal den gi toppledere i kommunal sektor veiledning for å skaffe seg kontroll, og opprettholde denne kontrollen over tid.

I **kapittel 1** setter vi arbeidet med personvern og informasjonssikkerhet i sammenheng med den øvrige virksomhetsstyringen.

I **kapittel 2** kan du øke din kunnskap om fagområdet personvern og informasjonssikkerhet.

I **kapittel 3** skisseres en modell for internkontroll bygd på Demmings sirkel. Kapittelet skal gi deg som kommunedirektør konkrete råd, kontrollspørsmål og innspill til aktiviteter slik at du kan utøve ditt ansvar som leder.

Under enkelte kapitler ligger det sjekklister med kontrollspørsmål som du kan benytte for å få kontroll og opprettholde kontroll på området. Hvert kapittel inneholder også spørsmål til refleksjon i form av de blå sidene «Tenk gjennom». Verktøykassen ønsker også å komme med anbefalinger og råd til kommunedirektøren.

Helt til slutt i verktøykassen er det lagt til en rekke vedlegg med mulighet for fordypning i enkelttema, samt en oversikt over relevante offentlige virksomheter hvor man kan søke råd. Enkeltord vil ikke alltid forklares fortløpende i verktøykassen, men de finnes i definisjonslisten som også er et vedlegg til dokumentet.

Verktøykassen er utarbeidet for toppledere, og vi anbefaler deg som kommunedirektør å lese hele dokumentet.



Figur 1: Demmings sirkel. Sirkelen vil, i kapittel 6, bli brukt for å skissere hvordan en kommunedirektør bør arbeide med personvern og informasjonssikkerhet

2. Sikkerhetsstyring som integrert del av virksomhetsstyringen

Sikkerhetsstyring bør være en integrert del av virksomhetsstyringen. Dette betyr at sikkerhetsarbeid skal være en naturlig del av hvordan virksomheten ledes og organiseres.

Det overordnede ansvaret for alle tjenesteleveranser i kommunen ligger hos ledelsen. Ledelsen gjør dette ved å sette mål og føringer for kvalitet og prioriteringer, samt ved å følge opp og lede forbedringsarbeidet. Det samme gjelder for styringen av arbeidet med personvern og informasjonssikkerhet. Ledelsen skal sette mål og føringer for kvalitet og prioriteringer innenfor fagområdet personvern og informasjonssikkerhet, mens det operative ansvaret for å ivareta sikkerheten for kommunens verdier ligger hos de ansatte.

God mål- og resultatstyring handler om å styre for å oppnå effekter. Det betyr at kommunen må følge opp at det er sannsynlig at leveransene våre, i form av kommunale tjenester, gir de effektene vi forventer å se hos brukerne og i samfunnet. For å oppnå disse effektene, må vi levere god kvalitet og effektivitet i tjenesteleveransene våre. For å få til dette trenger vi god internkontroll.

Internkontroll øker sannsynligheten for at vi oppnår effektene. God kvalitet i tjenesteleveransene, og alt som støtter opp om leveransene (f. eks informasjonssystemene) forutsetter igjen god internkontroll med innsatsfaktorer, aktiviteter og prosesser. Har vi for eksempel ikke kontroll med budsjettene våre, folkene vi ansetter, eller vi har manglende oversikt over informasjonssystemene vi bruker, ja da blir det vanskelig å levere gode tjenester, og dermed oppnå de effektene hos brukere og samfunn som vi ønsker.

Styringssystemet for personvern og informasjonssikkerhet bør samordnes med virksomhetsstyringen ellers. Dette vil gi et felles grunnlag for å håndtere risikoer kommunen står overfor.

2.1 Risikoforståelse og sikkerhetsstyring

Å forstå hvilke typer risiko kommunen står ovenfor på de ulike fagområdene er viktig. Hvilke uønskede hendelser kan kommunen stå overfor, når de kan oppstå og hvilke konsekvenser kan disse få for administrasjon, politikere og innbyggere?

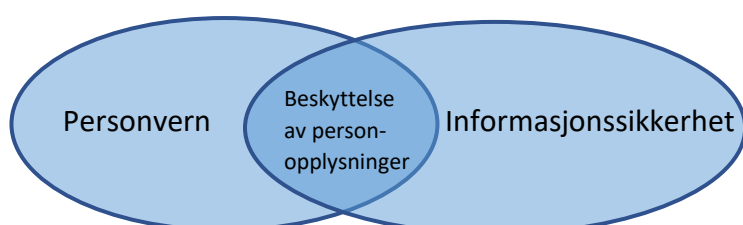
I en digital verden kan risikobildet være komplekst. Særlig gjelder dette når tjenester, støtteprosesser og ulike tekniske systemer og leverandører er avhengige av hverandre. Uønskede hendelsene kan oppstå på grunn av menneskelig svikt, svakheter i tekniske systemer, eller ufullstendige eller manglende prosedyrer. God risikoforståelse kjennetegnes ved at kunnskapen til den aktuelle risikoen er sterk, slik at man kjenner til hvordan en uønsket hendelse kan oppstå og hvilke konsekvenser den kan få.

Flere statlige veiledningsaktører har en aksje i veiledning om risikostyring, herunder [DSB](#), [DFØ](#), Digitaliseringsdirektoratet ([Digdir](#)), [Datatilsynet](#) og [NSM](#) på henholdsvis beredskap, økonomi, informasjonssikkerhet, personvern og nasjonal sikkerhet. [Digdir har veiledning hvor du kan lese om sammenhengen mellom virksomhetsstyring, informasjonssikkerhet, personvern og sikkerhetsstyring etter sikkerhetsloven.](#)

3. Om informasjonssikkerhet og personvern

Personvern og informasjonssikkerhet er to fagområder som har mye til felles, men også noen forskjeller. Fagene overlapper hverandre når det gjelder beskyttelsen av personopplysninger. Det er viktig å være oppmerksom på at informasjonssikkerhet er mer enn personopplysningssikkerhet, på samme måte som personvern er mer enn informasjonssikkerhet.

Forholdet mellom fagområdene kan forklares ved bruk av figuren under.

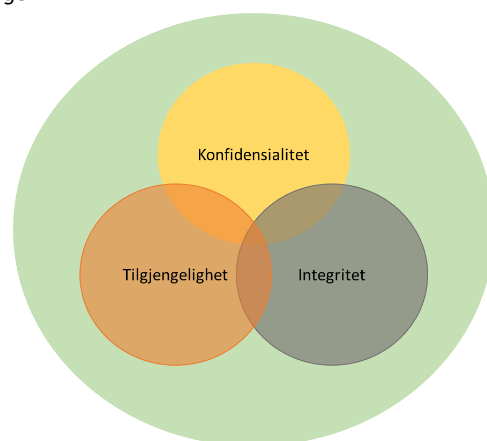


Figur 2: Figuren forklarer sammenhengen mellom informasjonssikkerhet og personvern. Det er to ulike fagområder, men overlapper når det gjelder beskyttelse av personopplysninger.

