Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet

Et tillegg til Kommunedirektørens internkontroll – Orden i eget hus

Innhold

Figuroversikt

INNLEDNING

Samfunnet digitaliseres i stadig større grad og bruken av teknologi er økende. Det kan gi store gevinster og muligheter, men kan også føre til nye typer risiko. Digitale «innbrudd» kan få alvorlige konsekvenser for kommunens tjenesteproduksjon, lede til driftsavbrudd, tap av kritisk informasjon og i forlengelsen økonomiske tap. Enkeltpersoner kan også rammes hardt og få sine liv snudd opp ned som en følge av for eksempel identitetstyveri. Evnen til å forstå og håndtere digitale risikoer er viktig for å kunne ivareta god informasjonssikkerhet og godt personvern. Slik kan lover og regler etterleves og tjenester leveres med god kvalitet.

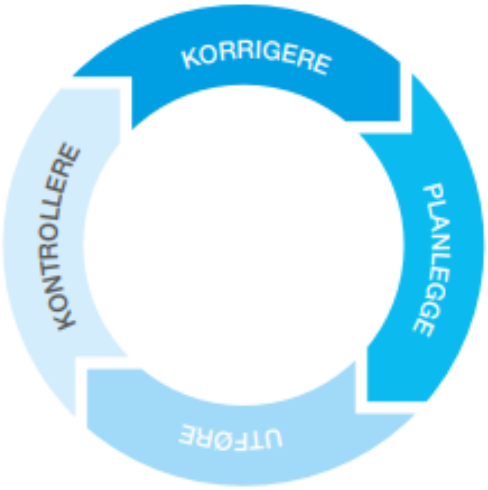
Kommuner behandler svært mange personopplysninger om innbyggere og ansatte, og mange av disse personopplysningene er av sensitiv karakter. I tillegg har kommuner en rekke samfunnskritiske oppgaver hvor det å ivareta informasjonsbehov og -beskyttelse har stor betydning. Økt digitalisering innebærer økt avhengighet av teknologiske løsninger. Teknologien må fungere for at kommunen skal kunne levere tjenester til innbyggerne. Leverandørkjeder blir også stadig mer komplekse. Det stiller krav til gode rutiner for oppfølging og kontroll.

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

1. Hvordan bruke verktøykassen?

Denne verktøykassen skal gjøre det enklere for deg som kommunedirektør å gjennomføre internkontroll på området personvern og informasjonssikkerhet. Den skal bidra til etterlevelse av lover og regler, samt at tjenester leveres med rett kvalitet og god ressursbruk. Verktøykassen tar utgangspunkt i *Orden i eget hus – Kommunedirektørens internkontroll*, og kan leses 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 ditt ansvar innenfor personvern og informasjonssikkerhet. Den tar for seg informasjonssikkerhet generelt, ikke kun knyttet opp mot personvern. Videre skal den gi toppledere i kommunal sektor veiledning for å skaffe seg kontroll, og opprettholde denne kontrollen over tid. Kapittel 2-5 kan ses på som kapitler for å øke din kunnskap til fagområdet. Kapittel 6 skisserer en modell for internkontroll bygd på Demmings sirkel. Kapittelet skal gi deg som kommunedirektør konkrete råd, kontrollspørsmål og innspill til aktiviteter for å kunne utøve ditt lederansvar. Kunnskap som gis i kapittel 2-5 vil altså være grunnlaget for kapittel 6.



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

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 søker også å komme med anbefalinger og råd til kommunedirektøren.

Helt til slutt i verktøykassen er det en oversikt over relevante offentlige virksomheter hvor man kan søke råd. Enkeltord vil ikke alltid forklares fortløpende i verktøykassen, men vil finnes i definisjonslisten nederst i dokumentet.

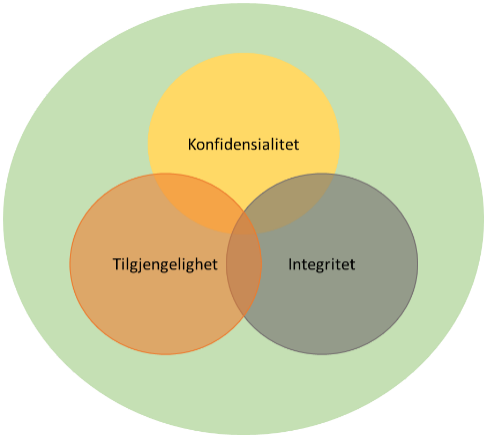
Verktøykassen er utarbeidet for toppledere, og vi anbefaler deg som kommunedirektører å lese hele dokumentet.

2. Om informasjonssikkerhet og personvern

2.1 HVA ER INFORMASJONSSIKKERHET?

Informasjonssikkerhet handler om å verne alle typer 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.



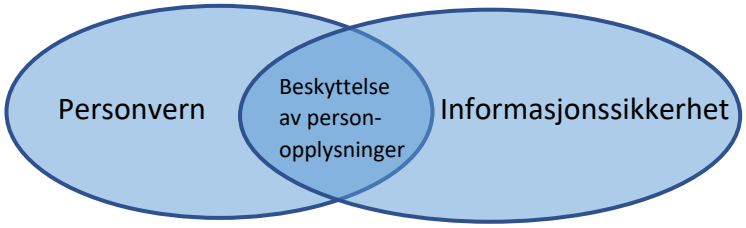
Figur 2: Konfidensialitet, integritet og tilgjengelighet

Noen eksempler på informasjon med ulike beskyttelsesbehov:

- For opplysninger knyttet til skjermet adresse er typisk vern mot uautorisert innsyn svært viktig å ivareta.
- For dokumentasjon i arkivsystemet vil det være viktig at opplysningene er sikret mot utilsiktet endring.
- For opplysninger i pasientjournalsystemet til den kommunale legevakten er både tilgjengelighet og konfidensialitet viktig å ivareta.
- Informasjon om gjenvinningsstasjonens åpningstider har ingen spesielle sikkerhetsbehov, men tilgjengelighet til informasjonen er viktig.

Informasjon behandles stadig oftere digitalt og på nye måter – i IKT-systemer. Det innebærer at beskyttelsesbehovet til informasjonen får konsekvenser for beskyttelsesbehovet til IKT-systemene. Skal IKT-systemet behandle informasjon med lavt behov for konfidensialitet, men høye krav til integritet og tilgjengelighet bør systemet settes opp slik at det ivaretar dette beskyttelsesbehovet.

Personopplysninger er en type informasjon som skal beskyttes. Personvernforordningen (GDPR) har dreid fokuset til informasjonssikkerhet noe over mot sikkerhet for personopplysninger. Informasjonssikkerhet er imidlertid mer enn personvern, på samme måte som personvern er mer enn informasjonssikkerhet. Personvern og informasjonssikkerhet overlapper når det gjelder beskyttelsen av personopplysninger. Forholdet mellom fagområdene kan forklares ved bruk av figuren under.



Figur 3: Figuren forklarer sammenhengen mellom informasjonssikkerhet og personvern. Det er to ulikefagområder, men overlapper hva gjelder beskyttelse av personopplysninger.

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.

2.1.1 INFORMASJONSVERDI

All informasjonen kommunen eier og behandler har en verdi. Verdien varierer ut fra typen informasjon og hvilken type virksomhet informasjonen tilhører. Informasjon i denne sammenhengen er alt fra kunnskap, personopplysninger, forretningshemmeligheter, beregningsmodeller, informasjon om hvordan saksbehandlingen skal gjennomføres, IKT-systemer hvor informasjon blir behandlet, teknisk infrastruktur mv. Det å kjenne sine verdier er viktig i informasjonssikkerhetssammenheng, ettersom det avgjør hvordan den skal beskyttes. Beskyttelsesgraden vurderes ut ifra hvor viktig informasjonen er, og hvordan behovet for konfidensialitet, tilgjengelighet og integritet skal bli ivaretatt.

Undervisningsmateriell er svært viktig, og dermed av stor verdi, for den lovpålagte plikten kommunen har til å gi opplæring.

Eksempel: Undervisningsmateriell er viktig, og nødvendig, for å gi opplæring, slik kommunen er forpliktet til å gjøre. Covid-19 og hjemmeundervisning har vist hvor viktig det er at undervisningsmateriellet er tilgjengelig på digitale plattformer for både elever og lærere. Om uvedkommende får tilgang til undervisningsmaterialet vil det ikke nødvendigvis føre til tap av verdien. For undervisningsmaterialets verdi er tilgjengelighet viktig og kommunen bør fokusere på at IKT-systemet hvor undervisningsmateriellet lagres har minimal «nedetid».

Det er ikke bare informasjon som er omfattet av nasjonale regelverk som har en verdi for kommunen. Informasjon om vannledningsnettet (digitalt, fysisk og for styringssystemer) er et eksempel. Selv om dette kanskje ikke dekkes av sikkerhetsloven, er vannforsyningens betydning for samfunnssikkerheten av en så høy verdi at den likevel bør beskyttes på en forsvarlig måte.

I figuren under identifiseres forskjellige typer informasjon. Disse er gitt en tenkt informasjonsverdi. I realiteten vil informasjonens verdi avhenge av kommunens egen vurdering.

