# Fellesoversikt over rettslige føringer som er relevante for alle deler av kommunens virksomhet

|  |  |  |
| --- | --- | --- |
| **Lov/forskrift/årstall** | **Stikkord** | **Byrådsavdeling**  |
| **Personvern** |  |  |
| Personopplysningsloven(2000) | * Setter vilkår for behandling av personopplysninger. Strengere vilkår for behandling av sensitive personopplysninger.
* Meldeplikt / konsesjonsplikt for enkelte typer behandlinger
* Den behandlingsansvarlige må ha oversikt over hvilke personopplysninger som behandles samt grunnlag for og formål med behandlingen.
* Innsynsrettigheter
* Krav til styring og kontroll av personvern og informasjonssikkerhet
* Krav til databehandleravtale ved avtale om behandling av personopplysninger på vegne av den behandlingsansvarlige.
* Krav om at personvern og informasjonssikkerhet skal ivaretas gjennom internkontrolltiltak
 | FIN |
| Personopplysningsforskriften (2000) | * Forskriftens kap 2 og 3 er sentrale for informasjonssikkerhet.
* Krav om sikring av konfidensialitet, integritet og tilgjengelighet, krav til ledelsens involvering, bruk av risikovurderinger, sikkerhetsrevisjoner, oppfølging av sikkerhetsbrudd og krav til sikring ved utveksling av informasjon med andre.
* Arbeidsgivers rett til innsyn i ansattes e-post mm.
 | FIN |
| **Saksbehandling / dokumenthåndtering** |  |  |
| Forvaltningsloven (1967) | * Taushetspliktreglene (§§ 13 – 13f) regulerer hva som er underlagt konfidensialitet og hvordan konfidensialitet skal ivaretas.
* Regler om rett til partsinnsyn og hvilken måte dette skjer på.
* § 15 er grunnlag for forskrift om elektronisk kommunikasjon.
 | BLK |
| E-signaturloven (2001) | * Loven regulerer bruk av elektronisk signatur gjennom krav til sertifikater, sertifikatutstedere og signaturfremstillingssystemer.
* En kvalifisert elektronisk signatur regnes som (minst) like god som en ordinær underskrift.
* Bruk av kvalifiserte elektroniske signaturer i kommunikasjon med og i forvaltningen kan reguleres av forskrift (eforvaltningsforskriften).
 | FIN |
| Eforvaltningsforskriften (2004) | * Forskriften gjelder for elektronisk kommunikasjon med forvaltningen og for elektronisk saksbehandling og kommunikasjon i forvaltningen når ikke annet er bestemt i lov eller i medhold av lov.
* Krav om systematisk styring og internkontroll av informasjonssikkerhet.
 | BLK/FIN |
| Forskrift om IT-standarder i offentlig forvaltning (2013) |  |  |
|  Arkivlova (1992) | * Arkivlova stiller krav om at offentlige organer må bevare dokumenter for ettertiden.
* Arkivloven (og forskriftens) krav får betydning for hvordan informasjon skal lagres, hvor lenge og hvem som skal ha tilgang til informasjon.
* Forbud mot å føre arkiv ut av landet (§ 9b) har betydning for valg av sky-løsninger.
 | KON |
| Forskrift om offentlige arkiv (1998) | * Forskriften stiller krav til journalføring av dokumenter, bruk av journalsystem, dokumentkvalitet, arkivlokale, kassasjon og avlevering med mer.
 | KON |
|  Offentleglova (2006) | * Loven regulerer rett til innsyn i offentlige dokumenter / informasjon. Dette får konsekvenser for hvilken informasjon som skal beskyttes og tilgangsbegrenses internt.
* Loven skiller mellom plikt til å nekte innsyn (taushetsplikt) og rett til å nekte innsyn. Hvis det er rett til å nekte innsyn, har man allikevel plikt til å vurdere såkalt meroffentlighet.
 | BLK |
| Offentlegforskrifta (2008) | * § 7 regulerer hva man ikke kan gjøre tilgjengelig på Internett
* § 10 regulerer innsyn i graderte dokumenter; før innsyn må saken forelegges for den som har opprettet dokumentet.
 | BLK |
| **Sikkerhet og beredskap** |  |  |
| Sikkerhetsloven (1998) | * Loven setter krav til om beskyttelse av informasjon ved hjelp av sikkerhetsgraderinger.
* Hensynet til rikets selvstendighet, sikkerhet og andre vitale nasjonale sikkerhetsinteresser avgjør gradering. Sikkerhetsgradert informasjon er taushetsbelagt.
* Loven gjelder også for «skjermingsverdige objekter».
