

Regler om informasjonssikkerhet med tekst fra Lovdata

Lov om folketrygd (ASD)	4
§ 25-16. Planplikt for beredskap i trygdeetaten	4
Lov om toll (tolloven) (FIN)	4
Kap. VI. Bruk av elektronisk datautveksling m.v.	4
Forskrift om elektronisk tilgang til opplysninger i ligningsforvaltningens registre (FIN)	6
Forskrift om bruk av informasjons- og kommunikasjonsteknologi (IKT) (FIN).....	7
Forskrift om registrering av juridiske personer m.m. i Enhetsregisteret (FIN).....	7
§ 23. Datasikkerhet.....	7
Forskrift om informasjonssikkerhet (FD)	7
Hele forskriften	7
Forskrift om sikkerhetsgraderte anskaffelser (FD)	7
§ 2-7. Gjennomføring av sikkerhetstiltak hos leverandøren	7
Forskrift om sikkerhetsinformasjon (FD)	8
Hele forskriften kan være aktuell	8
Forskrift om personellsikkerhet (FD).....	8
Hele forskriften kan være aktuell	8
Forskrift om register for lagring av opplysninger innsamlet ved bruk av satellittsporingssystemer på fiskefartøy (FKD).....	8
Lov om helseregistre og behandling av helseopplysninger (helseregisterloven) (HOD)	8
§ 16. Sikring av konfidensialitet, integritet, kvalitet og tilgjengelighet.....	8
Forskrift om pasientjournal (HOD).....	9
§ 4. (Journalssystem)	9
Forskrift om innsamling og behandling av helseopplysninger i Reseptbasert legemiddelregister (Reseptregisteret) (HOD)	9
Kapittel 4. Taushetsplikt, informasjonssikkerhet og internkontroll.....	9
Forskrift om innsamling og behandling av helseopplysninger i Norsk overvåkingssystem for antibiotikaresistens hos mikrober (NORM-registerforskriften) (HOD).....	11
Kapittel 4. Informasjonssikkerhet og internkontroll	11
Forskrift om innsamling og behandling av helseopplysninger i Dødsårsaksregisteret (Dødsårsaksregisterforskriften) (HOD).....	12
Kapittel 4. Taushetsplikt, informasjonssikkerhet og internkontroll.....	12
Forskrift om innsamling og behandling av helseopplysninger i Kreftregisteret (Kreftregisterforskriften) (HOD).....	14
Kapittel 4. Taushetsplikt, informasjonssikkerhet, internkontroll.....	14

Forskrift om innsamling og behandling av helseopplysninger i Medisinsk fødselsregister (Medisinsk fødselsregisterforskriften) (HOD)	16
Kapittel 4. Taushetsplikt, informasjonssikkerhet og internkontroll	16
Forskrift om innsamling og behandling av helseopplysninger i System for vaksinasjonskontroll (SYSVAK-registerforskriften) (HOD)	18
Kapittel 4. Taushetsplikt, informasjonssikkerhet og internkontroll	18
Forskrift om innsamling og behandling av helseopplysninger i Meldingssystem for smittsomme sykdommer og i Tuberkuloseregisteret og om varsling om smittsomme sykdommer (MSIS- og Tuberkuloseregisterforskriften) (HOD)	20
Kapittel 5. Taushetsplikt, informasjonssikkerhet og internkontroll	20
Lov om behandling av personopplysninger (personopplysningsloven) (JD)	22
§ 13. Informasjonssikkerhet	22
Forskrift til lov om Schengen informasjonssystem (SIS-forskriften) (JD)	23
Kapittel 7. Internkontroll og informasjonssikkerhet	23
Forskrift om tinglysning (JD)	26
§ 25. Datasikkerhet	26
Forskrift om offentleget arkin (KKD)	27
§ 4-9. Vern mot skadeverk, innbrot og ulovleg tilgjenge	27
Forskrift om kart og stedfestet informasjon i plan- og byggesaksbehandlingen (MD)	27
§ 11. Datasikkerhet	27
Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften) (MOD)	27
Hele forskriften	27
Forskrift om behandling av personopplysninger (personopplysningsforskriften) (MOD) ..	27
Kap 2 og 8	27
Forskrift om registrering av foretak (NHD)	27
§ 10. Datasikkerhet	27
Forskrift om føringen av grunneiendoms-, adresse- og bygningsregisteret (GAB-registeret) (MD)	28
§ 10. Informasjonssikkerhet, taushetsplikt, mv.	28
Forskrift om elektronisk signatur (NHD)	28
Forskrift om beredskap i kraftforsyningen (OED)	28
Kapittel 6. Informasjonssikkerhet	28
Forskrift om Petroleumstilsynet (OED)	31
§ 5-1. Datasikkerhet	31

Lov om elektronisk kommunikasjon (ekomloven)	31
Flere viktige bestemmelser	31
Forskrift om elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste (ekomforskriften) (SD).....	32
Kapittel 8. Sikkerhet og beredskap	32
Instruks for behandling av dokumenter som trenger beskyttelse av andre grunner enn nevnt i sikkerhetsloven med forskrifter (beskyttelsesinstruksen) (SMK).....	33
§ 10. Forsendelse	33

Lov om folketrygd (ASD)

§ 25-16. Planplikt for beredskap i trygdeetaten

Rikstrygdeverket skal påse at det utarbeides beredskapsplaner for å sikre virksomheten i trygdeetaten ved krise i fred eller krig. Planene skal inneholde krav til opprettholdelse av driftssikkerhet for behandling av krav om ytelser og for utbetaling, til lagring av materiell og utstyr, og til øvelser og opplæring av personell.

Rikstrygdeverket har ansvaret for å samordne tiltak etter første ledd med berørte organer for å sikre behandling og utbetaling av ytelser som utbetales gjennom trygdeetaten.

Lov om toll (tolloven) (FIN)

Kap. VI. Bruk av elektronisk datautveksling m.v.

§ 40. (tillatelse til bruk av elektronisk datautveksling m.v.)

Når noen etter loven her eller andre lover skal eller kan gi melding til tollvesenet, herunder fremlegge tolldeklarasjon, kan tollvesenet gi tillatelse til at slik melding gis ved hjelp av elektronisk datautveksling. Med melding menes enhver opplysning, erklæring, forespørsel eller meddelelse. Med elektronisk datautveksling menes utveksling av data strukturert etter anerkjente meldingsstandarder mellom datamaskinsystemer. Bestemmelsene i dette kapittel får tilsvarende anvendelse på annen datamaskinassistert kommunikasjon med tollvesenet, så langt de passer.

Kongen kan gi nærmere forskrifter om de vilkår som må være oppfylt for at det skal kunne gis tillatelse til bruk av elektronisk datautveksling, hvilke typer meldinger som kan overføres ved hjelp av elektronisk datautveksling, hvorledes overføringen skal skje, samt om tillatelsens øvrige innhold. Det kan også fastsettes at den som har fått tillatelse etter første ledd, ikke skal benytte annen overføringsmåte overfor tollvesenet enn den som fremgår av tillatelsen, med mindre det i enkelttilfeller gis adgang til dette.

Det kan fastsettes vilkår for den enkelte tillatelse. Tillatelsen kan begrenses til å gjelde enkelte typer meldinger og nærmere angitte overføringsmåter.