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.: • læringsplattformen for kommunikasjon mellom elev og skole. • informasjon som er unntatt offentligheten.
Lav verdi	Åpen informasjon uten spesielle sikkerhetsbehov, f.eks.: • informasjon som ligger åpent på hjemmesiden til kommunen, som for eksempel organisasjonskart.

Figur 4: Eksempler på ulik informasjonsverdi

Informasjon bør også ses i sammenheng, dvs. 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 godt grunnlag for å si noe om hvilken informasjon som er mest kritisk for kommunens drift og tjenesteproduksjon.

Kommunedirektøren anbefales å:

- **Lage en tilsvarende oversikt som i figur 4 for å prioritere ressurser**
- **Starte med de mest kritiske verdiene først**

2.2 HVA ER PERSONVERN?

Personopplysninger er enhver opplysning om en identifiserbar eller identifisert person. Personvernet skal bidra til å verne om personopplysninger og er knyttet til enkeltindividets rett til privatliv, selvbestemmelse og selvutfoldelse. Viktige elementer i personvernet er at den enkelte skal ha kontroll over, og i størst mulig grad kunne bestemme over egne personopplysninger. Dette omtales ofte som personopplysningsvern. Personvernforordningen er laget for å beskytte personopplysninger. For å opprettholde godt personvern kreves det at informasjonssikkerheten ivaretas og at man gjør fornuftige vurderinger om hvilke personopplysninger man trenger å behandle og over hvilket tidsrom, samt å kunne kommunisere godt og åpent til innbyggerne.

Personvernforordningen stiller krav til personvernet som kommunen må etterleve. Det gjelder blant annet innbyggernes rett til å få innsyn i personopplysninger om seg selv, og å kreve opplysninger rettet. Videre

handler det om å ivareta personvernprinsippene, som skal sikre enkeltindividets privatliv, selvbestemmelse og selvutfoldelse.

2.3 INFORMASJONSSIKKERHET OG PERSONVERN IVARETAS GJENNOM ULIKE SIKKERHETSTILTAK

For å ivareta krav til informasjonssikkerhet og personvern tenker vi ofte på bruken av tekniske sikkerhetstiltak slik som kryptering, tilgangsstyring, passordstyrke eller utvikling av sikre IKT-systemer. Tekniske sikkerhetstiltak er viktig, men god informasjonssikkerhet og godt personvern er også avhengig av andre typer sikkerhetstiltak, slik som gode arbeidsrutiner og sikkerhetsbevissthet hos de ansatte.

Eksempler på forskjellige sikkerhetstiltak:

Tekniske tiltak: Kryptering, passord

Organisatoriske: Tilgangsstyring, etablere internkontroll

Menneskelige: Opplæring

Fysisk: Adgangskontroll til eiendom, bygg og anlegg

2.4 ANDRE HENSYN KNYTTET TIL INFORMASJONSSIKKERHET OG PERSONVERN

Utover informasjonstyper, ulike informasjonsverdier og sikkerhetstiltak 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 målsetninger – virksomhetsstyringen. Kommunens ledelse har derfor et ansvar for å vurdere beskyttelsesbehov knyttet til 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 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 sikkerhetstiltak som bidrar til å redusere risikoen ned til et akseptabelt nivå slik at beskyttelsesbehovet til informasjon og personopplysninger ivaretas. En risikobasert tilnærming vil bidra til at sikkerhets- og personvernarbeidet retter fokus mot områder med høyest risiko.

Avvikshåndtering og gjenopprettelse av IT-drift. Fra tid til annen oppstår det hendelser som gjør at IKT-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-systemers etter hvor kritisk de er tilsi at et drift av pasientjournalsystemet bør prioriteres foran driften av arkivsystemet.

Menneskelige faktorer. God informasjonssikkerhet og personvern er til syvende og sist avhengig av menneskene i organisasjonen. Teknologi, etterlevelse, virksomhetsstyring, risikovurderinger og kontinuitet er alle avhengige av menneskenes ferdigheter og kunnskaper. Kommunens ledelse, fagpersoner for informasjonssikkerhet og personvern, IT-ansatte og alle andre ansatte må bidra til at teknologien brukes riktig, prosesser følges, taushetsplikt ivaretas, og avvik i 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.

Tenk gjennom

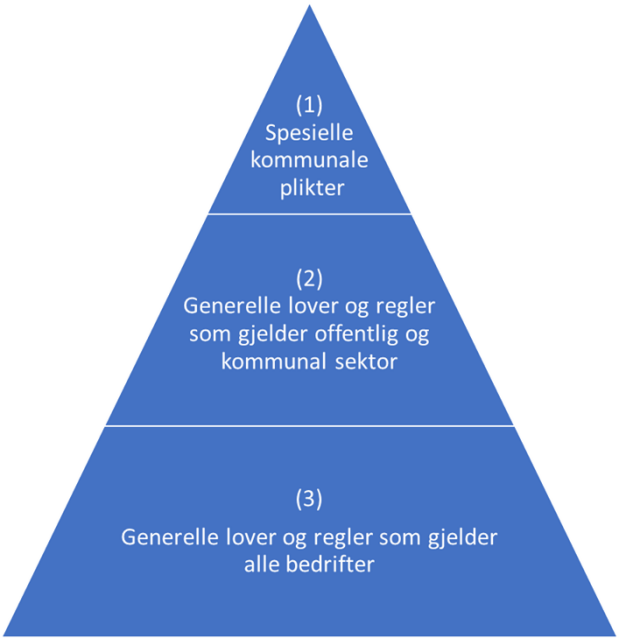
- Hvilke informasjonsverdier har min kommune?
- Hvilke informasjonsverdier er kritiske for å levere de ulike kommunale tjenestene?
- Hva er de viktigste sikkerhetstiltakene vi har etablert?
- Har vi nok fokus på personvern og informasjonssikkerhet i hele kommunen?

3. Relevant lovgivning

Personopplysningsloven, sikkerhetsloven og eForvaltningsforskriften er sektorovergripende lover og forskrifter som regulerer personvern og informasjonssikkerhet, og som gjelder for kommunal sektor. I tillegg til sektorovergripende lovgivning, finnes det også sektorspesifikk lovgivning som regulerer personvern og informasjonssikkerhet spesifikt. Dette gjelder for eksempel særlig helselovgivningen.

Etterlevelsen av regelverkene bør inngå i den sektorovergripende internkontrollen som er beskrevet i kapittel 5 i *Orden i eget hus*, for eksempel under «reglement for datasikkerhet og personvern».

Regelverkene som regulerer personvern og informasjonssikkerhet må ses i sammenheng med andre regelverk. Figur 5 viser hvordan generelle lover og regler gjelder for alle bedrifter, og for kommuner. Personopplysningsloven er en generell lov, som kan plasseres i (3) i figuren. Sikkerhetsloven og eForvaltningsforskriften er regler i (2) som er generelle og gjelder for offentlig og kommunal sektor. Disse gjelder ved siden av personopplysningsloven, med mindre annet er spesifisert i regelverket i (2). Norske kommuner må ta hensyn til personvern og informasjonssikkerhet i utøvelse av kommunale oppgaver, som for eksempel i barnevern, oppvekst, sosialtjenester, helse og omsorg, som kan plasseres i (1) i figuren. De generelle pliktene til personvern og informasjonssikkerhet gjelder også ved siden av andre generelle plikter, det vil si at de også gjelder i den generelle saksbehandlingen (etter forvaltningsloven) og arkiveringen som skjer i kommunen, (2) i figuren.



Figur 5: Generelle og spesielle lover og regler

I dette kapittelet redegjøres kort for lover og forskrifter som regulerer de generelle kravene til personvern og informasjonssikkerhet. Hvordan du som kommunedirektør skal gå frem for å etterleve regelverket finner du veiledning om i kapittel 6.

3.1 KORT OM PERSONOPPLYSNINGSLOVEN

Personopplysningsloven, hvor personvernforordningen - PVF (på engelsk GDPR) er innlemmet, regulerer behandling av personopplysninger. Personopplysninger er opplysninger eller vurderinger som kan knyttes til en identifiserbar eller identifisert person. Det er altså nok at opplysningene kan knyttes til en person som kan identifiseres. Eksempler på personopplysninger er IP-adresse, telefonnummer, navn, adresse, fingeravtrykk og bilder. Enkelte typer opplysninger som krever ekstra vern, kalles særlige kategorier av personopplysninger. Slike personopplysninger er opplysninger om, eller som kan avsløre,

- religion,
- seksualitet,
- fagforeningsmedlemskap,
- politisk og filosofisk overbevisning

- rasemessig eller etnisk opprinnelse,
- genetiske og biometriske opplysninger
- helseopplysninger.

Opplysninger om straffedommer og lovovertredelser regnes ikke som særlige kategorier av personopplysninger, men er likevel underlagt visse begrensninger i personvernforordningen. Dette innebærer blant annet at behandling av slike opplysninger kun kan skje med hjemmel i lov eller under en offentlig myndighets kontroll.

