

VEDLEGG 1 REGELVERKET

Relevant lovgivning

Personopplysningsloven, sikkerhetsloven og eForvaltningsforskriften er regelverk 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 helselovgivningen, opplæringsloven og arbeidsmiljøloven.

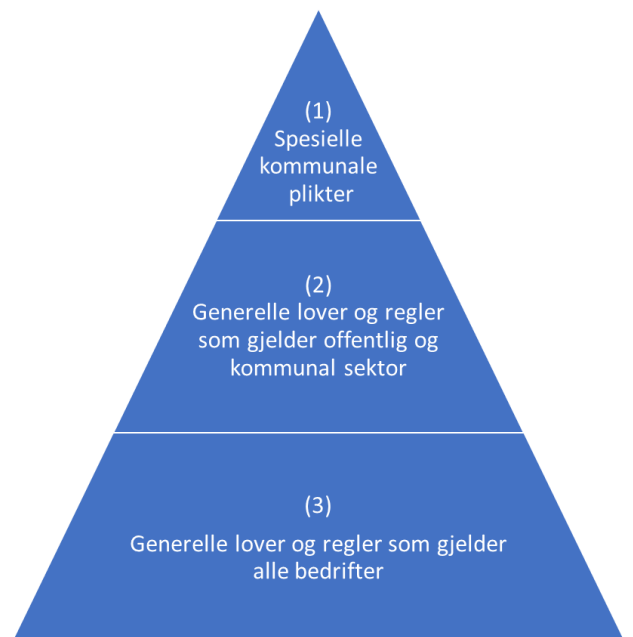
Etterlevelsen av regelverkene bør inngå i den sektorovergripende internkontrollen som er beskrevet i [kapittel 5](#) i *Orden i eget hus*, for eksempel under [«reglement for datasikkerhet og personvern»](#).

Regelverkene som regulerer personvern og informasjonssikkerhet må ses i sammenheng med andre regelverk. Figur 5 viser hvordan generelle og spesielle regler gjelder for kommuner.

Personopplysningsloven er en generell lov som gjelder alle virksomheter som behandler personopplysninger. Den er dermed et eksempel som kan plasseres i (3) i figuren.

Forvaltningsloven, eForvaltningsforskriften, offentlighetsloven og sikkerhetsloven er regler i (2) som er generelle og gjelder for både offentlig og kommunal sektor.

Kommuneloven er særregelverk for kommuner. I tillegg finnes det oppgaver som er spesielle for kommuner, og som reguleres av spesielle lovverk. Eksempler er barnevern, skole, sosialtjenester, helse og omsorg som kan plasseres i (1) i figuren.



Figur 1: 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](#).

Et viktig poeng for deg som kommunedirektør er at felles for alle lovene og forskriftene som er omtalt er at de er risikobaserte og i noen grad overlappende når det gjelder personvern og informasjonssikkerhet. Vi anbefaler derfor at kommunen har en [helhetlig tilnærming](#) til personvern og informasjonssikkerhet og virksomhetsstyring generelt.

Lover og forskrifter:

Forvaltningsloven	Forvaltningsloven regulerer saksbehandlingen i offentlig forvaltning og sikrer rettighetene til parter i forvaltningssaker	Lov om behandlingsmåten i forvaltningssaker (forvaltningsloven) - Lovdata
eForvaltningsforskriften	Forskrift om elektronisk kommunikasjon med og i forvaltningen	Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften) - Lovdata
Offentlighetsloven	Offentlighetsloven sikrer allmennheten rett til innsyn i dokumenter fra offentlige virksomheter for å fremme åpenhet og demokratisk kontroll	Lov om rett til innsyn i dokument i offentlig verksemd (offentleglova) - Lovdata
Kommuneloven	Regulerer organiseringen og virksomheten til kommuner og fylkeskommuner, og fremmer lokalt selvstyre	Lov om kommuner og fylkeskommuner (kommuneloven) - Lovdata
Personopplysningsloven	Beskytter personvernet ved behandling av personopplysninger og gjennomfører EUs personvernforordning (GDPR) i norsk rett	Lov om behandling av personopplysninger (personopplysningsloven) - Lovdata
Digitalsikkerhetsloven	Sikrer grunnleggende krav til digital sikkerhet i samfunnskritiske virksomheter for å forebygge og motvirke digitale trusler	Lov om digital sikkerhet (digitalsikkerhetsloven) - Lovdata
Sikkerhetsloven	Bidrar til å trygge Norges suverenitet og nasjonale sikkerhetsinteresser ved å forebygge, avdekke og motvirke sikkerhetstruende virksomhet	Lov om nasjonal sikkerhet (sikkerhetsloven) - Lovdata