Tillatelsen kan endres eller tilbakekalles dersom innehaveren av tillatelsen gjør seg skyldig i vesentlige eller gjentatte brudd på tillatelsens vilkår eller tilsvarende overtredelser av toll- og avgiftslovgivningen. Endring eller tilbakekall kan også skje der innehaveren ikke lenger oppfylder de tekniske krav som stilles, eller det finnes nødvendig i forbindelse med en generell omlegging av relevante systemer og sikkerhetsrutiner. Kongen kan gi nærmere forskrifter om vilkårene for og fremgangsmåten ved endring eller tilbakekall av tillatelsen.

Kongen kan ved forskrift bestemme at informasjonssystemer som tollvesenet etablerer, bare skal være tilgjengelige ved bruk av elektronisk datautveksling, samt fastsette nærmere bestemmelser om dette.

§ 41. (krav til meldingssikkerhet)

Kongen kan i forskrift stille krav til bruken av elektronisk datautveksling og gi nærmere bestemmelser om de plikter som pålegges brukeren, herunder om:

- a. sikring av meldingens integritet og tiltak som bidrar til å skape sikkerhet om meldingens opphav, samt andre identifikasjonsteknikker,
- b. tiltak som forebygger at feil oppstår under generering og overføring av meldingen, samt rutiner for varsling av feilsendinger, uteblitte returnmeldinger eller ukorrekte meldinger,
- c. behandlingsmåten for meldinger som mottas av feil adressat, samt plikt til å bevare taushet overfor uvedkommende om opplysninger som det fås kjennskap til ved mottagelse av slike meldinger,
- d. kontroll av returnmeldinger fra tollvesenet og hvorledes slike kontroller skal gjennomføres,
- e. plikt til å føre et historisk register som inneholder alle meldinger slik de blir sendt og mottatt, opplysning om hvem som har sendt og mottatt disse og tidspunkt for når dette er skjedd, samt krav til registerets øvrige innhold, organisering, sikring og vedlikehold.

Tilføyd ved lov 19 juni 1997 nr. 65 (i kraft 1 juni 2000 iflg. forskrift 25 mai 2000 nr. 535).

§ 42. (oppbevaring av meldinger, dokumenter m.v.)

Kongen kan gi nærmere forskrifter om hvor, på hvilken måte og hvor lenge meldinger som er sendt eller mottatt ved hjelp av elektronisk datautveksling skal oppbevares. Tilsvarende gjelder for de dokumenter, erklæringer m.v. som skal fremlegges i henhold til § 15.

Tilføyd ved lov 19 juni 1997 nr. 65 (i kraft 1 juni 2000 iflg. forskrift 25 mai 2000 nr. 535).

§ 43. (når melding er lagt frem m.v.)

Tolldeklarasjon som er avgitt ved hjelp av elektronisk datautveksling, anses å være lagt frem for tollvesenet når den er mottatt i tollvesenets datamaskinsystem. Oppstår det en hindring som tollvesenet er ansvarlig for, anses tolldeklarasjonen å være lagt frem når den er mottatt av nettverksleverandøren som mellommann og utskilt av denne for tollvesenet.

Tollvesenet skal uten ugrunnet opphold sende returnmelding til deklaranten etter at tolldeklarasjonen er behandlet. Returnmeldingen skal inneholde opplysninger som gjør det mulig å identifisere tolldeklarasjonen samt tidspunkt for når denne er mottatt.

Kongen kan gi nærmere bestemmelser om når andre meldinger skal anses å være lagt frem eller på annen måte få virkning etter sitt innhold.

§ 44. (nettverksleverandør som mellommann)

Kongen kan gi nærmere bestemmelser om plikter som kan pålegges nettverksleverandør som i forbindelse med elektronisk datautveksling opptrer som mellommann overfor tollvesenet.

Slike plikter kan blant annet omfatte:

- a. plikt til å føre et historisk register som inneholder alle meldinger slik de blir sendt og mottatt, opplysning om hvem som har sendt og mottatt disse og tidspunkt for når dette er skjedd, samt krav til registerets øvrige innhold, organisering, sikring og vedlikehold,
- b. plikt til vederlagsfritt å overlate registeret til tollvesenet etter en viss tid,

- c. plikt til å avgi bekreftet utskrift av registeret over meldinger utvekslet mellom tollvesenet og en annen innenfor en angitt tidsperiode, hvem som skal kunne kreve slik utskrift og i hvilken utstrekning det skal svares vederlag for slik bistand,
- d. prosedyrer for varsling og behandling av feil som oppstår under meldingsutvekslingen,
- e. hvilken adgang mellommannen har til å konvertere eller på annen måte gjøre endringer i meldinger som utveksles mellom tollvesenet og tredjemann samt hvordan slik konvertering eller endring kan skje, herunder de sikkerhetsrutiner mellommannen må iverksette ved leveringen av slike tjenester.

Rikstrykdeverket skal påse at avtaler med leverandører av varer og tjenester inneholder krav til leveringsdyktighet og informasjonssikkerhet ved kriser i freds- og krigstid.

Forskrift om elektronisk tilgang til opplysninger i ligningsforvaltningens registre (FIN)

I

§ 1. Skattedirektoratet kan gi offentlig myndighet som nevnt i ligningsloven § 3-13 nr. 2 bokstav a til c, bokstav f tredje punktum og bokstav h, elektronisk tilgang til opplysninger i ligningsforvaltningens registre.

§ 2. Den enkelte offentlige myndighet kan bare gis tilgang til de opplysningene som den kan ha bruk for i sitt arbeid, og som ligningsforvaltningen etter ligningsloven § 3-13 kan utlevere uten hinder av sin taushetsplikt.

§ 3. Opplysningene kan ikke brukes til annet formål enn det de er innhentet for. De kan ikke utleveres til andre offentlige myndigheter, privatpersoner eller lignende, med mindre dette følger av formålet eller skjer etter samtykke fra den opplysningene gjelder eller med hjemmel i lov.

§ 4. Skattedirektoratet gir nærmere retningslinjer om hvordan tilgang til opplysningene skal gis, om krav til informasjonssikkerhet som følger av personopplysningsloven med forskrifter og om betaling for opplysninger. Retningslinjene skal minst angi:

- a. regler om dokumentasjon av autorisert tilgang og forsøk på uautorisert tilgang til opplysninger i ligningsforvaltningens registre og om oppbevaring av slik dokumentasjon og
- b. regler om informasjonsplikt overfor den det innhentes opplysninger om.

II

Denne forskrift trer i kraft 1. januar 2004.

Forskrift om bruk av informasjons- og kommunikasjonsteknologi (IKT) (FIN)

Fastsatt av Kredittilsynet 21. mai 2003 med hjemmel i lov av 7. desember 1956 nr. 1 om tilsynet for kredittinstitusjoner, forsikringsselskaper og verdipapirhandel m.v. (kredittilsynsloven) § 4 nr. 2, lov av 17. november 2000 nr. 80 om børsvirksomhet m.m. (børsloven) § 3-4 første ledd annet punktum og lov av 17. desember 1999 nr. 95 om betalingssystemer m.v. § 3-3 første ledd annet punktum.