Personopplysningsloven stiller en rekke krav til virksomheter som ønsker å behandle personopplysninger. I regelverket blir det påpekt at barn og unge fortjener et særlig vern av sine personopplysninger. Kommunen bør derfor tenke ekstra nøye igjennom hvilke opplysninger som behandles om barn og unge, samt hvordan disse opplysningene behandles.

3.1.1 Overordnede krav

Alle virksomheter som ønsker å behandle personopplysninger er underlagt personopplysningsloven. Listen nedenfor trekker frem noen av kravene som gjelder:

- All bruk av personopplysninger skal ha et formål og et lovlig behandlingsgrunnlag (PVF art. 5 og 6).
- Kommuner skal gi innbyggerne informasjon om hvordan personopplysninger behandles – Overordnet informasjon gis ofte i en personvernerklæring (PVF art. 13 og 14).
- Som offentlig myndighet plikter kommuner å ha et personvernombud (PVF art. 37).
- Kommuner skal gjennomføre risikovurderinger for behandlinger (PVF art. 32).
- Der det er nødvendig, skal kommunen vurdere personvernkonsekvensvurderingene (DPIA) ved behandlingen og eventuelt kontakte Datatilsynet for forhåndsdrøftelse ved høy risiko for de registrertes rettigheter og friheter (PVF art. 35 og 36).
- All behandling av personopplysninger skal føres i en egen oversikt (behandlingsprotokoll) (PVF art. 30).
- I tilfeller hvor kommunen sammen med andre, for eksempel et statlig organ, bestemmer formål og virkemidler for behandlingen av personopplysninger, skal det inngås avtale om felles behandlingsansvar (PVF art. 26).
- I tilfeller hvor kommuner bruker eksterne leverandører, som behandler personopplysninger på vegne av kommunen, skal det inngås databehandleravtale (PVF art. 28).
- Brudd på personopplysningssikkerheten skal meldes Datatilsynet innen 72 timer (PVF art. 33).
    - I tilfeller hvor det er fare for høy risiko, dvs. når risikoen er større enn normalt, for de berørtes rettigheter, skal disse også kontaktes (PVF art. 34).
- Overføres personopplysninger utenfor EØS, skal det iverksettes tilstrekkelige beskyttelsestiltak (PVF kapittel V).
- Kommunen skal ha et internkontrollsystem som sikrer at alle pliktene i personvernregelverket etterleves (PVF art 24).

3.2 KORT OM SIKKERHETSLOVEN

Sikkerhetsloven gjelder for alle fylkeskommuner og kommuner og skal beskytte nasjonal suverenitet, territoriell integritet og demokratiske styreformer og andre nasjonale sikkerhetsinteresser mot

sikkerhetstruende virksomhet (tilsiktede handlinger som direkte eller indirekte kan skade nasjonale sikkerhetsinteresser). Loven skal altså beskytte nasjonal sikkerhet, og det må derfor skilles på nasjonal sikkerhet og samfunnssikkerhet. Kun førstnevnte faller inn under sikkerhetsloven. Loven med tilhørende forskrifter stiller krav til sikkerhetsstyring og forsvarlig sikkerhetsnivå for skjermingsverdige verdier, dvs.

- skjermingsverdig informasjon,
- skjermingsverdige informasjonssystemer, og
- skjermingsverdige objekter og infrastruktur.

Kommunedirektøren må sikre god sikkerhetsstyring, dvs. sikre at det blir gjennomført planlagte og systematiske aktiviteter som omfatter planlegging, utførelse, kontroll og korrigering av arbeidet med sikkerhetsloven og sikkerheten i kommunen (internkontroll). For å kunne gjøre dette på best mulig måte, må du være kjent med hvilke verdier kommunen besitter og hvilke risikoer som gjør seg gjeldende.

3.2.1 Overordnede krav

Sikkerhetslovens krav om sikkerhetsstyring gjelder uavhengig av om kommunen har skjermingsverdige verdier. Alle kommuner må derfor sikre at forebyggende sikkerhetsarbeid inngår som en del av kommunens styringssystem. Det innebærer blant annet å:

- Gjennomføre risikovurderinger og iverksette tiltak for å sikre et forsvarlig sikkerhetsnivå.
- Sikre tilstrekkelig kompetanse og ressurser for å kunne gjennomføre forebyggende sikkerhetsarbeid.
- Vurdere om kommunen har skjermingsverdige verdier som faller inn under loven.
    - Eventuelt iverksette tiltak for å sikre disse verdiene.

3.3 KORT OM EFORVALTNINGSFORSKRIFTEN OG DENS KRAV

Forskriften gjelder kommunal sektor og stiller krav til internkontroll på informasjonssikkerhetsområdet i § 15, samt at virksomhetene bør basere seg på anerkjente standarder for styring av informasjonssikkerhet. Formålet med forskriften er å legge til rette for sikker og effektiv bruk av elektronisk kommunikasjon i kommunene og med forvaltningen. Internkontroll på informasjonssikkerhetsområdet bør være en integrert del av virksomhetens helhetlige internkontroll og styringssystem. I tillegg skal virksomheten fastsette sikkerhetsmål og sikkerhetsstrategi, som skal ta opp i seg relevante krav som er fastsatt i annen lov og forskrift. Forskriften tar også opp i seg andre krav til personvern og informasjonssikkerhet.

3.4 HELHETLIG TILNÆRMING

De relevante lovene og forskriften som er omtalt over er risikobasert og er i noen grad overlappende hva gjelder personvern og informasjonssikkerhet. Vi anbefaler derfor at kommunen har en helhetlig tilnærming til personvern og informasjonssikkerhet.

Det er kommunedirektøren som har det øverste ansvaret for at kravene i personopplysningsloven, sikkerhetsloven og eForvaltningsforskriften etterleves i hele kommunen.

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?

4. Risikoforståelse

Forståelse av risiko, dvs. hvilke uønskede hendelser kommunen kan stå overfor og hvilke konsekvenser disse kan få for kommunen, er viktig. Dagens risikobilde er ofte komplekst, særlig når avhengigheter mellom tjenester, støtteprosesser og ulike IKT-systemer og leverandører tas i betraktning. Avhengighetene gjør eventuelle uønskede hendelser komplekse å forstå, avverge og håndtere. Slike uønskede hendelsene kan oppstå i et IKT-system, hos egen IT-avdeling eller hos leverandør og kan medføre driftsavbrudd for andre IKT-systemer.

Kommunens sakssystem for byggesaksbehandling blir utsatt for et løsepengevirus og data i pågående saker låses ned med den konsekvens at kommunen ikke er i stand til å overholde lovpålagte frister for byggesaksbehandling.

Risiko er ikke statisk og vil endre seg over tid, blant annet i takt med:

- Iverksetting av sikkerhetstiltak og hvordan tekniske, organisatoriske og menneskelige sikkerhetstiltak samvirker.
- Læring fra sikkerhetshendelser (hackerangrep mv.) fra egen eller annen kommune, eller annen offentlig og privat virksomhet i inn- og utland.
- Feil og suksesser.
- Anvendelse av ny teknologi.
- Utvikling av arbeidsmetoder.
- Endringer i lover og regler.
- Sektorovergripende internkontrollaktiviteter.

En uønsket hendelse vil ha større konsekvenser om informasjon med høy verdi er involvert – det vil si at det er en høyere iboende risiko knyttet til behandling av en bestemt type informasjon. For eksempel vil det ha større konsekvenser om det er innbyggernes helseopplysninger som berøres, enn om det er telefonnummer som enkelt kan finnes på et nettsted. Det vil derfor være større behov for å ivareta informasjonssikkerhet og personvern knyttet til helseopplysninger, og sikkerhetstiltakene vil derfor gjerne være flere eller strengere.

Kommunen bør ha oppdatert innsikt i overordnede trender og utviklingen i kommunens risikobilde. Fagpersoner på informasjonssikkerhets- og personvernområdet bør ha i oppgave å ivareta denne type risikovurderinger.

Kommunedirektøren anbefales å ha fokus på:

- **Risikoene som berører særskilte kategorier personopplysninger eller særlig sårbare personer. For eksempel:**
  - **Helse- og omsorgstjenester for eldre**
  - **Helsestasjon for ungdom**
  - **Barnevernet**
  - **Tannhelse**
  - **Skole og barnehager**
- **Informasjon, personopplysninger eller IKT-systemer med høyest verdi for drift og tjenesteproduksjon. For eksempel:**
  - **Informasjon om vannforsyning og avløp**
  - **Informasjon om veier og broer**
  - **Risikovurderinger**
  - **Beredskapsplaner**
- **De sikkerhets- eller personvernmessige hendelser som kan medføre konsekvenser som at drift og tjenesteproduksjon ikke lar seg gjennomføre, eller med sterkt redusert kvalitet, dvs. de høyeste risikoene.**
  - **Nedetid for IKT-systemer som er kritiske for tjenesteproduksjon, for eksempel pasientjournal, saksbehandlingssystem for barnevern eller læringsplattformer.**

Uønskede hendelser kan påvirke hvordan krav til tilgjengelighet, integritet og konfidensialitet er ivaretatt. I tillegg kan uønskede hendelser berøre personopplysninger og ha betydning for innbyggeres eller ansattes rett til personvern. **Noen eksempler på uønskede hendelser:**

Scenarier

Alle IT-tjenester i helse og omsorg stopper opp i kommunen som følge av en brann som ødelegger datasenteret hvor kommunens servere driftes fra. Det tar 14 dager å sette opp et nytt datasenter. Rom må gjøres klar, utstyr kjøpes inn og IKT-systemene må konfigureres. Da backup skal hentes frem viser det seg at data fra de siste 14 dager før brannen har gått tapt fordi backupene har vært oppbevart i samme bygg som datasenteret før de har blitt sendt til sikker oppbevaring. Det fører til at kommunen ikke har fullstendige pasientopplysninger og en pasient blir alvorlig syk fordi informasjon om endringer i helsetilstanden har gått tapt.