3.1 Hva er informasjonssikkerhet?

Informasjonssikkerhet handler om å verne all type informasjon, for eksempel opplysninger om kommunens innbyggere, ansatte, vannverk, økonomi eller kommunens servicetilbud. Ulik type informasjon vil ha forskjellig beskyttelsesbehov. Beskyttelsesbehovet kan deles opp i;

- Konfidensialitet: informasjon er beskyttet mot uautorisert innsyn
- Integritet: informasjonen er riktig, komplett og til å stole på
- Tilgjengelighet: informasjonen er tilgjengelig når det er behov for den



Figur 3: Konfidensialitet, integritet og tilgjengelighet

Noen eksempler på informasjon med ulike beskyttelsesbehov:

- Noen innbyggere har hemmelig adresse. For opplysninger som er knyttet til skjernet adresse er typisk vern mot uautorisert innsyn svært viktig å ivareta.
- Kommunen må journalføre og dokumentere sine aktiviteter. For dokumentasjon i arkivsystemet vil det være viktig at opplysningene er sikret mot utilsiktet endring og at det er tilrettelagt for innsyn i tråd med offentlighetsprinsippet (tilgjengelighet).
- Helsetjenesten skal dokumentere sine tjenester. For opplysninger i pasientjournalssystemet til den kommunale helsetjenesten og legevakten er både tilgjengelighet, integritet og konfidensialitet viktig å ivareta.
- Kommunen skal informere innbyggerne om tjenestene. Informasjon om gjenvinningsstasjonens åpningstider og adgangskontroll har ingen spesielle sikkerhetsbehov, men at informasjonen er tilgjengelig er viktig.

Informasjon behandles stadig oftere digitalt og på nye måter – i IKT/OT-systemer. Det innebærer at beskyttelsesbehovet til informasjonen får konsekvenser for beskyttelsesbehovet til IKT/OT-systemene. Hvis

f. eks et IKT/OT-system skal behandle informasjon med lavt behov for konfidensialitet, men høye krav til integritet og tilgjengelighet, bør systemet settes opp slik at det ivaretar dette konkrete beskyttelsesbehovet. Dersom IKT/OT-systemene behandler informasjon som er kritisk for kommunens tjenester til innbyggere, og bortfall vil medføre risiko for innbyggernes liv og helse, må disse vurderingene av risiko og tiltak knyttes opp mot arbeidet med helhetlig ROS-analyse i kommunen.

Ved vurderingene av hvilke tekniske tiltak som ivaretar det konkrete beskyttelsesbehovet er det viktig å også vurdere tiltak som bygger robuste og motstandsdyktige systemer slik at systemene kan stå imot digitale angrep og om nødvendig relativt enkelt lar seg reetablere. Det er viktig å etablere planer for reetablering av IKT/OT-systemene og gjennomføre jevnlig tester av disse planene.

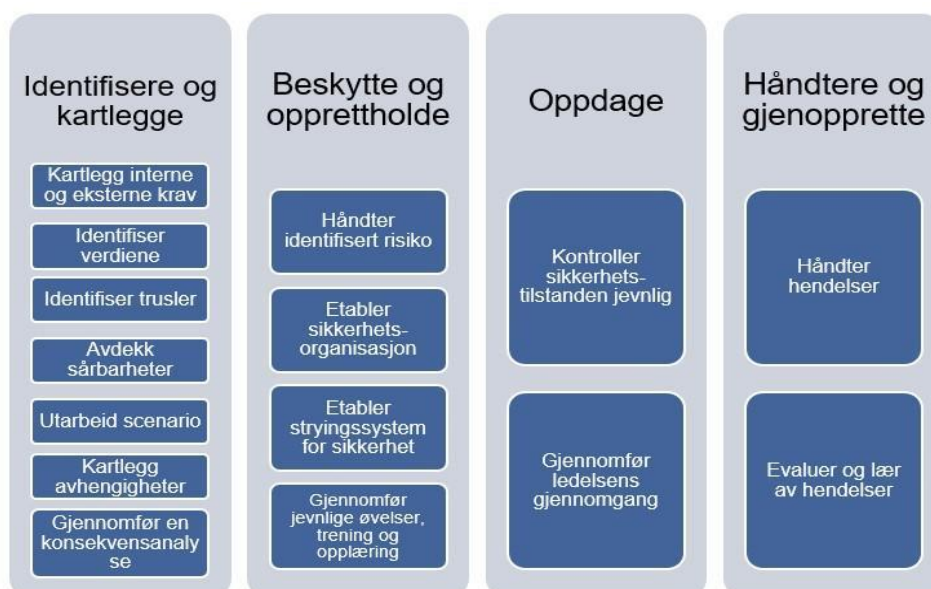


Som pasient har innbyggeren rett til personvern og forsvarlig helsehjelp. Helseopplysninger skal derfor være beskyttet mot uautorisert innsyn, inneholde riktige og komplette opplysninger, samt være tilgjengelig når behovet er der. Pasienten skal også ha innsyn i hvilken informasjon som registreres og hvem som har tilgang.

3.2 Grunnprinsipper for sikkerhetsstyring

Et godt utgangspunkt for sikkerhetsstyring er Nasjonal sikkerhetsmyndighets (NSM) grunnprinsipper og tiltak for sikkerhetsstyring. Disse beskriver hva kommunen kan gjøre for å oppnå og opprettholde et akseptabelt sikkerhetsnivå. Prinsippene er sektorovergripende og aktuelle for alle virksomheter. Hva har du av verdier og hvordan skal du beskytte disse verdiene?.

Grunnprinsippene er delt inn i fire kategorier:



Figur 1 NSMs grunnprinsipper for sikkerhetsstyring

NSM har fire viktige premisser som viktige suksessfaktorer for akseptabel sikkerhet:

- 1) **Virksomhetens leder er ansvarlig for sikkerheten.** Ledelsen skal sette mål og fastlegge prinsipper. Ledelsen skal også sørge for at arbeidet er organisert og blir fulgt opp med kontroll.
- 2) **Sikkerhetsstyringen er en integrert del av virksomheten.** Sørge for at sikkerhetsstyringen er en integrert del av virksomhetsstyringen, slik at sikkerhet blir ivarettatt i hele virksomheten.
- 3) **Det er god risiko- og sikkerhetsforståelse i hele virksomheten.** Bygge sikkerhetskultur, gjennom opplæring og et miljø som har et kontinuerlig forbedringsfokus, samt sørge for at samarbeidspartnere har god risiko- og sikkerhetsforståelse.
- 4) **Det forebyggende sikkerhetsarbeidet er helhetlig.** Helhetlig fokus oppnås når både organisatoriske, elektroniske, fysiske og menneskelige tiltak er kombinert og virker sammen – dette er en kontinuerlig aktivitet og må vurderes i hele verdiens levetid.