§ 5. Sikkerhet

Foretaket skal utarbeide prosedyrer som skal sikre beskyttelse av utstyr, systemer og informasjon av betydning for foretakets virksomhet, jf. § 1, mot skader, misbruk, uautorisert adgang og endring, samt hærverk. Videre skal prosedyrene inneholde retningslinjer for tildeling, endring, sletting og kontroll med autorisasjon for tilgang til IKT-systemene. Kravene til IKT-sikkerhet skal så langt det er praktisk mulig være målbare. Oppfyllelse av kravene til informasjonssikkerhet for personopplysninger etter forskrift av 15. desember 2000 nr. 1265 til personopplysningsloven skal anses som oppfyllelse av kravene i paragrafen her.

Forskrift om registrering av juridiske personer m.m. i Enhetsregisteret (FIN)

§ 23. Datasikkerhet

Det skal tas regelmessig sikkerhetskopi av det som er registrert i Enhetsregisterets database. Databehandlingen må dessuten tilrettelegges på en slik måte at kvaliteten av lagrede og avgitte opplysninger er tilstrekkelig god og slik at den blir best mulig beskyttet mot uønskede hendelser. Uhell, misbruk, feil og øvrige trusler mot datasikkerheten skal søkes avdekket og avverget så effektivt som mulig.

Forskrift om informasjonssikkerhet (FD)

Hele forskriften

Forskrift om sikkerhetsgraderte anskaffelser (FD)

§ 2-7. Gjennomføring av sikkerhetstiltak hos leverandøren

Leverandørens ansvar for en sikkerhetsgradert anskaffelse omfatter også ansvaret for den forebyggende sikkerhet. Mangler som leverandøren selv ikke kan rette på, skal straks rapporteres til anskaffelsesmyndigheten. Leverandøren skal også rapportere om sikkerhetstruende hendelser, jf. forskrift om sikkerhetsadministrasjon, og om forhold som reiser tvil om den sikkerhetsmessige skikkethet til noen som har befatning med den sikkerhetsgraderte anskaffelsen.

Personer som kan få tilgang til sikkerhetsgradert informasjon, herunder styre og daglig leder, skal sikkerhetsklareres og autoriseres i samsvar med sikkerhetsloven kapittel 6 og forskrift om personellsikkerhet. Leverandøren fremmer anmodninger om personklarering til anskaffelsesmyndigheten etter behov som vurderes av sikkerhetsleder.

Dersom det ikke er nødvendig eller mulig å gi et styremedlem sikkerhetsklarering, skal anskaffelsesmyndigheten innhente en erklæring om fraskrivelse av innsynsrett i skjermingsverdig informasjon fra vedkommende. Det kan utpekes stedfortredere som sikkerhetsklareres for styremedlemmer som ikke blir sikkerhetsklarert. Leverandøren skal rette seg etter øvrige gjeldende bestemmelser om sikkerhetsadministrasjon, personellsikkerhet, informasjonssikkerhet og objektsikkerhet.

Anskaffelsesmyndigheten skal foreta sikkerhetsinspeksjon hos leverandøren før leverandørklarering kan gis.

Når anskaffelsesmyndigheten har brakt på det rene at sikkerhetstiltak etter lov, forskrift og pålegg er gjennomført, meddeles dette skriftlig til NSM.

Anskaffelsesmyndigheten skal sørge for at leverandøren inspiseres jevnlig og minst en gang hver 18. måned i løpet av anskaffelsen. Anskaffelsesmyndigheten kan pålegge underordnede anskaffelsesmyndigheter eller bemyndige andre anskaffelsesmyndigheter å utføre inspeksjon dersom det er hensiktsmessig.

I forbindelse med inspeksjoner nevnt i denne paragraf skal anskaffelsesmyndigheten utarbeide inspeksjonsrapport. Inspeksjonsrapporten skal formidles til leverandøren med kopi til NSM.

Forskrift om sikkerhetsinformasjon (FD)

Hele forskriften kan være aktuell

Forskrift om personellsikkerhet (FD)

Hele forskriften kan være aktuell

Forskrift om register for lagring av opplysninger innsamlet ved bruk av satellittsporingssystemer på fiskefartøy (FKD)

Fastsatt av Fiskeridepartementet 7. april 1999 med hjemmel i lov av 3. juni 1983 nr. 40 om saltvannsfiske m.v. § 45 femte ledd.

§ 10. Sikkerhet

Den registeransvarlige skal iverksette og holde vedlike nødvendige sikkerhetstiltak, slik at hensynet til opplysningenes konfidensialitet, integritet og tilgjengelighet til enhver tid er tilstrekkelig ivaretatt.

Brudd på informasjonssikkerheten som har medført uautorisert utlevering av sensitive personopplysninger, eller ved mistanke om slik utlevering, skal meddeles Datatilsynet.

Lov om helseregistre og behandling av helseopplysninger (helseregisterloven) (HOD)

§ 16. Sikring av konfidensialitet, integritet, kvalitet og tilgjengelighet

Den databehandlingsansvarlige og databehandleren skal gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet, kvalitet og tilgjengelighet ved behandling av helseopplysninger.

For å oppnå tilfredsstillende informasjonssikkerhet skal den databehandlingsansvarlige og databehandleren dokumentere informasjonssystemet og sikkerhetstiltakene. Dokumentasjonen skal være tilgjengelig for medarbeiderne hos den databehandlingsansvarlige og hos databehandleren. Dokumentasjonen skal også være tilgjengelig for tilsynsmyndighetene.

En databehandlingsansvarlig som lar andre få tilgang til helseopplysninger, for eksempel en databehandler eller andre som utfører oppdrag i tilknytning til informasjonssystemet, skal påse at disse oppfyller kravene i første og annet ledd.

Kongen kan gi forskrift om sikkerhet ved behandling av helseopplysninger etter denne lov. Kongen kan herunder sette nærmere krav til elektronisk signatur, kommunikasjon og langtidslagring, om godkjenning (autorisasjon) av programvare og om bruk av standarder, klassifikasjonssystemer og kodeverk, samt hvilke nasjonale eller internasjonale standardssystemer som skal følges.

Forskrift om pasientjournal (HOD)

§ 4. (Journalssystem)

Virksomhet hvor det ytes helsehjelp må opprette pasientjournalssystem. Systemet må organiseres slik at det er mulig å etterleve krav fastsatt i eller i medhold av lov, blant annet regler om:

- a) innsyn i journal, jf. helsepersonelloven § 41 og pasientrettighetsloven § 5-1,
- b) tilgang til og utlevering av journal, jf. helsepersonelloven § 25 og § 45 samt pasientrettighetsloven § 5-3,
- c) meldeplikter og opplysningsplikter, jf. helsepersonelloven kapittel 6 og 7,
- d) redigering av journal, jf. helsepersonelloven § 39 andre ledd,
- e) retting og sletting, jf. helsepersonelloven § 42, § 43 og § 44 og
- f) sikring mot innsyn fra uvedkommende, jf. helsepersonelloven kapittel 5, herunder forsvarlig oppbevaring, jf. helsepersonelloven § 21.

Forskrift om innsamling og behandling av helseopplysninger i Reseptbasert legemiddelregister (Reseptregisteret) (HOD)

Kapittel 4. Taushetsplikt, informasjonssikkerhet og internkontroll

§ 4-1. Forbud mot samtidig tilgang

Ingen, verken TPF, databehandler eller databehandlingsansvarlig, skal kunne få samtidig tilgang til pseudonym, reseptopplysninger og fødselsnummer eller helsepersonellnummer.