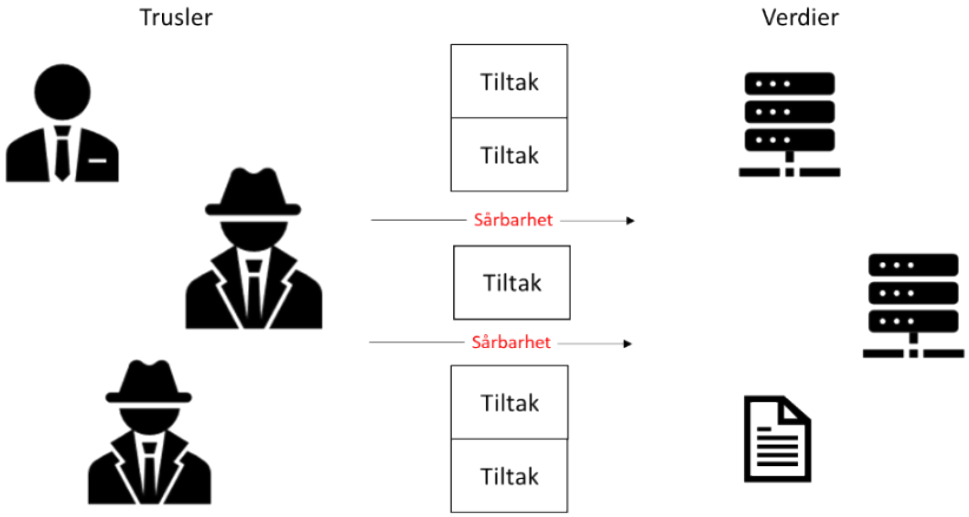
Det gjennomføres et hackerangrep mot skolene som fører til at personopplysninger om enkelte elever spres. En undersøkelse viser at sikkerhetskravene til pålogging har vært svake og at en elev har klart å logge seg inn på en bruker med administratortilganger og herfra delt personopplysninger. Saken får stor medieomtale, og kommunens omdømme svekkes.

En av kommunens innbyggere har en mor som er beboer på et av kommunens pleiesentre. Innbyggeren er verge for moren. I en samtale med en kommunalt ansatt som også jobber i helse- og omsorgstjenesten, men i en annen avdeling, får innbyggeren en følelse av at vedkommende har innsikt i morens pleieforhold. Som følge av dette ber innbyggeren om at det undersøkes hvem som har vært inne og sett på morens journalopplysninger. Loggen viser at en person som ikke har tjenstlig behov har sett på morens opplysninger i journalsystemet. Det iverksettes en intern undersøkelse, den det gjelder vedgår å ha snoket i pasientjournaler, med den følge at den det gjelder avskjediges.

Kommunens regnskapssjef får en e-post fra driftsleverandøren av økonomisystemet med melding om at det er problemer med hans konto i økonomisystemet. Brukernavn og passord er utløpt. Ettersom regnskapssjefen nettopp er tilbake fra ferie tenker hun ikke mer på det, og går inn på nettskjemaet hun har fått en lenke til. Hun fyller ut skjemaet og trykker ok. Da hun får svar og forsøker å logge inn igjen i økonomisystemet kommer hun ikke inn igjen. Etter kort tid opplever alle ansatte det samme: ingen kommer inn i noen av kommunens systemer. Kommunen har blitt utsatt for et løsepengevirus, og løsepenger må betales ut for å få tilgang til kommunens IT-systemer igjen.

Kommunen anskaffer et nytt HR-system. Som en del av anskaffelsen gjennomføres det sikkerhetstester og funksjonstester i leverandørens sikkerhetsmiljø. For å få gode tester benyttes data hentet fra HR-systemet som er i drift. Leverandøren har en underleverandør i Ukraina som gjennomfører sikkerhetstestingen. Media plukker opp saken og skriver om den. Når Datatilsynet fatter interesse for saken får kommunen bøter på grunn av bruken av ansattes personopplysninger i strid med behandlingsgrunnlaget og overføringen av data til Ukraina. Foruten økonomiske konsekvenser som følge av boten får saken konsekvenser for de ansattes tillit til kommunen som arbeidsgiver. Flere ansatte velger derfor å slutte.

Behandling av personopplysninger med høy risiko for den registrerte, for eksempel behandling av helseopplysninger i store mengder, skal være gjenstand for en egen risikovurdering; en personvernkonsekvensvurdering. Vurdering og oppfølging av risiko knyttet til informasjonssikkerhet og personvern bør følge kommunens etablerte rammeverk for risikostyring.



Figur 6: Kommunen har verdier som de ønsker å beskytte. For å gjøre dette iverksettes tiltak for å sikre verdiene. På venstre side i figuren finnes ulike trusselaktører som ønsker tilgang til verdiene. Dette kan være ansatte, fremmede stater eller andre som ønsker tilgang til informasjonen. Disse vil forsøke å utnytte sårbarheter hos kommunen. Dersom kommunen ikke adresserer sårbarhetene med relevante tiltak, vil det være lettere for trusselaktørene å få tilgang til verdiene.

Uønskede hendelser har to komponenter som medfører at ting kan gå galt. Det ene er trusler kommunen står overfor, det andre er sårbarhetene kommunen selv har. Truslene kan være eksterne, for eksempel hackere, eller interne, for eksempel misfornøyde ansatte.

Kommunen feilkoder en bekymringsmelding til barnevernet med den følge at brev som burde vært unntatt offentlighet ligger åpent i offentlig postjournal. Barnevernet klarer ikke å ivareta barnets og familiens rett til personvern og saken har svært negative konsekvenser for barnet og for familien. Datatilsynet fatter interesse for saken og bøtelegger kommunen. Saken fått økonomiske konsekvenser, og konsekvenser for kommunens omdømme.

Hvilke sikkerhetstiltak som mest effektivt kan bidra til å redusere høy risiko til et akseptabelt nivå kan være vanskelig å få et godt overblikk over. Det anbefales derfor å bygge et rammeverk som stiller krav til sikkerhetstiltak, som bidrar til at kommunen forholdsvis enkelt kan få en god informasjonssikkerhet og godt personvern som bidrar til å håndtere mange risikoer. Nasjonal sikkerhetsmyndighet har etablert rammeverket «Grunnprinsipper for IKT-sikkerhet», som anbefales for blant annet offentlige virksomheter og virksomheter med kritiske samfunnsfunksjoner, slik som kommunen.

Ulike typer av informasjon med særlig høy verdi kan ha like sikkerhetsbehov, og informasjonssikkerhet og personvern kan i stor grad ivaretas gjennom de samme sikkerhetstiltakene. Gjennom en oversikt over verdiene kan informasjon grupperes slik at fokus og arbeid med sikkerhetstiltak særlig rettes mot informasjon, personopplysninger og IKT-systemer med høyest verdi. Eksempelvis kan sikkerhetstiltak for særskilte kategorier personopplysninger også benyttes for informasjonsverdier knyttet til samfunnskritiske oppgaver.

Kommunen kan for eksempel dele sine informasjonsverdier i fire grupper, og liste tiltak og frekvens som vist i tabellen under. Figuren sier også noe om at et sett sikkerhetstiltak kan gjelde for ulike informasjonsverdier – forutsatt at de har en samsvarende verdi for kommunens drift og tjenester.

Informasjonsverdi	Eksempel på informasjon	Grad av sikkerhetstiltak	Kontrollfrekvens
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	4 ganger årlig
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.	Høy	Halvårlig
Middels verdi	Virksomhetsintern informasjon eller informasjon som kan skade kommunens funksjoner og tjenester i daglig drift, f.eks.: • læringsplattformen for kommunikasjon mellom elev og skole. • informasjon som er unntatt offentligheten.	Middels	Årlig
Lav verdi	Åpen informasjon uten spesielle sikkerhetsbehov, f.eks.: • informasjon som ligger åpent på hjemmesiden til kommunen, som for eksempel organisasjonskart.	Lav	Ingen aktiv oppfølging av sikkerhetstiltak

Figur 7: Eksempler på gruppering av informasjon.

Kommunedirektøren anbefales å starte med følgende tiltak:

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

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?