Et akseptabelt sikkerhetsnivå oppnås når virksomhetene har identifisert og iverksatt tiltak som reduserer organisatoriske, elektroniske, fysiske og menneskelige sårbarheter.

I vedlegg 2 kan du lese mer om grunnprinsippene for sikkerhetsstyring.

3.3 Hva er personvern?

Personvern er en menneskerettighet knyttet til grunnleggende friheter som privatliv, selvbestemmelse og selvutfoldelse. Personvern handler om menneskets rett til, og ønske om, å ha kontroll på informasjon om seg selv; **hvem vet hva om meg, hva brukes informasjonen til og hvordan brukes den?**

Retten til å vite hva opplysninger brukes til gjelder ovenfor kommunen så vel som ovenfor private virksomheter. Det er viktig at kommunen har kontroll på hvilke plikter som følger med når personopplysninger behandles og hvilke rettigheter innbyggere og ansatte har.

For å være i stand til å ivareta innbyggernes rettigheter etter personvernregelverket er det grunnleggende å ha en god forståelse av de grunnleggende prinsippene for lovlig behandling av personopplysninger, og ikke minst hva en personopplysning er. Utdypende om temaet i vedlegg 3.

3.4 Personvernprinsippene

Personvernforordningen er laget for å sørge for at virksomheter som behandler personopplysninger gjør dette etter at de på forhånd har gjennomført vurderinger av forholdsmessighet og risiko. Kommunen har ansvar for å gjøre disse vurderingene for å ivareta grunnleggende friheter for innbyggere, ansatte og andre som det behandles personopplysninger om. Kommunen må også kunne dokumentere at vurderingene er gjort.

Personvernforordningen er basert på syv grunnleggende prinsipper for behandling av personopplysninger, gjerne kalt «personvernprinsippene». To av prinsippene er det verdt å fremheve spesielt når det gjelder kommunesektoren. Det er prinsippet om lovlighet, rettferdighet og åpenhet og prinsippet om ansvarlighet.

Det første prinsippet fastslår at kommunen må ha et rettslig grunnlag for all behandling av personopplysninger, behandlingen må gjøres i respekt for innbyggere og ansattes rimelige forventninger og kommunen må sørge for åpenhet om hvordan opplysningene blir behandlet. Det er viktig å kunne kommunisere godt og åpent til innbyggerne og ansatte enten det gjelder å få tillatelse til å innhente

personopplysninger (samtykke) eller å informere om måten kommunen behandler personopplysninger ved å tilgjengeliggjøre en personvernerklæring. Andre måter å sørge for åpenhet kan være enten å legge til rette for at det er enkelt å få innsyn i egne opplysninger, eller å få opplysninger korrigert.

Prinsippet om ansvarlighet understreker viktigheten av at kommunens ledelse ikke bare har ansvaret, men er forpliktet til å vise at de tar dette ansvaret. Kommunen skal ved dokumentasjon kunne vise at den har tiltak på plass for å kunne opptre i tråd med regelverket.

“Personvernforordningen er et rammeverk for tillit”

Line Coll, direktør Datatilsynet, Personverndagen 2024

3.5 Informasjon som verdi

All informasjonen kommunen behandler har en verdi. Verdien varierer ut fra typen informasjon og hvilken type virksomhet som behandler informasjonen. Informasjon i denne sammenhengen er alt fra **kunnskap, personopplysninger, forretningshemmeligheter, beregningsmodeller, rutiner, systemoversikter, teknisk infrastruktur, risiko- og sårbarhetsanalyser og så videre.**

Det å kjenne sine verdier er viktig både for å ivareta informasjonssikkerhet og personvern ettersom verdien avgjør hvordan informasjonen skal behandles og beskyttes.

Fra et *informasjonssikkerhetsperspektiv* vurderes beskyttelsesgraden ut ifra hvor viktig informasjonen er for kommunen, og hvordan behovet for konfidensialitet, tilgjengelighet og integritet skal bli ivaretatt.

Et eksempel på informasjon som bør beskyttes er informasjon om vannledningsnett (digitalt, fysisk og styringssystemer). Vannforsyningens betydning for samfunnssikkerheten er av en så høy verdi at informasjon knyttet til denne bør beskyttes på en forsvarlig måte.

Fra et *personvernperspektiv* vurderes informasjon om ansatte og innbyggere ut fra hva slags informasjon som oppleves som privat og hvilken grad av selvbestemmelse de registrerte har over informasjonen. Personopplysninger skiller seg fra kommunens andre informasjonsverdier på den måten at verdien av en personopplysning må sees fra perspektivet til den opplysningen gjelder. Personinformasjon befinner seg på en skala fra det som er definert som særlige kategorier av personopplysninger til opplysninger som det er vanlig at er åpent tilgjengelig. Ulike personer vil likevel kunne ha ulikt perspektiv på hva slags informasjon om oppleves som privat. Kommunen kan for eksempel ikke uten videre beslutte at informasjon om alle innbyggers vannforbruk skal publiseres åpent fordi kommunen anser vannforbruk som lite beskyttelsesverdig informasjon. Vannforbruk kan fortelle mye om en families vaner og døgnrytme som de vil kunne oppleve som privat, og ikke noe enhver skal ha innsikt i. Dette må kommunen ta hensyn til når denne type informasjon forvaltes.

Som nevnt innledningsvis så handler personvern om innbyggere og ansattes rett til privatliv, selvbestemmelse og selvutfoldelse. Sett i sammenheng med personopplysninger som informasjonsverdi hos kommunen så handler personvern om i hvilken grad ansatte og innbyggere selv kan bestemme, eller ha en innflytelse på, hva slags informasjon kommunen skal ha om dem og hvordan den kan brukes.

I tillegg til å være på en skala over grad av sensitivitet så befinner personopplysninger seg altså også på en skala over grad av selvbestemmelse. Denne skalaen spenner fra full selvbestemmelse (samtykke), via bestemmelse via Stortinget som lovgivende forsamling (lovbestemte behandlinger) til behandlinger hvor de

berørte kun får informasjon gjennom oppslag eller annen generell informasjon (berettiget interesse). Kommunen må ha oversikt over på hvilke grunnlag personopplysninger er innhentet og hvilken grad av selvbestemmelse innbygger og ansatt skal ha når det gjelder hvordan opplysningene skal behandles.

«Verdien av en personopplysning må vurderes utfra perspektivet til den opplysningen gjelder»

I figuren under identifiseres forskjellige typer informasjon utfra et informasjonssikkerhetsperspektiv. I figuren foreslår vi en verdi på en skala fra kritisk til lav informasjonsverdi. Kommunen bør selv gjøre en vurdering av hvilke informasjonstyper som skal tilordnes de ulike informasjonsverdiene.