§ 4-2. Tilgang til Reseptregisteret

Bare den databehandlingsansvarlige, databehandlere og den som arbeider under den databehandlingsansvarliges eller databehandlers instruksjonsmyndighet, kan gis tilgang til Reseptregisteret. Tilgang kan bare gis i den grad dette er nødvendig for vedkommendes arbeid og i samsvar med gjeldende bestemmelser om taushetsplikt.

§ 4-3. Behandling av opplysninger

Den databehandlingsansvarlige og databehandler skal gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet, kvalitet og tilgjengelighet ved behandling av opplysninger omhandlet i forskriften, se helseregisterloven § 16.

§ 4-4. Taushetsplikt

Enhver som behandler opplysninger etter denne forskriften, har taushetsplikt etter helseregisterloven § 15.

§ 4-5. Plikt til å sørge for internkontroll

Den databehandlingsansvarlige skal etablere internkontroll i samsvar med helseregisterloven § 17. De systematiske tiltakene skal tilpasses virksomhetens art, aktiviteter og størrelse i det omfang det er nødvendig for å etterleve krav gitt i eller i medhold av helseregisterloven, med særlig vekt på bestemmelser gitt i medhold av helseregisterloven § 16.

§ 4-6. Innholdet i internkontrollen

Internkontrollen innebærer at den databehandlingsansvarlige skal ha kunnskap om gjeldende regler om behandling av helseopplysninger, tilstrekkelig og oppdatert dokumentasjon for gjennomføring av rutiner, og har denne dokumentasjonen tilgjengelig for dem den måtte angå.

Dokumentasjonen av internkontrollen skal minst inneholde

1. oversikt over hvordan virksomheten er organisert,
2. oversikt over ansvars- og myndighetsforhold,
3. oversikt over de krav i og i medhold av helseregisterloven som gjelder for virksomheten,
4. rutiner virksomheten følger for å sikre at kravene blir overholdt,
5. rutiner virksomheten følger dersom avvik oppstår, og opplysninger om hvem som er ansvarlig for at rutinene blir overholdt,
6. rutiner virksomheten følger for å hindre gjentakelse av avvik og opplysninger om hvem som er ansvarlig,
7. rutiner for hvordan virksomheten systematisk og regelmessig gjennomgår sin

internkontroll for å kontrollere at aktivitetene og resultatene av dem stemmer overens med det systemet virksomheten har fastlagt, og om det medfører oppfyllelse av helseregisterlovgivningen,

8. rutiner for hvordan virksomheten sikrer at de ansatte har tilstrekkelig kompetanse til å overholde forskriftens krav.

Skriftlig dokumentasjon skal minst omfatte dokumentasjon av rutiner som nevnt i annet ledd nr. 1 til 8. Tilsynsmyndighetene kan gi pålegg om skriftlig dokumentasjon ut over dette, dersom det anses påkrevet. Tilsynsmyndighetene kan dispensere fra hele eller deler av dette kapitlet når særlige forhold foreligger.

Forskrift om innsamling og behandling av helseopplysninger i Norsk overvåkingssystem for antibiotikaresistens hos mikrober (NORM-registerforskriften) (HOD)

Kapittel 4. Informasjonssikkerhet og internkontroll

§ 4-1. (Informasjonssikkerhet)

Nasjonalt folkehelseinstitutt og databehandleren skal gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet, kvalitet og tilgjengelighet ved behandling av opplysninger etter forskriften, jf. helseregisterloven § 16 flg.

Der behandling av opplysningene skjer helt eller delvis med elektroniske hjelpemidler, gjelder bestemmelsene om informasjonssikkerhet i personopplysningsforskriften § 2-1 til § 2-16.

§ 4-2. (Plikt til internkontroll)

Nasjonalt folkehelseinstitutt skal etablere internkontroll i samsvar med helseregisterloven § 17. De systematiske tiltakene skal tilpasses virksomhetens art, aktiviteter og størrelse i det omfang det er nødvendig for å etterleve krav gitt i eller i medhold av helseregisterloven, med særlig vekt på bestemmelser gitt i medhold av helseregisterloven § 16.

Databehandler som behandler helseopplysninger på vegne av Nasjonalt folkehelseinstitutt, skal behandle opplysninger i samsvar med rutiner Nasjonalt folkehelseinstitutt har oppstilt.

§ 4-3. (Internkontrollens innhold)

Internkontrollen innebærer at Nasjonalt folkehelseinstitutt skal ha kunnskap om gjeldende regler om behandling av helseopplysninger, tilstrekkelig og oppdatert dokumentasjon for gjennomføring av rutiner, samt ha denne dokumentasjonen tilgjengelig for dem det måtte angå.

Internkontrollen skal blant annet inneholde:

1. oversikt over hvordan virksomheten er organisert,

2. oversikt over ansvars- og myndighetsforhold,
3. oversikt over de krav i og i medhold av helseregisterloven som gjelder for virksomheten,
4. rutiner virksomheten følger for å sikre overholdelse av kravene, herunder rutiner for:
 - 4.1. dokumentasjon og kvalitetskontroll av helseopplysningene, jf. forskriften § 1-8,
 - 4.2. hvordan virksomheten oppfyller bestemmelsene om tilgang til helseregistre, jf. forskriften § 3-1 og § 3-2,
 - 4.3. oppfyllelse av reglene om meldeplikt til Datatilsynet, jf. helseregisterloven § 29,
5. rutiner virksomheten følger dersom avvik oppstår, og opplysninger om hvem som er ansvarlig,
6. rutiner virksomheten følger for å hindre gjentakelse av avvik, og opplysninger om hvem som er ansvarlig,
7. rutiner for hvordan virksomheten systematisk og regelmessig gjennomgår sin internkontroll for å kontrollere at aktivitetene og resultatene av dem stemmer overens med det system virksomheten har fastlagt, og om det medfører oppfyllelse av helseregisterlovgivningen,
8. rutiner for hvordan virksomheten sikrer seg at alle aktuelle og kun gjeldende rutiner blir benyttet, og
9. rutiner for hvordan virksomheten sikrer at de ansatte har tilstrekkelig kompetanse til å overholde forskriftens krav.

Skriftlig dokumentasjon skal minst omfatte dokumentasjon av rutiner som nevnt i annet ledd nr. 1 til 8. Tilsynsmyndighetene kan gi pålegg om skriftlig dokumentasjon ut over dette, dersom det anses påkrevet. Tilsynsmyndigheten kan dispensere fra hele eller deler av dette kapittel når særlige forhold foreligger.

Forskrift om innsamling og behandling av helseopplysninger i Dødsårsaksregisteret (Dødsårsaksregisterforskriften) (HOD)

Kapittel 4. Taushetsplikt, informasjonssikkerhet og internkontroll

§ 4-1. (Taushetsplikt)

Enhver som behandler helseopplysninger etter denne forskriften har taushetsplikt etter forvaltningsloven § 13 til § 13e, samt etter helsepersonelloven.

Taushetsplikten etter første ledd gjelder også pasientens fødested, fødselsdato, personnummer, pseudonym, statsborgerforhold, sivilstand, yrke, bopel og arbeidssted.