5. Tjenesteutsetting

Tjenesteutsetting betyr at kommunen setter ut arbeidsoppgaver og/eller funksjoner til eksterne leverandører og tjenesteytere. Det kan for eksempel være å lagre opplysninger i skytjenester, å sette ut drift av IT-tjenester eller å sette ut driften av en kommunal tjeneste.

Ved tjenesteutsetting kan kun det utførende ansvaret settes bort. Det er aldri mulig å sette bort ansvaret for å følge kravene i lover og regler. Kommunedirektøren vil derfor alltid stå ansvarlig for personvern og informasjonssikkerhet i kommunen, og plikter å sikre at kravene på fagområdene etterleves også ved tjenesteutsetting. Dette kan gjøres ved å stille de rette kravene til personvern og informasjonssikkerhet ved anskaffelsen/utkontrakteringen, samt å følge opp leverandøren og kravene i avtalen gjennom hele avtaleforholdet. Gjennom oppfølging av leverandør og avtale, vil kommunen kunne gjennomføre kontrollaktiviteter for å sikre at kommunen etterlever sitt ansvar, og på den måten sikre egenkontroll.

Typiske risikoer ved utkontraktering:

- utilstrekkelige eller dårlige avtaler med leverandøren, typisk databehandleravtaler og tjenestenivåavtale.
- mangelfull oversikt over leverandører og deres underleverandører (leverandørkjeden).
- mangelfull identifisering av og kontroll på verdiene sine.
- mangelfulle eller manglende risikovurderinger.
- utilstrekkelig bestillerkompetanse i kommunen til å stille gode nok krav til personvern og informasjonssikkerhet i anskaffelser, og kunne følge opp avtaler.
- mangelfull oversikt over hvilke avhengigheter kommunen har i leverandør- og verdikjeder (hendelser hos leverandøren som kan få konsekvenser for kommunen).

Kommunal sektor utkontrakterer ofte tjenester og arbeidsoppgaver fordi de selv ikke har tilstrekkelig kompetanse eller ressurser. Det er viktig å sikre at kommunen har tilstrekkelig kompetanse og ressurser for å kunne håndtere risikoene ved utkontraktering.

Tjenesteutsetting og risikoene knyttet til dette kan forklares ved bruk av treet til høyre. Røttene i treet utgjør det man ikke ser til daglig – typisk bruk av skytjenester, nettverk og eksterne tilbydere av tjenester. Grenene i treet symboliserer tjenestene kommunen skal tilby til innbyggerne. Stammen i treet symboliserer avhengighetene mellom det å kunne levere en tjeneste og det man har tjenesteutsatt. Kommunen kan for eksempel være avhengig av at skytjenesten fungerer for å kunne behandle pasienter i en omsorgsbolig for eldre.

Det er ikke mulig å sette ut ansvaret for personvern og informasjonssikkerhet – det ligger til enhver tid hos kommunedirektøren.

5.1 SJEKKLISTE FOR TJENESTEUTSETTING

Sjekkliste for tjenesteutsetting		Ja	Vet ikke	Nei
1	Har kommunen gjennomført nødvendig vurderinger, herunder risikovurdering, av om tjenesteutsettinger kan gjennomføres og hvordan?			
2	Omfatter risikovurderingene både personvern og sikkerhet?			
3	Har kommunen sikret tilstrekkelig personvern og informasjonssikkerhet i kontrakten som regulerer tjenesteutsettingen?			
4	Har kommunen regulert hvordan den skal følge opp leverandører og leveranser, samt kommunens endringsbehov i kontakten?			
5	Har kommunen regulert forholdet om hvordan tilbakeføring og sletting skal skje ved opphør av tjenesteutsettingen?			
6	Følger kommunen opp sine eksterne leverandører?			
7	Har kommunen tilstrekkelig ressurser og kompetanse til å følge opp tjenesteutsettingen? - Dette innebærer virksomhetskompetanse, sikkerhetskompetanse, integrasjonskompetanse, kompetanse om anskaffelser og juridisk kompetanse.			
8	Revideres risikovurderinger for tjenesteutsetting jevnlig?			
9	Har kommunen inngått særskilt avtale om behandling av personopplysninger med leverandøren (databehandleravtale)?			
10	Har kommunen inngått sikkerhetsavtale i henhold til sikkerhetsloven der det er nødvendig?			
11	Er behandlingsprotokollen oppdatert med at tjenesten er satt ut?			
12	Er det gjennomført personvernkonsekvensvurderinger der dette er nødvendig?			
13	Har kommunen oversikt over hvor personopplysninger lagres. I EØS eller utenfor EØS?			
14	I tilfeller hvor personopplysninger lagres utenfor EØS, har kommunen iverksatt tiltak for å sikre personvernet og inngått tilstrekkelige avtaler?			
15	Har kommunen oversikt over hvor informasjon er lagret?			
16	Har kommunen oversikt over hvem hos leverandøren som har tilgang til informasjonen?			

Tenk gjennom

- Har vi oversikt over alle IT-tjenestene og applikasjonene vi bruker i kommunen?
- Har vi oversikt over om våre leverandører etterlever krav til personvern og informasjonssikkerhet?
- Har vi tilstrekkelig kompetanse for å håndtere risikoene ved utkontraktering?

6. Hvordan oppnå etterlevelse og hvordan organisere arbeidet?

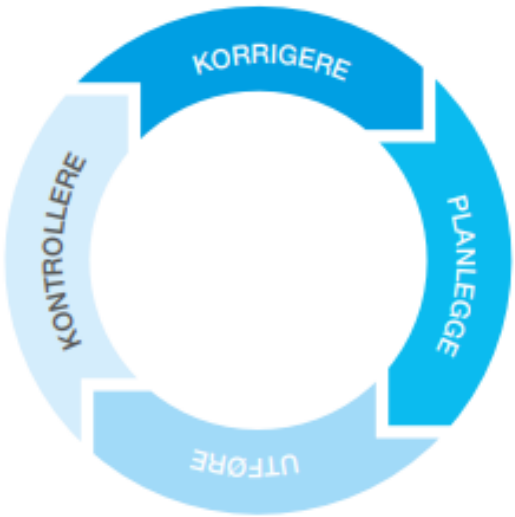
Kommuneloven § 25-1 pålegger kommunen at «internkontrollen skal være systematisk», dette gjelder også arbeidet med informasjonssikkerhet og personvern. I tillegg stiller regelverkene som er beskrevet i kapittelet *Relevant lovgivning* krav til internkontroll/styringssystem innen personvern og informasjonssikkerhet. 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 skape synergier i kontrollarbeidet. Effektiv internkontrollen bidrar til at kommunen kan levere tjenester med høy kvalitet og etter de krav som er stilt.

Internkontrollen skal bidra til at kommunen ivaretar 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, vil kommunen kunne identifisere sikkerhetstiltak som skal inngå i internkontrollen.

Regelverket for informasjonssikkerhet og personvern er teknologinøytralt og risikobasert, noe som medfører at internkontrollen også bør innrettes slik at den er risikobasert. Andre faktorer som har betydning for internkontrollen er kommunens størrelse, aktiviteter og egenart.

Arbeid med internkontroll på informasjonssikkerhets- og personvernområdet kan ses som en sammenhengende og gjentagende prosess; gjerne i form av en kvalitetssirkel.

En viktig forutsetning for å lykkes med en velfungerende internkontroll knyttet til informasjonssikkerhet og personvern, er at kommunen har kapasitet til og kunnskap på området. Det er derfor helt nødvendig at kommunedirektøren knytter til seg fagressurser, og sikrer at disse har nødvendig kunnskap og kapasitet til å gjennomføre og bistå i arbeidet. Nødvendig kompetanse kan skaffes på flere måter. For mindre kommuner kan et interkommunalt samarbeid om fagressursene være hensiktsmessig. Kompetanse kan også skaffes ved å ansette personell eller gjennom å leie inn eksterne eksperter. Uansett vil det være viktig å bygge og vedlikeholde kompetanse hos sine egne ansatte. Fagressurser bør være kjent og tilgjengelig for hele kommunen



Figur 8: 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 du som kommunedirektør ikke kan fraskrive deg ansvaret. Du bør derfor sikre at fagressursene du knytter til deg har rett kompetanse og kan spille deg god.

Omfanget av ressurser – behovet for kapasitet og dybdekompetanse vil variere med kommunens størrelse, men også i takt med antall prosjekter og innføring av ny eller endret teknologi.

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

6.1 PLANLEGGE

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

Arbeidet i planleggingsfasen bør organiseres som et prosjekt og kommunedirektøren må sikre at noen er ansvarlig for å gjennomføre aktivitetene. Kommunedirektøren bør ha rollen som prosjekteier. De som skal utføre jobben må kunne involvere og ansvarliggjøre andre deler av kommunen, slik at deres bidrag innlemmes i planene. Planleggingsfasen bør inneholde følgende aktiviteter:

A. Skaffe oversikt over:
   - sentrale lover og regler – og ha kunnskap om hvilke betydning de har for kommunen. Se kapittel 3 for en introduksjon.
   - sentrale informasjonsverdier og vurdere deres kritikalitet for kommunens drift og tjenesteproduksjon. Herunder etablere en oversikt over behandling av personopplysninger i kommunen. Se kapittel 2.1.1 for en introduksjon.