Informasjonsverdi	Eksempel på informasjon
Kritisk verdi	Informasjon som er kritisk for kommunen i en krisesituasjon., f.eks.: - informasjon om, eller som understøtter, samfunnskritiske funksjoner (typisk vannverk, kraftforsyning og vei). - beredskapsplaner, sensitive personopplysninger (inkludert helseopplysninger) og kode 6/7-opplysninger.
Høy verdi	Informasjon som vil være ødeleggende for funksjoner og tjenester som er kritisk for kommunens daglige drift, f.eks.: - strategidokumenter, eksamens- og tentamenoppgaver før de er gitt, - tilbud og protokoller for pågående anskaffelsesprosesser - informasjonssystem for lønnsutbetaling.
Middels verdi	Virksomhetsintern informasjon eller informasjon som kan skade kommunens funksjoner og tjenester i daglig drift, f.eks.: - møtereferater - e-postkommunikasjon mellom ansatte
Lav verdi	Åpen informasjon uten spesielle sikkerhetsbehov, f.eks.: informasjon som ligger åpent på hjemmesiden til kommunen, som for eksempel organisasjonskart.

Figur 2: Eksempler på ulik informasjonsverdi informasjonssikkerhet

Informasjon bør også ses i sammenheng, det vil si at man ser på informasjonen alene og samlet, for å vurdere beskyttelsesbehov. Kommunens ledningsnett for vannforsyning vil samlet utgjøre en betydelig større verdi enn informasjon om enkelte ledningsplasseringer.

God oversikt over informasjonsverdiene gir kommunen et godt grunnlag for å si noe om hvilken informasjon som er mest kritisk for kommunens drift og tjenesteproduksjon.

I figuren under identifiseres forskjellige typer informasjon utfra et personvernperspektiv. I figuren foreslår vi en verdi på en skala fra privat informasjon som innbygger/ansatt bestemmer over selv til informasjon som innbygger/ansatt velger å dele åpent. Også her bør kommunen vurdere hvilke informasjonstyper som skal tilordnes de ulike informasjonsverdiene.

Informasjonsverdi	Eksempel på informasjon	Hva betyr det for kommunen
Høy verdi for innbygger Personlig informasjon med stor grad av selvbestemmelse	Informasjon som enkeltpersoner selv bestemmer over: • Bilder • Kommunikasjon (chat, SMS) • Kontaktliste telefon • Lokasjon / posisjon	Nødvendig med: ☐ system for å kunne gi/trekke samtykke ☐ jevnlig sjekk av om informasjon blir slettet iht. godkjenning gitt av innbygger
Høy verdi for innbygger Personlig informasjon, men mindre grad av selvbestemmelse	Informasjon som forteller mye om våre valg, interesser og daglige liv, men som i mindre grad er frivillig å dele da kommunen har lovhjemmel til å behandle den: • Lønn, økonomi • Karakterer, vurderinger • Personalmappe, elevmappe, pasientjournal • Kommunikasjon mellom elev og skole, hjem/barnehage, institusjon/pasient, kunde/renovasjon • Vannforbruk, avfallshåndtering	Nødvendig med: ☐ utfyllende og tilgjengelig informasjon til innbygger ☐ jevnlig sjekk av at informasjonen ikke blir brukt til andre enn de lovbestemte formålene ☐ bruk til andre formål må dokumenteres
Middels verdi for innbygger Indirekte personlig informasjon Ingen selvbestemmelse Interesseavveining	Informasjon som indirekte kan fortelle mye om våre valg, interesser og daglige liv, men som det ikke er frivillig å dele da andre hensyn veier tyngre – f. eks sikkerhet, arbeidsgivers styringsrett • Logger over aktivitet i systemer • Kameraovervåking	Nødvendig med: ☐ dokumentert interesseavveining ☐ kompensierende tiltak ☐ involvering av representanter for de registrerte ☐ informasjon
Middels verdi for innbygger Informasjon vi selv velger å dele åpent	Åpen informasjon som det er forutsigbart at er tilgjengelig • Informasjon som ligger åpent på nettsider og sosiale medier • Ytringer i media og andre åpne kanaler	Ingen særskilte tiltak

Figur 5: Eksempler på ulike informasjonsverdi personvern

Kommunedirektøren anbefales å:

- Lage en tilsvarende oversikt som i figur 4 og 5 for å prioritere ressurser
- Starte med de mest kritiske verdiene og informasjonen av mest privat karakter

3.6 Informasjonssikkerhet og personopplysningssikkerhet ivaretas gjennom sikkerhetstiltak

For å ivareta krav til informasjonssikkerhet og personopplysningssikkerhet er det vanlig først og fremst å tenke på tekniske sikkerhetstiltak slik som kryptering, tilgangsstyring, passordstyrke og sterk autentisering (slik som multifaktor autentisering), eller utvikling av sikre IKT/OT-systemer. Tekniske sikkerhetstiltak er viktig, men god informasjonssikkerhet og personopplysningssikkerhet er også avhengig av andre typer sikkerhetstiltak, slik som for eksempel gode arbeidsrutiner og sikkerhetsbevissthet hos de ansatte.

Eksempler på forskjellige sikkerhetstiltak:



Tekniske tiltak:	Kryptering, passord, sterk autentisering
Organisatoriske:	Tilgangsstyring, etablere internkontroll
Menneskelige:	Opplæring
Fysisk:	Adgangskontroll til eiendom, bygg og anlegg

3.7 Personvern ivaretas gjennom involvering, medbestemmelse, åpenhet og forutsigbarhet

Personvern er, som nevnt innledningsvis, mer enn personopplysningssikkerhet. Kjernen av personvernet er at offentlige myndigheter ikke skal tilegne seg mer informasjon om innbyggerne enn det som er nødvendig for å kunne tilby tjenester og sikkerhet. Offentlige myndigheter skal heller ikke bruke personopplysninger på måter som vil være i strid med de registrertes forventninger.

For å ivareta krav til personvern er det derfor viktig å ha en klar formening om hvor grensen går for hvor langt inn i privatlivet til innbyggere og ansatte kommunen kan gå. For å få til dette er det mange ganger nødvendig å spørre dem direkte, eller sørge for å ha en gruppe som representerer deres interesser. Det er heller ikke nok å bare lytte til innbyggere og ansatte. Deres meninger skal vektlegges og det bør kunne dokumenteres at deres interesser er ivaretatt i form av konkrete tiltak. Det betyr at kommunen må være beredt til å faktisk gjøre ting på en annen måte enn det som var den opprinnelige planen, som følge av innbyggere og ansattes innvendinger.



Eksempler på tiltak for å sikre personvern

Personvernerklæringer, medbestemmelse/involvering for innbygger/ansatt, åpenhet om grunnlag for beslutninger
redusere risiko for diskriminering, lett tilgjengelige innsynsløsninger

3.8 Ledelse av arbeid med informasjonssikkerhet og personvern

Utover ulike informasjonsverdier og tiltak for å sikre sikkerhet og personvern, er det flere faktorer som spiller en viktig rolle for å bidra til god informasjonssikkerhet og godt personvern.