Under følger korte beskrivelser av de regelverkene som er særlig relevante for å ivareta informasjonssikkerhet og personvern, samt hvilke plikter kommunen må ivareta.

Kort om eforvaltningsforskriften

Forskriften gjelder for kommunal sektor og stiller krav til internkontroll på informasjonssikkerhetsområdet. Forskriften anbefaler dessuten at kommunen baserer 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 i 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.

Kort om personopplysningsloven

Personopplysningsloven, hvor personvernforordningen (på engelsk GDPR) er innlemmet, regulerer [behandling](#) av personopplysninger.

Regelverket er basert på noen overordnede prinsipper, men som kommer til uttrykk i spesifikke plikter som virksomheter som ønsker å behandle personopplysninger må etterleve. Disse er nærmere beskrevet i vedlegg 3 Grunnprinsipper for behandling av personopplysninger.

Noen plikter som er særlig relevante når det gjelder til kommunens internkontroll:

- Kommunen skal ha et styringssystem for personvern og informasjonssikkerhet som gjør det mulig å etterleve kommunens plikter (artikkel 24).
- Kommunen skal ta stilling til konsekvenser for ansatte og innbyggernes rettigheter etter personvernforordningen før behandlingsaktiviteter igangsettes (vurdere personvernkonsekvens/DPIA) (PVF art. 24 og 35).
- Aktiviteter som innebærer at personopplysninger behandles skal føres i en egen oversikt (behandlingsprotokoll) (PVF art. 30).
- I tilfeller hvor kommuner bruker eksterne leverandører, som behandler personopplysninger på vegne av kommunen, skal det inngås databehandleravtale (PVF art. 28).
- 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).
- Brudd på personopplysningssikkerheten skal meldes Datatilsynet innen 72 timer (PVF art. 33).

Kort om digitalsikkerhetsloven

Digitalsikkerhetsloven skal etter planen tre i kraft i løpet av 2024. Loven skal styrke den digitale sikkerheten i samfunnet og følger opp EU-direktivet om sikkerhet i nettverks- og informasjonssystemer (NIS1-direktivet).

Loven har som formål å bidra til å sikre grunnleggende krav til digital sikkerhet i virksomheter med særlig samfunnsmessig betydning gjennom å stille strengere krav til kontroll på sikkerhetsarbeidet.

Digitalsikkerhetsloven skal primært gjelde for samfunnskritiske sektorer som energi, transport, helse, vannforsyning, bank, finansmarkeder, og digital infrastruktur, samt for digitale tjenesteleverandører. NIS1 har imidlertid allerede fått en oppfølger i NIS 2-direktivet, og dette har et virkeområde som også inkluderer offentlige myndigheter, utdanningsinstitusjoner og avfallshåndtering. Dette er tjenester som gjør regelverket desto mer relevant for kommuner.

For kommunene betyr dette at de må iverksette sikkerhetstiltak for å beskytte sine nettverks- og informasjonssystemer mot digitale trusler. I den grad kommunene blir omfattet av loven, vil kommunene dessuten være forpliktet til å varsle om alvorlige digitale hendelser som kan påvirke deres evne til å levere viktige tjenester.

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 (tilsiktete 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.

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.