B. Plassere ansvar
   - Som minimum bør følgende ansvar fastsettes og dokumenteres som en del av kommunens eksisterende interkontroll:
     - Hvem skal føre oversikt over informasjonsverdier, vurdere kritikalitet og vedlikeholde en behandlingsprotokoll? Bør det skilles på administrative fellesprosesser og fagområder?
     - Hvem skal gjennomføre 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? Se kapittel 6.5 for informasjon.
     - Har vi nødvendig kompetanse i eget hus til å gjennomføre oppgavene?

C. Gjennomføre risikovurderinger
   - For de systemer og behandleringer som er identifisert under punkt A, må kommunen sikre at det blir gjennomført risikovurderinger for sikkerhet og personvern. Vi anbefaler at kommunens etablerte metode for risikostyring benyttes for å bidra til at informasjonssikkerhet blir en naturlig del av kommunenes ordinære risikostyring.
   - 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. Kommunedirektøren bør få regelmessig orientering om fremdrift.

6.2 UTFØRE

Hensikten med utførerfasen er å utforme, innføre og gjennomføre fastsatte internkontrollaktiviteter.

De fleste aktivitetene i denne fasen vil gjennomføres av andre enn kommunedirektøren, men du er likevel ansvarlig for å sikre at aktivitetene blir gjennomført. Internkontrollen skal bestå av rutiner og prosedyrer for *når*, *hvordan* og *av hvem* oppgaver skal utføres. Som minimum anbefaler vi at kommunen, som en integrert del av internkontrollen, sikrer at følgende er beskrevet og blir ivaretatt:

- Overordnet beskrivelse av kommunens sikkerhetsbehov.
- Organisering av arbeidet, herunder roller og ansvar for sikkerhet og personvern.
- Hvordan og hvor kommunen skal føre oversikt over informasjonsverdier og behandling av personopplysninger.
- Sikrer at IKT og personvern er en del av kommunens kontinuitets- og beredskapsplan.
- Hvordan kommunen skal ivareta personvernet og de registrertes rettigheter:
    - Utarbeide og vedlikeholde en personvernerklæring som gir informasjon om kommunens behandling av personopplysninger.
    - Forespørsel om innsyn, retting og sletting av personopplysninger.
    - Dataportabilitet.
    - Forespørsler om begrensning i eller protest mot bruk av personopplysninger.
    - Rettigheter ved automatiserte avgjørelser.
    - Retting og sletting av personopplysninger.
    - Ivaretakelse av personvernprinsippene.
- Hva som skal gjøres ved en ny behandling av personopplysninger og innføring av nye IKT systemer.
- Hvordan kommunen skal arbeide med kompetanse og opplæring knyttet til personvern og informasjonssikkerhet 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-systemer for å sikre at disse til enhver tid er oppdatert og har forsvarlig drift.
- Hvilke krav vi stiller til våre IKT-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 status på hvilke tiltak som er utarbeidet og implementert.

6.2.1 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 at sikkerhet og personvern som en integrert del av IKT- 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 i forhold til personvern og informasjonssikkerhet.
- Etablere tilstrekkelige avtaler med leverandør, herunder tjenestenivåavtaler, databehandleravtaler og eventuelt sikkerhetsavtaler.
- Sikre at man etter innføring også kvalitetssikrer leveranser med tanke på informasjonssikkerhet og personvern.

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

6.3 KONTROLLERE

Kontrollaktivitetene skal i hovedsak bidra til to ting. For det første skal de bidra til at definerte internkontrollaktiviteter (utføringsdelen) gjennomføres og fungerer som forutsatt. For det andre skal de bidra til videreutvikling av internkontrollen gjennom blant annet å:

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

Det kan finnes mange ulike kontrollaktiviteter. Internkontrollsystemet bør være bygd opp slik at det stilles krav til jevnlig oppdatering, dvs. at reglement, rutiner, veiledere, risikovurderinger, oversikter og andre relevante dokumenter til enhver tid er aktuelle. Det betyr også at man stiller krav til revisjon av dokumentene som inngår i systemet. Det vanlige er å stille krav til at dokumentene skal oppdateres årlig. Det vil tvinge de ansvarlige for dokumentene til å vurdere om det har skjedd endringer i praksis i kommunen, og om det har skjedd endringer i lovverk eller rettspraksis som innebærer at kommunen må endre praksis. Denne kontrollaktiviteten krever at de som eier dokumentene som skal gjennomgås, har tid og ressurser til å gjøre dette på en god måte.

Det er smart å legge kontrollaktivitetene i internkontrollen inn i et årshjul. Da vil man enklere holde oversikt over når kontrollaktiviteter skal gjennomføres, og det sette av tid til å gjennomføre. Alle aktivitetene som er nevnt i listen over kan inngå i et årshjul. Eksempler på kontrollaktiviteter er:

A. Ledelsens gjennomgang

Ledelsen bør minimum en gang per år holde en gjennomgang av personvern og informasjonssikkerhet. Formålet med møtet bør være å gå gjennom status for arbeidet med personvern og informasjonssikkerhet i kommunen. På den måten vil du som leder få tilstrekkelig informasjon om status og risikoer 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. sikkerhetsansvarlig, 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.

B. Egenkontroll

Egenkontroll handler om å vurdere og evaluere kommunens praksis for personvern og informasjonssikkerhet, fungerer etter hensikten. Med andre ord handler det om å gjennomføre evalueringer for å sikre at internkontrollsystemet fungerer etter sin hensikt. Egenkontrollen bør være risikobasert. Det vil si at ett år bør den kanskje fokusere på hvordan kommunens opplæring og tilgangsstyring er, mens et annet år bør den ta for seg sletting av personopplysninger og oppfølging av tiltak som skal være etablert i henhold til risikovurderinger.

C. 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.

6.4 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 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 påse at det er klart definert ansvarlige med frister for når tiltak skal være iverksatt. Vi anbefaler at ansvaret for disse tiltakene følger linjen.

6.4.1 Avvik

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 oppstå igjen eller motvirke negative følger.

Eksempler på særlig alvorlige avvik er:

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

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.**
  - **Ansvaret for lukking av avvik innen informasjonssikkerhet og personvern bør følge linjeansvaret.**

6.5 ROLLER OG ANSVAR

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

6.5.1 Sikkerhetsansvarlig

Kommunen bør ha en egen rådgiver eller sikkerhetsansvarlig. Denne medarbeideren bør ha nødvendig kunnskap på området og ha ansvar for å etablere og følge opp internkontroll. Sikkerhetsansvarlig vil typisk:

- Ivareta kommunedirektørens behov for styring og fagkompetanse på sikkerhetsområdet.
- Etablere og vedlikeholde prinsipper og rutiner (styringssystem) for informasjonssikkerhet.
- Ha ansvar for rådgivning og opplæring i informasjonssikkerhet internt.
- Påse at bestemmelser (internkontrollaktiviteter) for informasjonssikkerhet følges opp i digitaliseringsprosjekter, anskaffelser og i daglig drift.

Ansvar for å følge opp avvik på informasjonssikkerhetsområdet ligger også gjerne hos sikkerhetsansvarlig.

6.5.2 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. Oppgavene er 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:

- 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.
- Hjelpe innbyggere med spørsmål om deres personopplysninger.

6.6 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 selv gjennom det man sier og gjør være gode sikkerhetsforbilder.

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

6.7 AVSLUTTENDE MERKNADER

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.
- ha et styringssystem for informasjonssikkerhet og personvern som beskriver hvordan kommunen skal etterleve informasjonssikkerhet og personvern, og hvilket ansvar den ansatte selv har.
- 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.
  For eksempel vil en prosjektleder i et IKT-prosjekt ha et annet opplæringsbehov enn en ansatt på kommunens sykehjem.

Kommunedirektøren bør:

- 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 hverken til egne fagressurser, til egen ledergruppe eller til de som har ansvaret for gjennomføring av IT- eller digitaliseringsprosjekter

6.8 SJEKKLISTER FOR Å FÅ KONTROLL OG HA KONTROLL

FÅ kontroll		**Ja**	**Vet ikke**	**Nei**
1	**Oversikt**			
1.1	Har kommunen kartlagt og identifisert relevante krav de er underlagt (eks. lover, myndighetskrav mv.)?			
1.2	Har kommunen identifisert verdiene sine? Dvs. hvilke informasjon, personopplysninger, funksjoner, gjenstander, systemer mv. den sitter på som må beskyttes.			
1.3	Har kommunen kartlagt avhengighetene de har for å kunne ivareta sine funksjoner og beskytte sine verdier?			
1.4	Har kommunen vurdert om de har informasjon eller funksjoner som faller inn under sikkerhetsloven?			