Ledelse og styring

Arbeidet med informasjonssikkerhet og personvern skal bidra til å realisere kommunens oppgaver og mål – altså virksomhetsstyringen. Kommunens ledelse har derfor et ansvar for å vurdere forholdet og risiko knyttet til informasjonsbehandlingen i de ulike tjenestene kommunen leverer, og følge opp dette.

Lovgivning

Arbeidet med informasjonssikkerhet og personvern skal bidra til å ivareta de lovmessige kravene som kommunen må etterleve. I denne sammenhengen er det lov og krav som regulerer informasjonssikkerhet og personvern.

Risikoforståelse

Kommunen bør gjennomføre risikovurderinger for å få oversikt over mulige uønskede hendelser med uønskede konsekvenser. For disse risikoene skal det identifiseres og iverksettes tiltak som bidrar til å redusere risikoen ned til et akseptabelt nivå slik at innbyggere og ansattes rettigheter ta vare på. En risikobasert tilnærming vil bidra til at sikkerhets- og personvernarbeidet retter fokus mot områder med høyest risiko. Risikoforståelse og aksept av restrisiko er et lederansvar. At aksept av restrisiko besluttes og dokumenteres er avgjørende for å kunne jobbe risikobasert og prioritere tiltak for aktiviteter som innebærer høy risiko.

Avvikshåndtering og gjenoppretting

Fra tid til annen oppstår det hendelser som gjør at IKT/OT- tjenestene er nede og at informasjon som er nødvendig for å gjennomføre ulike aktiviteter, ikke er tilgjengelig. I slike situasjoner er det viktig å ha beredskapsplaner for å kunne gjenopprette normal drift, og planer for å registrere, håndtere, evaluere og følge opp avvik i drift. Beredskapsplanene bør være utformet slik at de bidrar til å ivareta kravene til personvern og informasjonssikkerhet. For eksempel kan en rangering av ulike IKT/OT-systemer etter hvor kritiske de er, gi grunnlag for å mene at f. eks drift av pasientjournalssystemet bør prioriteres foran driften av arkivsystemet.

Menneskelige faktorer

God informasjonssikkerhet og godt personvern er til syvende og sist avhengig av menneskene i organisasjonen. Teknologi, etterlevelse, virksomhetsstyring, risikoforståelse, involvering av ansatte og innbyggere, samt kontinuitet er alle avhengige av menneskenes ferdigheter og kunnskaper.

Kommunens ledelse, fagpersoner for informasjonssikkerhet og personvern og alle ansatte må bidra til at teknologi brukes riktig, prosesser følges, taushetsplikt ivaretas, og avvik knyttet til sikkerhet eller personvern registreres og følges opp. Det er derfor viktig med tilstrekkelig opplæring i alle ledd i kommunen. Råd om hvordan dette kan gjøres i praksis kan du lese i kapittel 6.I kommunens daglige arbeid med informasjonssikkerhet og personvern vektlegges ofte de menneskelige faktorene lavt, og de diskuteres ikke nødvendigvis i risikovurderinger. Kommunens ledelse må sørge for at både risikoer knyttet til utilsiktede feil som følge av ansattes bruk av IKT/OT-systemene reduseres, men også ta høyde for at ansatte kan bevisst utføre uønskede handlinger mot arbeidsgiver knyttet til behandlingene av informasjon.

Kommunedirektøren anbefales å starte med følgende tiltak:

- Skaff oversikt over kommunens informasjonsverdier, samt avhengighetene i og mellom IKT/OT-systemene.
- Skaff kjennskap, forståelse og oversikt over de viktigste risikoene: Uønskede hendelser med størst sannsynlighet for å inntreffe, og med de alvorligste konsekvensene.
- Sikre at personvern og informasjonssikkerhet er en del av kommunens sektorovergripende internkontroll.



Tenk gjennom

- Hvilke informasjonsverdier har min kommune, og hvem bestemmer hva som er høy/lav verdi?
- Hvilke informasjonsverdier er kritiske for å levere de ulike kommunale tjenestene?
- Hvilke personopplysninger om seg selv er det viktig for innbyggerne å ha kontroll over?
- Hva er de viktigste tiltakene vi har etablert for medbestemmelse og åpenhet om behandling av personopplysninger ovenfor innbyggere og ansatte?



Tenk gjennom

- Har vi oversikt over lovene og reglene som regulerer informasjonssikkerhet og personvern i kommunen?
- Hvordan etterlever vi lovkravene?
- Har vi et styringssystem som bidrar til at vi kan etterleve lovens krav?



Tenk gjennom

- Har jeg som kommunedirektør tilstrekkelig risikoforståelse?
- Dekker vår risikovurdering også hendelser med konsekvenser for personvern og informasjonssikkerhet?
- Oppstår det hendelser i kommunen som burde vært med i risikovurderinger?

4. Hvordan oppnå etterlevelse og organisere arbeidet?

Kommuneloven § 25-1 pålegger kommunen at «internkontrollen skal være systematisk», dette gjelder også arbeidet med informasjonssikkerhet og personvern. I tillegg stiller regelverkene som er beskrevet i kapittelet [Relevant lovgivning](#) krav til styringssystem (ledelsessystem) for personvern og informasjonssikkerhet, som en del av kommunens internkontroll.

Arbeidet med personvern og informasjonssikkerhet bør derfor organiseres som en del av kommunens øvrige internkontrollarbeid, og integreres med øvrige kontrollaktiviteter i styringssystemet. Dette skaper en helhetlig internkontroll, effektiviserer og skaper synergier i kontrollarbeidet. Effektiv internkontrollen bidrar til at kommunen kan levere tjenester med høy kvalitet og at lovverk etterleves.

[Internkontrollen](#) skal bidra til at kommunen ivaretar og etterlever beskyttelsesbehovet til informasjon- og personopplysninger og er kommunaldirektørens viktigste verktøy for å styre risiko på personvern- og informasjonssikkerhetsområdet. Ved å vurdere krav i lovverk og gjennom risikostyring, kan kommunen identifisere sikkerhetstiltak som skal inngå i internkontrollen. Det er vesentlig at styringssystemet for personvern og informasjonssikkerhet er godt forankret i ledelsen og har en klar ansvarsfordeling, delegering og beskrivelse av roller. Videre må styringssystemet være systematisk, oversiktlig og fremstå praktisk anvendelig og lett tilgjengelig. Det må også innføres rutiner for regelmessig gjennomgang og revisjon.

Regelverket for informasjonssikkerhet og personvern er teknologinøytralt og risikobasert, noe som medfører at internkontrollen også bør innrettes slik at den er risikobasert.

Arbeid med internkontroll kan ses som en sammenhengende og gjentakende prosess; gjerne i form av en kvalitetssirkel, ref. figuren nedenfor og de kommende avsnitt.