Opplysninger til andre forvaltningsorganer etter forvaltningsloven § 13b nr. 5 og 6 kan bare gis når det er nødvendig for å bidra til løsning av oppgaver etter forskriften her, eller for å forebygge vesentlig fare for liv eller alvorlig skade for noens helse.

§ 4-2. (Informasjonssikkerhet)

Nasjonalt folkehelseinstitutt og databehandleren skal gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet, kvalitet og tilgjengelighet ved behandling av helseopplysninger etter forskriften, jf. helseregisterloven § 16 flg.

Der behandling av helseopplysningene skjer helt eller delvis med elektroniske hjelpemidler, gjelder bestemmelsene om informasjonssikkerhet i personopplysningsforskriften § 2-1 til § 2-16.

§ 4-3. (Plikt til internkontroll)

Nasjonalt folkehelseinstitutt skal etablere internkontroll i samsvar med helseregisterloven § 17. De systematiske tiltakene skal tilpasses virksomhetens art, aktiviteter og størrelse i det omfang det er nødvendig for å etterleve krav gitt i eller i medhold av helseregisterloven, med særlig vekt på bestemmelser gitt i medhold av helseregisterloven § 16.

Databehandlere som behandler helseopplysninger på vegne av Nasjonalt folkehelseinstitutt, skal behandle opplysninger i samsvar med rutiner Nasjonalt folkehelseinstitutt har oppstilt.

§ 4-4. (Internkontrollens innhold)

Internkontrollen innebærer at den databehandlingsansvarlige skal ha kunnskap om gjeldende regler om behandling av helseopplysninger, tilstrekkelig og oppdatert dokumentasjon for gjennomføring av rutiner, samt ha denne dokumentasjonen tilgjengelig for dem den måtte angå. Internkontrollen skal blant annet inneholde:

1. oversikt over hvordan virksomheten er organisert,
2. oversikt over ansvars- og myndighetsforhold,
3. oversikt over de krav i og i medhold av helseregisterloven som gjelder for virksomheten,
4. rutiner virksomheten følger for å sikre overholdelse av kravene, herunder rutiner for:
 - 4.1. oppfyllelse av krav om at personidentifiserende opplysninger bare behandles når dette er nødvendig for å fremme formålet med behandlingen av opplysningene, og i tråd med gjeldende bestemmelser om taushetsplikt, jf. helseregisterloven § 11 og § 15,

- 4.2. kvalitetskontroll og dokumentasjon av helseopplysningene, jf. forskriften § 1-7 og § 2-6,
- 4.3. oppfyllelse av begjæringer om informasjon og innsyn, jf. helseregisterloven § 21, § 22 og § 25, samt forskriften § 5-1,
- 4.4. hvordan virksomheten oppfyller bestemmelsene om tilgang til helseregistre, jf. § 3-1, § 3-3, § 3-4 og § 3-5,
- 4.5. oppfyllelse av reglene om meldeplikt til Datatilsynet, jf. helseregisterloven § 29,
5. rutiner virksomheten følger dersom avvik oppstår og opplysninger om hvem som er ansvarlig,
6. rutiner virksomheten følger for å hindre gjentakelse av avvik og opplysninger om hvem som er ansvarlig,
7. rutiner for hvordan virksomheten systematisk og regelmessig gjennomgår sin internkontroll for å kontrollere at aktivitetene og resultatene av dem stemmer overens med det system virksomheten har fastlagt, og om det medfører oppfyllelse av helseregisterlovgivningen,
8. rutiner for hvordan virksomheten sikrer seg at alle aktuelle og kun gjeldende rutiner blir benyttet, og
9. rutiner for hvordan virksomheten sikrer at de ansatte har tilstrekkelig kompetanse til å overholde forskriftens krav.

Skriftlig dokumentasjon skal minst omfatte dokumentasjon av rutiner som nevnt i første ledd nr. 1 til 8. Tilsynsmyndighetene kan gi pålegg om skriftlig dokumentasjon ut over dette dersom det anses påkrevet. Tilsynsmyndighetene kan dispensere fra hele eller deler av dette kapittel når særlige forhold foreligger.

Forskrift om innsamling og behandling av helseopplysninger i Krefregisteret (Krefregisterforskriften) (HOD)

Kapittel 4. Taushetsplikt, informasjonssikkerhet, internkontroll

§ 4-1. (Taushetsplikt)

Enhver som behandler helseopplysninger etter denne forskriften har taushetsplikt etter forvaltningsloven § 13 til § 13e, samt etter helsepersonelloven.

Taushetsplikten etter første ledd gjelder også pasientens fødested, fødselsdato, personnummer, pseudonym, statsborgerforhold, sivilstand, yrke, bopel og arbeidssted.

Opplysninger til andre forvaltningsorganer etter forvaltningsloven § 13b nr. 5 og 6 kan bare gis når det er nødvendig for å bidra til løsning av oppgaver etter forskriften her, eller for å forebygge vesentlig fare for liv eller alvorlig skade for noens helse.

§ 4-2. (Informasjonssikkerhet)

Den databehandlingsansvarlige for Kreftregisteret og databehandleren skal gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet, kvalitet og tilgjengelighet ved behandling av helseopplysninger etter forskriften, jf. helseregisterloven § 16 flg.

Der behandling av helseopplysningene skjer helt eller delvis med elektroniske hjelpemidler, gjelder bestemmelsene om informasjonssikkerhet i personopplysningsforskriften § 2-1 til § 2-16.

§ 4-3. (Plikt til internkontroll)

Den databehandlingsansvarlige for Kreftregisteret skal etablere internkontroll i samsvar med helseregisterloven § 17. De systematiske tiltakene skal tilpasses virksomhetens art, aktiviteter og størrelse i det omfang det er nødvendig for å etterleve krav gitt i eller i medhold av helseregisterloven, med særlig vekt på bestemmelser gitt i medhold av helseregisterloven § 16.

Databehandlere som behandler helseopplysninger på vegne av den databehandlingsansvarlige, skal behandle opplysninger i samsvar med rutiner databehandlingsansvarlig har oppstilt.

§ 4-4. (Internkontrollens innhold)

Internkontroll innebærer at den databehandlingsansvarlige skal ha kunnskap om gjeldende regler om behandling av helseopplysninger, tilstrekkelig og oppdatert dokumentasjon for gjennomføring av rutiner, samt ha denne dokumentasjonen tilgjengelig for dem den måtte angå. Internkontrollen skal blant annet inneholde:

1. oversikt over hvordan virksomheten er organisert,
2. oversikt over ansvars- og myndighetsforhold,
3. oversikt over de krav i og i medhold av helseregisterloven som gjelder for virksomheten,
4. rutiner virksomheten følger for å sikre overholdelse av kravene, herunder rutiner for:
 - 4.1. oppfyllelse av krav om at personidentifiserende opplysninger bare behandles når dette er nødvendig for å fremme formålet med behandlingen av opplysningene, og i tråd med gjeldende bestemmelser om taushetsplikt, jf. helseregisterloven § 11 og § 15,
 - 4.2. dokumentasjon og kvalitetskontroll av helseopplysningene, jf. forskriften § 1-11 og § 2-4,

- 4.3. oppfyllelse av begjæringer om informasjon og innsyn, jf. helseregisterloven § 21 til § 25, samt forskriften § 5-1,
- 4.4. hvordan virksomhetene oppfyller bestemmelsene om tilgang til helseregistre, jf. § 3-1, § 3-3, § 3-4 og § 3-5,
- 4.5. oppfyllelse av reglene om meldeplikt til Datatilsynet, jf. helseregisterloven § 29,
5. rutiner virksomheten følger dersom avvik oppstår og opplysninger om hvem som er ansvarlig,
6. rutiner virksomheten følger for å hindre gjentakelse av avvik og opplysninger om hvem som er ansvarlig,
7. rutiner for hvordan virksomheten systematisk og regelmessig gjennomgår sin internkontroll for å kontrollere at aktivitetene og resultatene av dem stemmer overens med det system virksomheten har fastlagt, og om det medfører oppfyllelse av helseregisterlovgivningen,
8. rutiner for hvordan virksomheten sikrer seg at alle aktuelle og kun gjeldende rutiner blir benyttet, og
9. rutiner for hvordan virksomheten sikrer at de ansatte har tilstrekkelig kompetanse til å overholde forskriftens krav.