1.5	Har kommunen oversikt over all behandling av personopplysninger, og slik oversikt blir ført i et eget dokument/system (behandlingsprotokoll)?			
1.6	Har kommunen oversikt over alle tjenester som er utkontraktert?			
2	**Risikovurderinger**			
2.1	Har kommunen gjennomført sårbarhetskartlegging og -vurderinger (risikovurderinger)?			
2.2	I risikovurderingen, har kommunen identifisert hvilke trusler som kan ramme deres verdier?			
2.3	Har kommunen utarbeidet scenarioer med tenkte situasjoner hvor trusselaktører forsøker å påvirke dens verdier?			
2.4	Har kommunen gjennomført vurderinger av konsekvensene for personvernet der det er sannsynlighet for en høy risiko for personvernet til innbyggerne?			
2.5	Har kommunen gjennomført konsekvensvurderinger for å fastsette eventuelle skadefølger det vil ha om dets verdier faller helt eller delvis bort?			
2.6	Har kommunen iverksatt tiltak for å håndtere risiko, basert på risikovurderinger som er gjennomført?			
3	**Organisering**			
3.1	Har kommunen integrert personvern og informasjonssikkerhet i den sektorovergripende internkontrollen?			
3.2	Har kommunen en plan for avvikshåndtering, som sikrer at kommunen er i stand til å oppdage, håndtere og lære av sine avvik?			
3.3	Legger avvikshåndteringen til rette for å overholde kravet om å varsle Datatilsynet innen 72 timer?			
3.4	Har kommunen etablert klare roller og ansvar for etterlevelse og oppfølging av personvern og informasjonssikkerhet?			
3.5	Har kommunen tilstrekkelig kompetanse og kapasitet til å ivareta informasjonssikkerheten?			
3.6	Har kommunen tilstrekkelig kompetanse og kapasitet til å ivareta personvernet?			
3.7	Har kommunen et personvernombud?			
3.8	Har kommunen sikret personvernombudets uavhengighet, og at det er fri for interessekonflikter mellom ombudsrollen og andre oppgaver?			
3.9	I årlig rapportering til politiske organer for internkontroll; inkluderes informasjonssikkerhet og personvern?			
4	**Kompetanse og kultur**			
4.1	Er det gjennomført opplæringskampanjer for de ansatte? (og responderer de ansatte)?			
5	**Personvern**			
5.1	Har kommunen tilrettelagt for at innbyggere og ansatte kan ta kontakt og påberope seg sine rettigheter etter personvernregelverket?			
5.2	Har kommunen en personvernerklæring som er tilgjengelig for innbyggere, ansatte og andre kommunen behandler personopplysninger for?			
HA kontroll		**Ja**	**Vet ikke**	**Nei**
1	**Oversikt**			

1.1	Holder kommunen seg oppdatert på relevante krav de er underlagt?			
1.2	Har kommunen oppdatert oversikt over sine verdier og hvilke avhengigheter de har for å ivareta sine funksjoner og beskytte verdiene?			
1.3	Er behandlingsprotokollen oppdatert?			
2	**Risikovurderinger**			
2.1	Har kommunen oppdaterte risikovurderinger som tar inn over seg dagens risiko?			
2.2	Holdes personvernkonsekvensvurderinger oppdatert?			
2.3	Kontrollerer kommunen sikkerhetstilstanden jevnlig?			
3	**Organisering**			
3.1	Gjennomfører kommunedirektøren ledelsens gjennomgang av personvern og informasjonssikkerhet jevnlig?			
3.2	Mottar jeg rapportering fra kommunens tjenesteområder som inkluderer noe om informasjonssikkerhet og personvern?			
3.3	Gjennomfører kommunen kontroller for å vurdere om internkontrollsystemet er kjent for ansatte og fungerer?			
3.4	Sikrer kommunen at kompetansen innen personvern og informasjonssikkerhet blir holdt ved like og oppdatert?			
4	**Kompetanse og kultur**			
	Har kommunen jevnlige øvelser, treninger og opplæring innen personvern og informasjonssikkerhet?			
	Evaluerer og lærer kommunen av uønskede hendelser?			
	Gjennomfører kommunen jevnlige opplæring- og/eller synlighetskampanjer for personvern og informasjonssikkerhet?			
5	**Personvern**			
5.1	Holdes personvernerklæringen oppdatert?			

6.9 SJEKKLISTE FOR PROSJEKTER

Sjekkliste for (digitaliserings)prosjekter		**Ja**	**Vet ikke**	**Nei**
1	Har kommunedirektøren/kommunen oversikt over hvilke digitaliseringsplaner og -initiativer har kommunen?			
2	Har kommunen oversikt over hvilke digitaliseringsprosjekter som vil håndtere personopplysninger?			
3	Er det etablert policyer for digitalisering som sier noe om hvordan informasjonssikkerhet og personvern skal ivaretas i et digitaliseringsprosjekt?			
4	Er personer med kompetanse innen personvern og informasjonssikkerhet involvert i prosjekter?			
5	Blir det vurdert hvilke konsekvenser prosjektets utfall vil ha for verdi- og leverandørkjeden til kommunen, og hvilke konsekvenser det til ha for kommunens mulighet til å levere tjenestene sine?			

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?

7. Nasjonale ressurser på personvern og informasjonssikkerhet

I Norge har vi flere myndigheter og ekspertmiljøer på personvern og informasjonssikkerhet. Nedenfor følger en liste over nasjonale ressurser og hva de kan tilby:

1. **Datatilsynet**

Datatilsynet er et uavhengig forvaltningsorgan som skal bidra til bedre personvern i hele Norge. Det fører tilsyn med virksomheters etterlevelse av personvernforordningen, har en ombudsrolle overfor publikum og gir råd om personvernforordningen.

Datatilsynets nettsider inneholder mye relevant informasjon for kommunal sektor. Her finnes blant annet veiledere for hvordan virksomheter skal etterleve regelverket. Datatilsynet har også en egen veiledningstelefon.

Nyttige lenker:
https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/

https://www.datatilsynet.no/rettigheter-og-plikter/personvernprinsippene/

2. **Nasjonal sikkerhetsmyndighet (NSM)**

Nasjonal sikkerhetsmyndighet er Norges ekspertorgan for informasjons- og objektsikkerhet, samt det nasjonale fagmiljøet for IKT-sikkerhet. NSM gir råd, informasjon og veiledning om forebyggende sikkerhetsarbeid, og kravene i sikkerhetsloven.

NSM har mange relevante veiledere og håndbøker for etterlevelse av sikkerhetsloven. I tillegg har de flere veiledere som gir god informasjon om sikkerhetsarbeid som faller utenfor sikkerhetsloven.

Nyttige lenker:
https://nsm.no/regelverk-og-hjelp/veiledere-og-handboker-til-sikkerhetsloven/

https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/introduksjon-1/

3. **Digitaliseringsdirektoratet (Digdir)**

Digitaliseringsdirektoratet (Digdir) er statens organ for digitalisering. Direktoratet har blant annet som oppgave å gi anbefalinger for internkontroll på området informasjonssikkerhet. Dette ansvaret gjelder overfor både statlig og kommunal sektor. Direktoratet har utarbeidet veiledere for internkontroll for informasjonssikkerhet som er relevant for alle kommuner. På direktoratets nettsider finnes det også guide til topplederens arbeid med informasjonssikkerhet og e-læringskurs for ledere.

Nyttige lenker:
https://internkontroll-infosikkerhet.difi.no/

https://www.digdir.no/informasjonssikkerhet/helhetlig-styring-og-kontroll-av-informasjonssikkerhet/2284

https://laeringsplattformen.difi.no/kurs/991825827/er-det-sikkert-et-e-laeringskurs-i-informasjonssikkerhet-ledere

4. **Direktoratet for forvaltning og økonomistyring (DFØ)**

Direktoratet for forvaltning og økonomistyring er statens fagorgan for offentlige innkjøp. DFØ eier nettstedet www.anskaffelser.no, der du finner informasjon om hvordan offentlig anskaffelser bør gjennomføres, og oversikt over regelverk som skal følges. Her finnes i tillegg relevant informasjon om personvern og informasjonssikkerhet ved anskaffelser.

Nyttige lenker:
https://www.anskaffelser.no/avtaler-og-regelverk/sikkerhetsloven-og-offentlige-anskaffelser

https://www.anskaffelser.no/verktoy/kontrakter-og-avtaler/databehandleravtale-og-sjekkliste

5. Kommune-CSIRT

Kommune-CSIRT har som mål å være et nasjonalt senter for informasjonssikkerhet i kommunesektoren. De støtter kommuner over hele landet med informasjon om trusler, hendelser og sårbarheter i det digitale rom.

Nyttige lenker:
https://kommunecsirt.no/

6. Norsk Senter for Informasjonssikring (NorSIS)

NorSIS er en del av regjeringens helhetlige satsing på informasjonssikkerhet i Norge. Målgruppen for NorSIS' aktivitet er norske virksomheter i privat og offentlig sektor. NorSIS skal så langt som mulig også imøtekomme innbyggernes behov, og alle samfunnsgrupper skal kunne dra nytte av NorSIS tjenester. NorSIS opptrer som en nøytral informasjonssikkerhetsinstans, og skal samarbeide med virksomheter for gjennomføring av informasjonssikkerhetstiltak.