En viktig forutsetning for å lykkes med en velfungerende internkontroll knyttet til informasjonssikkerhet og personvern, er at kommunen har kapasitet til og kompetanse på området. Det er derfor helt nødvendig at kommunedirektøren knytter til seg fagressurser, og sikrer at disse har nødvendig kompetanse og kapasitet til å gjennomføre og bistå i arbeidet. Nødvendig kompetanse kan skaffes på flere måter, men det er viktig å bygge og vedlikeholde kompetansen hos sine egne ansatte. Fagressurser bør være kjente og tilgjengelige for hele kommunen.



Figur 3: Demings sirkel: Plan, Do, Check, Act

Det er viktig å sette av nok tid til arbeidet med internkontroll. Det er også viktig å huske på at som kommunedirektør er det du som har ansvaret. Du bør derfor sikre at fagressursene du knytter til deg har rett kompetanse og kan spille deg god.

Demings sirkel består av fasene planlegge, utføre, kontrollere og korrigere. Gjennomgangen under tar for seg de viktigste elementene i hver fase.

4.1 Planlegge

Hensikten med planleggingsfasen er å etablere internkontrollaktiviteter for å ivareta behov og plikter knyttet til personvern og informasjonssikkerhet.

Planleggingsfasen bør inneholde følgende aktiviteter:

A. Skaffe oversikt over:

- sentrale lover og regler – og ha kunnskap om hvilken betydning de har for kommunen.
- sentrale informasjonsverdier og vurdere deres kritikalitet for kommunens drift og tjenesteproduksjon. Herunder etablere en oversikt over behandling av personopplysninger i kommunen.
- Har vi nødvendig kompetanse i eget hus til å gjennomføre oppgavene?

B. Plassere ansvaret for oppgaver

- Som minimum bør følgende ansvar fordeles og dokumenteres som en del av kommunens eksisterende internkontroll:
 - Informasjonsverdier, kritikalitet og behandlingsprotokoller? Bør det skilles på administrative fellesprosesser og fagområder?
 - Risikovurderinger av ulike behandlinger og teknologiske løsninger?
 - Der det er nødvendig, hvem skal sikre at det gjennomføres personvernkonsekvensvurderinger?
 - Hvem har ansvar for å stille krav til, og følge opp eksterne leverandører?
 - I prosjekter, hvem skal gjennomføre og ivareta oppgavene nevnt over og hvem skal ta over ansvaret når prosjektet er fullført?
 - Hvem er personvernombud og har vi behov for en sikkerhetsleder eller -rådgiver?

C. Gjennomføre risikovurderinger

- For de systemer og behandlinger som er identifisert under punkt A, må kommunen sikre at det blir gjennomført risikovurderinger for sikkerhet og personvern.
- Kommunedirektøren bør som minimum kjenne til resultatet av risikovurderingene og ta stilling til uakseptabel risiko. Der det er identifisert høy risiko må kommunedirektøren sikre at tiltak blir iverksatt, og forsikre seg om at risiko blir redusert.

D. Utarbeide tiltaksplan

Kommunedirektøren må sikre at det blir utarbeidet en tiltaksplan med tilhørende ansvarlige (se punkt B) for de tiltak som skal innføres med bakgrunn i identifiserte plikter (se punkt A) og gjennomførte risikovurderinger (se punkt C). Tiltakene utarbeides i neste fase

4.2 Utføre

Hensikten med utførerfasen er å utforme, innføre og gjennomføre fastsatte internkontrollaktiviteter, som består av rutiner og prosedyrer for når, hvordan og hvem som skal utføre oppgaver..

Som minimum anbefaler vi at kommunen sikrer at følgende er beskrevet og blir ivaretatt:

- Overordnet beskrivelse av kommunens sikkerhetsbehov.
- Utarbeide overordnede styrende dokumenter, herunder et ledelsessystem for informasjonssikkerhet og personvern som blant annet beskriver sikkerhetsmål og strategi.
- Organisering av arbeidet, herunder roller og ansvar for sikkerhet og personvern.
- Hvordan og hvor kommunen skal føre [oversikt over informasjonsverdier](#) og [behandling av personopplysninger](#).
- Sikrer at informasjonssikkerhet og personvern er en del av kommunens [kontinuitets- og beredskapsplan](#).
- Hvordan kommunen skal ivareta personvernet og [de registrertes rettigheter](#):
 - Utarbeide og vedlikeholde en personvernerklæring som gir [informasjon](#) om kommunens behandling av personopplysninger.
 - Forespørsel om [innsyn](#), [retting](#) og [sletting](#) av personopplysninger.
 - Retten til [Dataportabilitet](#) og folks kontroll over egne personopplysninger.
 - Forespørsler om [begrensning](#) i eller [protest](#) mot bruk av personopplysninger.
 - [Rettigheter ved automatiserte avgjørelser](#).
 - Ivaretagelse av [personvernprinsippene](#).
- Hva som skal gjøres ved en [ny behandling av personopplysninger](#) og innføring av nye IKT-systemer.
- Hvordan kommunen skal arbeide med kompetanse og opplæring knyttet til personvern og informasjonssikkerhet, både generelt og på det enkelte fagområdet i kommunen.
- Hvordan kommunens skal jobbe med [tilgangskontroll](#) til systemer og informasjon.
- Når og hvordan det skal gjennomføres [risikovurderinger](#) og [personvernkonsekvensvurderinger](#).
- Hvordan kommunen skal jobbe med drift og utvikling av IKT/OT-systemer for å sikre at disse til enhver tid er [oppdatert](#) og har forsvarlig drift.
- Hvilke krav vi stiller til våre [IKT/OT-systemer og leverandører](#), og hvordan vi følger dem opp.
- Håndtering av avvik knyttet til [personvern](#) og [informasjonssikkerhet](#) som en integrert del i kommunens avvikssystem.

Denne listen er ikke uttømmende, men må ses som et absolutt minimum for hva internkontrollen må inneholde. Med bakgrunn i tiltaksplanen utarbeidet i planleggingsfasen, bør kommunedirektøren få regelmessig informasjon om status på hvilke tiltak som er utarbeidet og implementert.

Digitaliseringsprosjekter

De fleste kommuner jobber aktivt med digitalisering, og innfører jevnlig nye digitale løsninger. Kunnskap om personvern og informasjonssikkerhet er en forutsetning for å sikre trygg digitalisering. Grad av digitalisering og antall prosjekter vil påvirke behovet for kunnskap og kapasitet. Det er derfor viktig å sikre at det stilles krav til sikkerhet og personvern som en integrert del av IKT/OT- og digitaliseringsprosjekter.