Skriftlig dokumentasjon skal minst omfatte dokumentasjon av rutiner som nevnt i første ledd nr. 1 til 8. Tilsynsmyndighetene kan gi pålegg om skriftlig dokumentasjon ut over dette dersom det anses påkrevet. Tilsynsmyndighetene kan dispensere fra hele eller deler av dette kapittel når særlige forhold foreligger.

Forskrift om innsamling og behandling av helseopplysninger i Medisinsk fødselsregister (Medisinsk fødselsregisterforskriften) (HOD)

Kapittel 4. Taushetsplikt, informasjonssikkerhet og internkontroll

§ 4-1. (Taushetsplikt)

Enhver som behandler helseopplysninger etter denne forskriften har taushetsplikt etter forvaltningsloven § 13 til § 13e, samt etter helsepersonelloven.

Taushetsplikten etter første ledd gjelder også pasientens fødested, fødselsdato, personnummer, statsborgerforhold, sivilstand, yrke, bopel og arbeidssted.

Opplysninger til andre forvaltningsorganer etter forvaltningsloven § 13b nr. 5 og 6 kan bare gis når det er nødvendig for å bidra til løsning av oppgaver etter forskriften her, eller for å forebygge vesentlig fare for liv eller alvorlig skade for noens helse.

§ 4-2. (Informasjonssikkerhet)

Nasjonalt folkehelseinstitutt og databehandleren skal gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet, kvalitet og tilgjengelighet ved behandling av helseopplysninger etter forskriften, jf. helseregisterloven § 16 flg.

Der behandling av helseopplysningene skjer helt eller delvis med elektroniske hjelpemidler, gjelder bestemmelsene om informasjonssikkerhet i forskrift til personopplysningsloven § 2-1 til § 2-16.

§ 4-3. (Plikt til internkontroll)

Nasjonalt folkehelseinstitutt skal etablere internkontroll i samsvar med helseregisterloven § 17. De systematiske tiltakene skal tilpasses virksomhetens art, aktiviteter og størrelse i det omfang det er nødvendig for å etterleve krav gitt i eller i medhold av helseregisterloven, med særlig vekt på bestemmelser gitt i medhold av helseregisterloven § 16.

Databehandlere som behandler helseopplysninger på vegne av den databehandlingsansvarlige, skal behandle opplysninger i samsvar med rutiner databehandlingsansvarlig har oppstilt.

§ 4-4. (Internkontrollens innhold)

Internkontrollen innebærer at den databehandlingsansvarlige skal ha kunnskap om gjeldende regler om behandling av helseopplysninger, tilstrekkelig og oppdatert dokumentasjon for gjennomføring av rutiner, samt ha denne dokumentasjonen tilgjengelig for dem den måtte angå. Internkontrollen skal blant annet inneholde:

1. oversikt over hvordan virksomheten er organisert,
2. oversikt over ansvars- og myndighetsforhold,
3. oversikt over de krav i og i medhold av helseregisterloven som gjelder for virksomheten,
4. rutiner virksomheten følger for å sikre overholdelse av kravene, herunder, rutiner for:
 - 4.1. oppfyllelse av krav om at personidentifiserende opplysninger bare behandles når dette er nødvendig for å fremme formålet med behandlingen av opplysningene, og i tråd med gjeldende bestemmelser om taushetsplikt, jf. helseregisterloven § 11 og § 15 og forskriften § 1-11,
 - 4.2. kvalitetskontroll og dokumentasjon av helseopplysningene, jf. forskriften § 1-13 og § 2-4,

- 4.3. oppfyllelse av begjæringer om informasjon og innsyn, jf. helseregisterloven § 21 til § 25, samt forskriften § 5-1,
- 4.4. for hvordan virksomheten oppfyller bestemmelsene om tilgang til helseregistre, jf. § 3-1, § 3-3, § 3-4 og § 3-5,
- 4.5. oppfyllelse av reglene om meldeplikt til Datatilsynet, jf. helseregisterloven § 29,
5. rutiner virksomheten følger dersom avvik oppstår og opplysninger om hvem som er ansvarlig,
6. rutiner virksomheten følger for å hindre gjentakelse av avvik og opplysninger om hvem som er ansvarlig,
7. rutiner for hvordan virksomheten systematisk og regelmessig gjennomgår sin internkontroll for å kontrollere at aktivitetene og resultatene av dem stemmer overens med det system virksomheten har fastlagt, og om det medfører oppfyllelse av helseregisterlovgivningen,
8. rutiner for hvordan virksomheten sikrer seg at alle aktuelle og kun gjeldende rutiner blir benyttet, og
9. rutiner for hvordan virksomheten sikrer at de ansatte har tilstrekkelig kompetanse til å overholde forskriftens krav.

Skriftlig dokumentasjon skal minst omfatte dokumentasjon av rutiner som nevnt i første ledd nr. 1 til 8. Tilsynsmyndighetene kan gi pålegg om skriftlig dokumentasjon ut over dette dersom det anses påkrevet. Tilsynsmyndighetene kan dispensere fra hele eller deler av dette kapittel når særlige forhold foreligger.

Forskrift om innsamling og behandling av helseopplysninger i System for vaksinasjonskontroll (SYSVAK-registerforskriften) (HOD)

Kapittel 4. Taushetsplikt, informasjonssikkerhet og internkontroll

§ 4-1. (Taushetsplikt)

Enhver som behandler helseopplysninger etter denne forskriften, har taushetsplikt etter forvaltningsloven § 13 til § 13e, samt etter helsepersonelloven.

Taushetsplikten etter første ledd gjelder også pasientens fødested, fødselsdato, personnummer, statsborgerforhold, sivilstand, yrke, bopel og arbeidssted eller andre personentydige opplysninger jf. forskriften § 1-7 annet ledd.

Opplysninger til andre forvaltningsorganer etter forvaltningsloven § 13b nr. 5 og 6 kan bare gis når det er nødvendig for å bidra til løsning av oppgaver etter forskriften her, eller for å forebygge vesentlig fare for liv eller alvorlig skade for noens helse.