Nyttige lenker:
https://norsis.no/

7. Foreningen Kommunal Informasjonssikkerhet (KiNS)

Formålet med KiNS er å bidra til økt informasjonssikkerhet i kommuner og fylkeskommuner. KiNS arrangerer en stor årlig konferanse der medlemmer møtes for nettverksbygging og faglig påfyll. KiNS arrangerer kurs innenfor ISO 2700x, teknisk informasjonssikkerhet og GDPR i tillegg til lokale/regionale seminarer.

Nyttige lenker:
https://kins.no/
https://kins.no/verktoykasse/

8. Definisjoner og lover

Definisjoner er i hovedsak hentet fra eller anvendt som utgangspunkt Datatilsynets ordliste, samt Digitaliseringsdirektoratets ordliste for internkontroll med informasjonssikkerhet.

Definisjoner

Avvik	Hendelse eller situasjon som bryter med gjeldende regler eller interne retningslinjer. Et avvik kaller også en uønsket hendelse. Avvik, eller brudd, knyttet til personopplysningssikkerhet skal meldes til Datatilsynet innen 72 timer, med mindre avviket sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter.
Behandling av personopplysninger	All bruk av personopplysninger, slik som innsamling, registrering, sammenstilling, lagring og utlevering, eller en kombinasjon av slike bruksmåter.
Behandlingsansvarlig	Den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes. Dette er vanligvis en virksomhet.
Behandlingsgrunnlag	Rettslig grunnlag for å behandle personopplysninger. Dette kan for eksempel være samtykke eller lov.
Behandlingsprotokoll	Oversikt over alle behandlinger av personopplysninger i virksomheten. Må inneholde informasjon som er opplistet i GDPR artikkel 30.
Brudd på personopplysningssikkerhet	Et brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet.
Databehandler	Den som behandler personopplysninger på oppdrag fra den behandlingsansvarlige. Dette er vanligvis en virksomhet.
Databehandleravtale	En avtale mellom databehandler og behandlingsansvarlig om hvordan personopplysninger skal behandles.
Etableringsaktivitet	Etableringsaktiviteter er aktiviteter som bør gjennomføres når en virksomhet første gang skal etablere systematisk internkontroll på informasjonssikkerhetsområdet. De kan også være aktuelle ved behov for oppdatering eller vesentlig forbedring av ulike deler i det grunnleggende arbeidet.
Iboende risiko	Den risiko som ligger naturlig i virksomheten, på bakgrunn av drift og bransje, eller risikoen som ligger naturlig i produktet mv.
IKT-system	IKT-systemer er et fellesbegrep for informasjons- og kommunikasjonssystemer, dvs. systemer som samler inn, behandler, overfører, lagrer og presenterer informasjon. Begrepet inkluderer her også infrastruktur og nettverk som er knyttet til IKT-systemet.
Informasjonssikkerhet	Sikring av opplysninger ved å bruke prinsippene om konfidensialitet, integritet og tilgjengelighet. Det betyr å sikre informasjonssystemene som benyttes for å behandle informasjon – inkludert sikkerhet i alle IKT-systemer, IKT-tjenester og IKT-komponenter som inngår i systemene.

Informasjonssikkerhetsbrudd	Informasjonssikkerhetsbrudd er brudd på konfidensialitet, integritet og/eller tilgjengelighet. Bruddet kan ha store, små eller ingen konsekvenser.
Informasjonssystem (IKT-system)	Et informasjonssystem er et system for innsamling, lagring, behandling, overføring og presentasjon av informasjon.
Informasjonsverdi	Informasjonsverdi, eller bare verdi i en informasjonssikkerhetssammenheng, er et samlebegrep. Begrepet inkluderer både informasjon og tilhørende støtteverdier som IKT-system, digitale tjenester, datautstyr av ulike varianter mv. Støtteverdiene er «noe» som benyttes i behandlingen av informasjonen.
Integritet	Prinsipp om at opplysninger skal være sikret mot utilsiktet eller uautorisert endring eller sletting.
Internkontroll	Planlagt og systematisk styringssystem som virksomheter etablerer for å oppdage brudd på gjeldende regler.
Konfidensialitet	Prinsipp om at opplysninger må være sikret mot at uvedkommende får tilgang til dem.
Personopplysning	Opplysning eller vurdering som kan knyttes til en enkeltperson. Dette kan være navn, adresse, telefonnummer, e-postadresse, bilnummer, bilder eller fødselsdato.
Personopplysningsloven	Personvernforordningen inngår i personopplysningsloven. Personopplysningsloven består i tillegg av særnorske regler.
Personvernforordningen	EUs forordning (regelverk) for personvern og en del av personopplysningsloven. På engelsk: the General Data Protection Regulation (GDPR). På norsk er personvernforordningen forkortet PVF.
Personvernkonsekvensvurdering (DPIA)	En prosess som skal bidra til å håndtere de risikoene behandlingen medfører for enkeltpersoners rettigheter og friheter ved å vurdere dem og fastlegge risikoreduserende tiltak. DPIA er en forkortelse for Data Protection Impact Assessment, en vurdering av personvernkonsekvenser.
Personvernombud	En person som er utpekt av en behandlingsansvarlig. Personen har som oppgave å bidra til at den behandlingsansvarlige følger personopplysningsloven med forskrift.
Risiko	Hypotese om hvilken fare en hendelse representerer eller sannsynlighet kombinert med konsekvens.
Risikostyring	Risikostyring er et sett av aktiviteter for å styre og kontrollere risiko. De kalles ofte «risikostyringsprosessen», men aktivitetene er ikke nødvendigvis sekvensielle. De ulike aktivitetene kan i hovedsak være foranlediget av hvilken som helst av de andre aktivitetene.
Sikkerhetsavtale	Avtale etter sikkerhetsloven som skal regulere sikkerheten ved gjennomføre en sikkerhetsgradert anskaffelse som gir leverandøren tilgang til sikkerhetsgradert informasjon, skjermingsverdige objekter eller skjermingsverdig infrastruktur uten oppsyn av en representant fra kommunen.

Sikkerhetstiltak	Når det snakkes om sikkerhetstiltak menes alt som gjøres for å redusere risikoer på informasjonssikkerhets- og personvernområde. I personvernforordningen er sikkerhetstiltakene kategorisert som tekniske og organisatoriske.
Skjermingsverdig verdi	Skjermingsverdige verdier er skjermingsverdig informasjon, informasjonssystem, infrastruktur eller objekter. Med skjermingsverdig menes at f.eks. informasjon er skjermingsverdig om det kan skade nasjonale sikkerhetsinteresser om den blir kjent for uvedkommende, går tapt, blir endret eller blir utilgjengelig.
Styringssystem	Betegnelse brukt for det sett av prosesser, tiltak mv. som må etableres og fungere for at en virksomhet skal ha tilstrekkelig intern styring og kontroll.
Særlig kategori av personopplysning	Også kalt sensitive personopplysninger. Dette er opplysninger som krever ekstra vern, slik som opplysninger om rasemessig eller etnisk opprinnelse, religion, helseopplysninger, seksuell orientering med mer.
Tilgjengelighet	Prinsippet om at opplysninger skal være tilgjengelig for det formålet de er tiltenkt.
Tiltak	Dette veiledningsmateriellet benytter begrepet tiltak på alt som gjøres både for å redusere risikoer på det som er i fokus, i vårt tilfelle informasjonssikkerhet, og det som gjøres for å gjøre internkontrollprosessene bedre.
Tjenestenivåavtaler	Avtale mellom leverandør av en tjeneste og kunden. Tjenestene det er snakk om er typisk IT-tjenester. På engelsk blir slike avtaler omtalt som *Service level agreement (SLA).*
Tjenesteutsetting	Det å sette ut arbeidsoppgaver og/eller funksjoner til eksterne leverandører og tjenesteytere. Tjenesteutsetting blir også kalt utkontraktering eller konkurranseutsetting. På engelsk heter det Outsourcing.
Trusler eller trusselaktører/-kilde	Begrepet trusler brukes her som synonym til trusselkilder. Begrepet benyttes om både aktører for villede handlinger og farekilder.
Verdivurdering	En kartlegging av informasjonsverdier (også kalt verdivurdering) innebærer å få en tilstrekkelig oversikt over informasjonsverdier som er omfattet av spesielt regelverk for informasjonssikkerhet eller som er av så vesentlig betydning for virksomhetens mål for informasjonssikkerhet at de bør omfattes av risikovurderinger.

Lover og forskrifter:

eForvaltningsforskriften	Forskrift om elektronisk kommunikasjon med og i forvaltningen	https://lovdata.no/pro/#document/SF/forskrift/2004-06-25-988
Kommuneloven	Lov om kommuner og fylkeskommuner	https://lovdata.no/pro/#document/NL/lov/2018-06-22-83?searchResultContext=1238&rowNumber=1&totalHits=2461

Personopplysningsloven	Lov om behandling om personopplysninger	https://lovdata.no/pro/#document/NL/lov/2018-06-15-38
Sikkerhetsloven	Lov om nasjonal sikkerhet	https://lovdata.no/pro/#document/NL/lov/2018-06-01-24?searchResultContext=2368&rowNumber=1&totalHits=373