Dette kan for eksempel være å:

- Gjennomføre risikovurderinger av nye løsninger.
- Ivareta sikkerhet og personvern i kravspesifikasjoner på et så tidlig tidspunkt som mulig i prosjektgjennomføring.
- Stille riktige og gode krav til leverandører.
- Vurdere tilbudte løsninger når det gjelder personvern og informasjonssikkerhet.
- Gjennomfør personvernkonsekvensutredning hvis løsningen behandler persondata.
- Etablere tilstrekkelige avtaler med leverandør, herunder [tjenestenivåavtaler](#), [databehandleravtaler](#) og eventuelt [sikkerhetsavtaler](#), slik at det kan gjøres god forvaltning.
- Sikre at man også etter innføringen kvalitetssikrer leveranser med tanke på informasjonssikkerhet og personvern.

Som kommunedirektør bør du ikke akseptere innføring av ny teknologi før overnevnte er gjennomført og du er tilstrekkelig opplyst om eventuell risiko.

4.3 Kontrollere

Kontrollaktivitetene skal i hovedsak bidra til å sikre etterlevelse ved å kontrollere at de definerte internkontrollaktiviteter (utføringsdelen) gjennomføres og fungerer som forutsatt. I tillegg skal det også bidra til videreutvikling av internkontrollen gjennom blant annet å:

- Identifisere og følge opp nye eller endrede lovkrav for informasjonssikkerhet og personvern.
- Holde rutiner og instruksjer oppdatert.
- Holde oversikt over informasjonsverdier oppdatert.
- Holde oversikt over behandling av personopplysninger oppdatert.
- Holde risikovurderinger oppdatert på periodisk basis, eller i tråd med endringer i kommunens risikoforståelse.
- Følge opp leverandørs tjenesteleveranser.
- Forvaltnings- eller sikkerhetsrevisjoner av sikkerhets- og personvernområdet.
- Sikre etterlevelse.

Det kan finnes mange ulike kontrollaktiviteter som er godt beskrevet i hoveddokumentet «Orden i eget hus». Eksempler på kontrollaktiviteter på informasjonssikkerhet og personvern finner du under her.

1. [Ledelsens gjennomgang](#)

Ledelsen bør minimum en gang per år gjøre en gjennomgang av personvern og informasjonssikkerhet. På den måten vil du som leder få tilstrekkelig informasjon om status og risiko knyttet til området. Det gjør det enklere å ta avgjørelser om nødvendige tiltak og forbedringer i internkontrollen, type aktiviteter i internkontrollen eller organiseringen av arbeidet med personvern og informasjonssikkerhet.

Til dette arbeidet bør du invitere personer som jobber med fagområdene i kommunen, dvs. informasjonssikkerhetsansvarlig, ansvarlig for personvern i kommunen, personvernombudet etc. Du bør sette opp noen enkle rutiner for hvordan dette møtet skal gjennomføres og hvilke forberedelser og oppfølgingsaktiviteter som forventes etter at møtet er gjennomført.

Typisk agenda for ledelsens gjennomgang:

- Orientering om relevante endringer på rettsområdet.
- Orientering om risiko- og trusselbildet for personvern og informasjonssikkerhet.
- Gjennomgang av vesentlige og/eller alvorlige avviksaker i kommunen siden forrige ledelsens gjennomgang, herunder hvordan disse er håndtert og fulgt opp.
- Gjennomgang av behandlingsaktivitetene (behandlingsprotokoll)
- Overordnet gjennomgang av endringer i risikovurderinger og tiltak som er innført.
- Gjennomgang av oppfølgingen av leverandører.

2. Sikkerhetsrevisjoner

Sikkerhetsrevisjoner vil kontrollere hvordan kommunen tester, analyserer og vurderer effekten av tekniske og organisatoriske sikkerhetstiltak for å beskytte personopplysninger (jfr. personvernforordningen Art. 32.1.d).

For kommunen som behandlingsansvarlig betyr dette å etablere rutiner for å jevnlig vurdere effekten av tekniske og organisatoriske sikkerhetstiltak, dokumentere resultatene og følge opp disse for å justere eller iverksette nye risikoreduserende tiltak. Det innebærer også å utføre sikkerhetsrevisjon av databehandlere og leverandører som har betydning for personopplysningssikkerheten.

3. Forvaltningsrevisjon

Kommunens forvaltningsrevisor kan foreta risikobaserte forvaltningsrevisjoner for å identifisere risiko og avvik, samt bidra til å forbedre gjeldende praksis. Det kan gjennomføres forvaltningsrevisjoner på området personvern og informasjonssikkerhet. På den måten vil du som kommunedirektør få et uavhengig syn på hvordan kommunen jobber med personvern og informasjonssikkerhet.

4.4 Korrigere

Over tid vil arbeidet med informasjonssikkerhet og personvern gjennom utførings- og kontrollfasene gi kommunen erfaringer om og innsikt i hva som fungerer som forutsatt og hva som kan forbedres i informasjonssikkerhets- og personvernarbeidet. Denne fasen skal gi grunnlag for økt kvalitet, effektivisering av rutiner, organisering og på sikt gi økt modenhet.

Grunnlaget for korrigering legges i hovedsak gjennom kontrollaktivitetene. Gjennom kontrollaktivitetene må det være innarbeidet krav om tiltak for oppfølging av svakheter og mangler. Kommunedirektøren må fokusere på oppfølgingen av tiltakene, og passe på at det er klart definert ansvarlige med frister for når tiltak skal være iverksatt. Vi anbefaler at ansvaret for disse tiltakene følger linjen.

Avvik (Forbedringsprosess)

Et spesielt grunnlag for erfaring og læring er [avvik](#) og håndtering av dem. Alle kommuner vil på et tidspunkt oppleve avvik som kan påvirke informasjonssikkerhet og personvern. For å håndtere slike situasjoner bør kommunen ha etablert rutiner for å håndtere avvik og rette eventuelle feil. Det bør også etableres rutiner for å evaluere årsaker og følger av oppståtte avvik. Dette gjøres for å redusere sannsynligheten for at de oppstår igjen, eller for å motvirke negative følger.

Eksempler på særlig alvorlige avvik er:

- Avvik som berører personopplysninger som må meldes til Datatilsynet og/eller til den eller dem som er berørt av avviket.
- Avvik i informasjonssikkerheten som har medført eller kan medføre omfattende tap av informasjon.
- Datalekkasje enten internt eller til eksterne.

4.5 Roller og ansvar

Informasjonssikkerhet og personvern som egne fagområder krever ressurser med definerte roller og ansvar. Kommunens størrelse, egenart, aktiviteter og risikoforhold legger føringer for hvordan rollene ivaretas. Det bør minimum være én dedikert ressurs for informasjonssikkerhet og personvern.