§ 4-2. (Informasjonssikkerhet)

Nasjonalt folkehelseinstitutt og databehandleren skal gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet, kvalitet og tilgjengelighet ved behandling av helseopplysninger etter forskriften, jf. helseregisterloven § 16 flg

Der behandling av helseopplysningene skjer helt eller delvis med elektroniske hjelpemidler, gjelder bestemmelsene om informasjonssikkerhet i forskrift til personopplysningsloven § 2-1 til § 2-16.

§ 4-3. (Plikt til internkontroll)

Nasjonalt folkehelseinstitutt skal etablere internkontroll i samsvar med helseregisterloven § 17. De systematiske tiltakene skal tilpasses virksomhetens art, aktiviteter og størrelse i det omfang som er nødvendig for å etterleve krav gitt i eller i medhold av helseregisterloven, med særlig vekt på bestemmelser gitt i medhold av helseregisterloven § 16.

Databehandlere som behandler helseopplysninger på vegne av Nasjonalt folkehelseinstitutt, skal behandle opplysninger i samsvar med rutiner Nasjonalt folkehelseinstitutt har oppstilt.

§ 4-4. (Internkontrollens innhold)

Internkontrollen innebærer at den databehandlingsansvarlige skal ha kunnskap om gjeldende regler om behandling av helseopplysninger, tilstrekkelig og oppdatert dokumentasjon for gjennomføring av rutiner, samt ha denne dokumentasjonen tilgjengelig for dem den måtte angå.

Internkontrollen skal blant annet inneholde:

1. oversikt over hvordan virksomheten er organisert,
2. oversikt over ansvars- og myndighetsforhold,
3. oversikt over de krav i og i medhold av helseregisterloven som gjelder for virksomheten,
4. rutiner virksomheten følger for å sikre overholdelse av kravene, herunder rutiner for:
 - 4.1. oppfyllelse av krav om at personidentifiserende opplysninger bare behandles når dette er nødvendig for å fremme formålet med behandlingen av opplysningene, og i tråd med gjeldende bestemmelser om taushetsplikt, jf. helseregisterloven § 11 og § 15,
 - 4.2. dokumentasjon og kvalitetskontroll av helseopplysningene, jf. forskriften § 1-8 og § 2-5,

- 4.3. oppfyllelse av begjæringer om informasjon og innsyn, jf. helseregisterloven § 21 til § 25, samt forskriften § 5-1,
- 4.4. hvordan virksomheten oppfyller bestemmelsene om tilgang til helseregistre, jf. § 3-1, § 3-3, § 3-4 og § 3-5,
- 4.5. oppfyllelse av reglene om meldeplikt til Datatilsynet, jf. helseregisterloven § 29,
5. rutiner virksomheten følger dersom avvik oppstår, og opplysninger om hvem som er ansvarlig,
6. rutiner virksomheten følger for å hindre gjentakelse av avvik, og opplysninger om hvem som er ansvarlig,
7. rutiner for hvordan virksomheten systematisk og regelmessig gjennomgår sin internkontroll for å kontrollere at aktivitetene og resultatene av dem stemmer overens med det system virksomheten har fastlagt, og om det medfører oppfyllelse av helseregisterlovgivningen,
8. rutiner for hvordan virksomheten sikrer seg at alle aktuelle og kun gjeldende rutiner blir benyttet, og
9. rutiner for hvordan virksomheten sikrer at de ansatte har tilstrekkelig kompetanse til å overholde forskriftens krav.

Skriftlig dokumentasjon skal minst omfatte dokumentasjon av rutiner som nevnt i annet ledd nr. 1 til 8. Tilsynsmyndighetene kan gi pålegg om skriftlig dokumentasjon ut over dette, dersom det anses påkrevet. Tilsynsmyndighetene kan dispensere fra hele eller deler av dette kapittel når særlige forhold foreligger.

Forskrift om innsamling og behandling av helseopplysninger i Meldingssystem for smittsomme sykdommer og i Tuberkuloseregisteret og om varsling om smittsomme sykdommer (MSIS- og Tuberkuloseregisterforskriften) (HOD)

Kapittel 5. Taushetsplikt, informasjonssikkerhet og internkontroll

§ 5-1. (Taushetsplikt)

Enhver som behandler helseopplysninger etter denne forskriften, har taushetsplikt etter forvaltningsloven § 13 til § 13e, samt etter helsepersonelloven.

Taushetsplikten etter første ledd gjelder også pasientens fødested, fødselsdato, personnummer, pseudonym, statsborgerforhold, sivilstand, yrke, bopel og arbeidssted.

Opplysninger til andre forvaltningsorganer etter forvaltningsloven § 13b nr. 5 og 6 kan bare gis når det er nødvendig for å bidra til løsning av oppgaver etter forskriften her, eller for å forebygge vesentlig fare for liv eller alvorlig skade for noens helse.

§ 5-2. (Informasjonssikkerhet)

Nasjonalt folkehelseinstitutt og databehandleren skal gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet, kvalitet og tilgjengelighet ved behandling av helseopplysninger etter forskriften, jf. helseregisterloven § 16 flg.

Der behandling av helseopplysningene skjer helt eller delvis med elektroniske hjelpemidler, gjelder bestemmelsene om informasjonssikkerhet i personopplysningsforskriften § 2-1 til § 2-16.

§ 5-3. (Plikt til internkontroll)

Nasjonalt folkehelseinstitutt skal etablere internkontroll i samsvar med helseregisterloven § 17. De systematiske tiltakene skal tilpasses virksomhetens art, aktiviteter og størrelse i det omfang som er nødvendig for å etterleve krav gitt i eller i medhold av helseregisterloven, med særlig vekt på bestemmelser gitt i medhold av helseregisterloven § 16.

Databehandleren som behandler helseopplysninger på vegne av Nasjonalt folkehelseinstitutt, skal behandle opplysninger i samsvar med rutiner Nasjonalt folkehelseinstitutt har oppstilt.

§ 5-4. (Internkontrollens innhold)

Internkontrollen innebærer at den databehandlingsansvarlige skal ha kunnskap om gjeldende regler om behandling av helseopplysninger, tilstrekkelig og oppdatert dokumentasjon for gjennomføring av rutiner, samt ha denne dokumentasjonen tilgjengelig for dem det måtte angå.

Internkontrollen skal blant annet inneholde:

1. oversikt over hvordan virksomheten er organisert,
2. oversikt over ansvars- og myndighetsforhold,
3. oversikt over de krav i og i medhold av helseregisterloven som gjelder for virksomheten,
4. rutiner virksomheten følger for å sikre overholdelse av kravene, herunder rutiner for:
 - 4.1. oppfyllelse av krav om at personidentifiserende opplysninger bare behandles når dette er nødvendig for å fremme formålet med behandlingen av opplysningene, og i tråd med gjeldende bestemmelser om taushetsplikt, jf. helseregisterloven § 11 og § 15,
 - 4.2. dokumentasjon og kvalitetskontroll av helseopplysningene, jf. forskriften § 1-10 og § 2-6,
 - 4.3. oppfyllelse av begjæringer om informasjon og innsyn, jf. helseregisterloven § 21 til § 25, samt forskriften § 6-2,

- 4.4. hvordan virksomheten oppfyller bestemmelsene om tilgang til helseregistre, jf. § 4-1, § 4-3, § 4-4 og § 4-5,
- 4.5. oppfyllelse av reglene om meldeplikt til Datatilsynet, jf. helseregisterloven § 29,
5. rutiner virksomheten følger dersom avvik oppstår, og opplysninger om hvem som er ansvarlig,
6. rutiner virksomheten følger for å hindre gjentakelse av avvik, og opplysninger om hvem som er ansvarlig,
7. rutiner for hvordan virksomheten systematisk og regelmessig gjennomgår sin internkontroll for å kontrollere at aktivitetene og resultatene av dem stemmer overens med det system virksomheten har fastlagt, og om det medfører oppfyllelse av helseregisterlovgivningen,
8. rutiner for hvordan virksomheten sikrer seg at alle aktuelle og kun gjeldende rutiner blir benyttet, og
9. rutiner for hvordan virksomheten sikrer at de ansatte har tilstrekkelig kompetanse til å overholde forskriftens krav.