* IKT-system som skal inneholde sikkerhetsgradert informasjon, må være godkjent av Nasjonal sikkerhetsmyndighet (sikkerhetsloven § 13). Konsekvensen er at sikkerhetsgradert informasjon normalt kun foreligger som papirdokumenter i kommunen.
* Personer som skal ha tilgang til skjermingsverdig informasjon må være autorisert eller ha sikkerhetsklarering i tråd med sikkerhetsloven kap 6.
 | MOS |
| Forskrift om sikkerhetsadministrasjon (2001) | * Forskrift til sikkerhetsloven
* Pålegger kommunen å ha en sikkerhetsleder som skal sørge for sikkerhetsadministrasjon, herunder bl a veiledning, risikohåndtering, rapportering mm knyttet til håndtering av sikkerhetsgradert informasjon.
* Funksjonen som sikkerhetsleder etter sikkerhetsloven er lagt til MOS og BER for Oslo kommune. I tillegg skal hver virksomhet ha sin sikkerhetsorganisasjon, med en lokal sikkerhetsleder.
 | MOS |
| Forskrift om informasjonssikkerhet (2001) | * Forskrift til sikkerhetsloven
* Krav til gradering, merking, informasjonshåndtering, journalføring mm. Forskriften stiller også detaljerte krav til informasjonssikkerhet i IKT-systemer som skal inneholde gradert informasjon.
* Det forekommer tilfeller av slike dokumenter i kommunen. I postjournal kan dokumenter inntil BEGRENSET registreres, men med anonymisert sakstittel. Skanning av dokumentet er ikke tillatt. Fra og med gradering KONFIDENSIELT skal dokumenter føres i egen journal.
 | MOS |
| Forskrift om objektsikkerhet (2010) | * Forskrift til sikkerhetsloven.
* I den grad kommunen har skjermingsverdige objekter, vil Byrådsavdeling for miljø og samferdsel og Beredskapsetaten søke å ha oversikt over disse.
* Skjermingsverdige objekter kan være både bygninger, anlegg, rom med mer.
* Det er særskilte krav til systemer hvor man håndterer informasjon knyttet til skjermingsverdige objekter.
 | MOS |
| **Annet**  |  |  |
| Børsloven 82007) | * Regler om taushetsplikt i § 14
 |  |
| Verdipapirhandelsloven (2007) | * Regler om taushetsplikt (§ 3-4) og tilbørlig informasjonshåndtering
 |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Kommunens regelverk og instrukser** | **Stikkord** | **Referanse** | **Byrådsavd** |
| IKT-reglementet | * Regulerer hvem som har ansvar for å ivareta informasjonssikkerhet og hovedoppgaver.
* Krav om at tjenesteavtaler skal inneholde krav til informasjonssikkerhet
* Intern leverandør har ansvar for operativ informasjonssikkerhet i infrastrukturen.
 | Reglement for informasjons- og kommunikasjonsteknologi og informasjonssikkerhet (2010) | FIN |
| Informasjonssikkerhets-instruksen | * Instruksen har som formål å sikre grunnlag for god styring og kontroll med informasjonssikkerhetsarbeidet, fastsette felles minimumskrav for informasjonssikkerhet, og fremme god sikkerhetskultur
* Instruksen gjelder all behandling av informasjon i kommunen.
 | Instruks for informasjonssikkerhet (2013) | FIN |
| Dokumentstandarder ved publisering på nettsteder | * Rundskrivet legger føringer for bruk av dokumentstandarder og veiledning om bruk av slike. Jf forskrift om bruk av IT-standarder i forvaltningen.
 | Rundskriv 15-2010 | FIN |
| Instruks for bruk av datautstyr i Oslo kommune | * Regulerer tjenstlig bruk av kommunens datautstyr.
 | Rundskriv 19-2009 | FIN |
| Fjernarbeid som arbeidsform i Oslo kommune | * Oslo kommune har etablert løsninger for å gjøre det mulig å utføre fjernearbeid (herunder hjemmekontor). Rundskrivet regulerer dette.
* Rundskrivet inneholder retningslinjer som bl a sier noe om dokumenthåndtering og informasjonssikkerhet.
 | Rundskriv 2009-11 | FIN |
| Instruks for bruk av e-post | * Rundskrivet setter grenser for hvilken informasjon som kan sendes med e-post.
* Instruksen fører til at e-post ikke kan brukes som alternativ til / som erstatning for journalpliktige dokumenter.
 | Rundskriv 24-2001 | FIN/KON/BLK |
| **Andre forpliktelser**  |  |  |  |
| Norm for informasjonssikkerhet i helse- og sosialsektoren | * Alle som er tilknyttet Norsk Helsenett må forplikte seg til å overholde normens vilkår og krav. Normen gjelder dermed som krav til disse virksomhetene med grunnlag i avtalen.
 | [www.normen.no](http://www.normen.no)  | EST |