Kommunedirektøren anbefales å sikre at:

- Det gjøres vurderinger av:
 - Årsaken til avviket.
 - Faktiske eller mulige konsekvenser av avviket.
 - Aktuelle tiltak for å forhindre nye avvik.
- Du holdes informert om særlig alvorlige avvik, herunder årsak, konsekvenser og tiltak.
- De som er ansvarlig for sikkerhet og personvern gjennomfører vurderingen av avviket.
- Det settes frister og ansvarlig for lukking av avvik.
 - Ansvar for lukking av avvik innen informasjonssikkerhet og personvern bør følge linjeansvaret.

Informasjonssikkerhetsansvarlig

Kommunen bør ha en ressurs som har nødvendig kunnskap om informasjonssikkerhet og som derfor kan etablere og følge opp internkontroll for fagområdet. Den slik ressurs omtales gjerne som enten informasjonssikkerhetsansvarlig, CISO (Chief Information Security Officer) eller rådgiver for informasjonssikkerhet. Denne medarbeideren vil typisk har følgende oppgaver:

- Rapportere til kommunedirektøren for å ivareta behov for styring og fagkompetanse på informasjonssikkerhetsområdet.
- Rapportere til sikkerhetsansvarlig eller Chief Security Officer (CSO).

- Etablere og vedlikeholde prinsipper og rutiner gjennom et styringssystem for informasjonssikkerhet.
- Bidra til at det gjennomføres helhetlig informasjonssikkerhet i organisasjonen.
- Ha ansvar for rådgivning og opplæring i informasjonssikkerhet internt, og bidra til å bygge en god digital sikkerhetskultur
- Påse at internkontrollaktiviteter for informasjonssikkerhet følges opp i digitaliseringsprosjekter, anskaffelser og i daglig drift. Ansvar for å følge opp avvik på informasjonssikkerhetsområdet ligger også gjerne hos informasjonssikkerhetsansvarlig.

Det er viktig å skille mellom rollene sikkerhetsansvarlig (CSO) og informasjonssikkerhetsansvarlig (CISO). – Sikkerhetsansvarlig (CSO) vil typisk være kommunedirektør, eller den hen har delegert fullmakt til for oppfølging/koordinering av hele sikkerhetsområdet. Det vil si både personellsikkerhet, fysisk sikkerhet og informasjonssikkerhet. Sikkerhetsansvarlig er også et begrep som brukes av NSM i forbindelse med sikkerhetsloven, og hvor denne rollen også vil ha ansvar for håndtering av sikkerhetsklareringer m.m.

Informasjonssikkerhetsansvarligs (CISO) ansvarsområde er avgrenset til informasjonssikkerhet og denne rollen kan typisk rapportere til CSO som har et mer overordnet ansvar.

Personvernombud

Som offentlig virksomhet plikter kommuner å ha personvernombud. Denne rollen skal være faglig uavhengig, og rollen skal organiseres på en måte som gjør at den ikke bestemmer hvorfor og/eller hvordan personopplysninger skal behandles. Dette innebærer at kommuner bør sikre tilstrekkelig kompetanse innen personvern til å kunne vurdere personvernombudets råd på en selvstendig måte.

Personvernforordningen fastslår at de registrerte (alle nåværende og tidligere ansatte og innbyggere i kommunen) kan kontakte personvernombudet dersom de har spørsmål om behandlingen av personopplysninger og utøvelsen av sine rettigheter og friheter på dette området. Dette er med på å gjøre oppgavene omfattende og krever at personvernombudet har tilstrekkelige ressurser, kompetanse og personlige egenskaper for å fungere på en god måte. Ombudet skal veilede kommunens tjenesteområder og ansatte, slik at personopplysninger blir behandlet på en god måte og i tråd med regelverket.

Personvernombudet skal blant annet:

- Informere og gi råd til kommunens tjenesteområder og ansatte om de forpliktelsene kommunen har etter personvernlovgivningen.
- Kontrollere at kommunen overholder personvernforordningen og andre relevante regelverk med personvernbestemmelser.
- Bidra til håndtering av avvik i behandling av personopplysninger.
- Samarbeide med og fungere som kontaktpunkt for Datatilsynet.
- Hjelp innbyggerne med spørsmål om deres personopplysninger.
- Råd og veiledning ved gjennomføring av personvernkonsekvensvurdering.

4.6 Sikkerhetskultur

Organisasjonens sikkerhetskultur er summen av de ansattes kunnskap, motivasjon, holdninger og adferd som kommer til uttrykk gjennom virksomhetens totale ivaretagelse av informasjonssikkerhet og personvern. En viktig forutsetning for å bygge en kultur hvor informasjonssikkerhet og personvern ivaretas er «tonen på

toppen». Kommunedirektøren og kommunens øvrige ledelse bør derfor sette temaet på kommunens agenda, og være gode forbilder gjennom det man sier og gjør.

”

Hvorfor skal de ansatte bry seg om internkontroll, personvern og informasjonssikkerhet dersom kommunedirektøren og ledelsen ikke bryr seg?

Kommunedirektøren **må**:

- ha et styringssystem for informasjonssikkerhet og personvern som beskriver hvordan kommunen skal etterleve informasjonssikkerhet og personvern, og hvilket ansvar den ansatte selv har.

Kommunedirektøren **anbefales** å:

- benytte seg av fagressurser i kommunen for å sette seg inn i de viktigste risikoene kommunen har, og i tillegg være godt orientert om sentrale bestemmelser for personvern og informasjonssikkerhet.
- inkludere informasjonssikkerhet og personvern i den sektorovergripende internkontrollen og påse at beslutninger om sikkerhetstiltak etterleves.
- ha et opplæringsprogram hvor alle ansatte bevisstgjøres på hvordan kommunen skal ivareta god informasjonssikkert og godt personvern, og hva dette betyr for den enkelte. Kunnskap er ferskvare og opplæringen bør tilpasses den enkeltes stilling.
- inkludere personvern og informasjonssikkerhet i internkontrollrapportering til folkevalgte organer.
- ha en synlig profil og fremme informasjonssikkerhet og personvern i intern kommunikasjon.
- være nysgjerrig og stille spørsmål om informasjonssikkerhet og personvern til egne fagressurser, til egen ledergruppe og til de som har ansvaret for gjennomføring av IT- eller digitaliseringsprosjekter.



Tenk gjennom

- Har vi som kommune tilstrekkelig kontroll på informasjonssikkerhet- og personvernområdet?
- Har vi etablert internkontroll på området, og fungerer den etter sin hensikt?
- Har vi klare og tydelige definerte roller og ansvar på området?

VEDLEGG

Vedlegg 1 Regelverket

Vedlegg 2 Grunnprinsipper for sikkerhetsstyring

Vedlegg 3 Grunnprinsipper for behandling av personopplysninger

Vedlegg 4 Tjenesteutsetting

Vedlegg 5 Sjekklistor

Vedlegg 6 Definisjoner og nasjonale ressurser personvern og informasjonssikkerhet

Vedlegg 7 Kunstig intelligens

Vedlegg 8 Mal Nødplakat (fylles ut/ferdigstilles av den enkelte kommune)