Skriftlig dokumentasjon skal minst omfatte dokumentasjon av rutiner som nevnt i annet ledd nr. 1 til 8. Tilsynsmyndighetene kan gi pålegg om skriftlig dokumentasjon ut over dette, dersom det anses påkrevet. Tilsynsmyndighetene kan dispensere fra hele eller deler av dette kapittel når særlige forhold foreligger.

Lov om behandling av personopplysninger (personopplysningsloven) (JD)

§ 13. Informasjonssikkerhet

Den behandlingsansvarlige og databehandleren skal gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger.

For å oppnå tilfredsstillende informasjonssikkerhet skal den behandlingsansvarlige og databehandleren dokumentere informasjonssystemet og sikkerhetstiltakene. Dokumentasjonen skal være tilgjengelig for medarbeiderne hos den behandlingsansvarlige og hos databehandleren. Dokumentasjonen skal også være tilgjengelig for Datatilsynet og Personvernemnda.

En behandlingsansvarlig som lar andre få tilgang til personopplysninger, f.eks. en databehandler eller andre som utfører oppdrag i tilknytning til informasjonssystemet, skal påse at disse oppfyller kravene i første og annet ledd.

Kongen kan gi forskrift om informasjonssikkerhet ved behandling av personopplysninger, herunder nærmere regler om organisatoriske og tekniske sikkerhetstiltak.

Forskrift til lov om Schengen informasjonssystem (SIS-forskriften) (JD)

Kapittel 7. Internkontroll og informasjonssikkerhet

§ 7-1. Internkontroll

Den registeransvarlige og databehandleren (øvrige myndighetene som har tilgang til SIS) skal etablere og holde vedlike planlagte systematiske tiltak (internkontroll) som er nødvendig for å oppfylle kravene i SIS-loven og bestemmelser gitt i medhold av SIS-loven.

Tiltakene skal særlig legge vekt på å sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger i SIS. Tiltakene skal stå i forhold til sannsynligheten for og konsekvensene av sikkerhetsbrudd.

Med konfidensialitet menes beskyttelse mot utilsiktet innsyn, med tilgjengelighet menes tilsiktet innsyn, og med integritet menes beskyttelse mot utilsiktet endring.

§ 7-2. Pålegg om sikring av opplysninger i SIS

Datatilsynet kan gi pålegg om sikring av opplysninger og herunder fastlegge kriterier for akseptabel risiko forbundet med behandlingen av opplysninger.

§ 7-3. Sikkerhetsledelse

Den registeransvarlige og lederen av de myndigheter som har direkte tilgang til SIS har ansvar for at bestemmelsene i dette kapitlet følges.

Formålet med behandling av opplysninger og overordnede føringer for bruk av informasjonsteknologi, skal beskrives i sikkerhetsmål.

Valg og prioriteringer i sikkerhetsarbeidet skal beskrives i en sikkerhetsstrategi.

Bruk av informasjonssystemet skal jevnlig gjennomgås for å klarlegge om den er hensiktsmessig i forhold til virksomhetens behov, og om sikkerhetsstrategien gir tilfredsstillende informasjonssikkerhet som resultat.

Resultat fra gjennomgangen skal dokumenteres og benyttes som grunnlag for eventuell endring av sikkerhetsmål og -strategi.

§ 7-4. Risikovurdering

Ved endringer som har betydning for informasjonssikkerheten skal risikovurdering gjennomføres for å klarlegge sannsynligheten for, og konsekvenser av sikkerhetsbrudd.

Resultat fra risikovurdering skal sammenlignes med fastlagte kriterier for akseptabel risiko forbundet med behandlingen av opplysninger.

Resultat av risikovurdering skal dokumenteres.

§ 7-5. Sikkerhetsrevisjon

Sikkerhetsrevisjon av bruk av informasjonssystemet skal gjennomføres jevnlig.

Sikkerhetsrevisjon skal omfatte vurdering av organisering, sikkerhetstiltak og bruk av kommunikasjonsparter og leverandører.

Dersom sikkerhetsrevisjon avdekker bruk av informasjonssystemet som ikke er forutsatt, skal dette behandles som avvik jf. § 7-6.

Resultat fra sikkerhetsrevisjon skal dokumenteres.

§ 7-6. Avvik

Bruk av informasjonssystemet som er i strid med fastlagte rutiner, og sikkerhetsbrudd, skal behandles som avvik.

Avviksbehandlingen skal ha som formål å gjenopprette normal tilstand, fjerne årsaken til avviket og hindre gjentakelse.

Dersom avviket har medført uautorisert utlevering av opplysninger hvor konfidensialitet er nødvendig, eller ved mistanke om slik utlevering, skal Datatilsynet varsles.

Resultat fra avviksbehandling skal dokumenteres.

§ 7-7. Organisering

Det skal etableres klare ansvars- og myndighetsforhold for bruk av informasjonssystemet.

Ansvars- og myndighetsforhold skal dokumenteres og ikke endres uten autorisasjon fra daglige leder hos den registeransvarlige eller hos de myndigheter som har tilgang til SIS.

Informasjonssystemet skal konfigureres slik at tilfredsstillende informasjonssikkerhet oppnås.

Konfigurasjonen skal dokumenteres og ikke endres uten autorisasjon fra den registeransvarliges daglige leder.

Bruk av informasjonssystemet som har betydning for informasjonssikkerheten, skal utføres i henhold til fastlagte rutiner.

§ 7-8. Personell

Medarbeidere hos den registeransvarlige og hos de myndigheter som har tilgang til SIS skal kun bruke informasjonssystemet for å utføre pålagte oppgaver, og selv være autorisert for slik bruk, jf. § 1-6.

Medarbeiderne skal ha nødvendig kunnskap for å bruke informasjonssystemet i samsvar med de rutiner som er fastlagt.

All bruk av informasjonssystemet skal registreres.

§ 7-9. Taushetsplikt

Medarbeidere hos den registeransvarlige og hos myndigheter som har tilgang til SIS skal pålegges taushetsplikt for opplysninger i SIS. Taushetsplikten skal også omfatte annen informasjon med betydning for informasjonssikkerheten.

§ 7-10. Fysisk sikring

Det skal treffes tiltak mot uautorisert adgang til utstyr benyttet for behandling av opplysninger etter denne forskriften.

Sikkerhetstiltakene skal også hindre uautorisert adgang til annet utstyr med betydning for informasjonssikkerheten.

Utstyr skal installeres slik at ikke påvirkning fra driftsmiljøet får betydning for behandlingen av opplysninger.

§ 7-11. Sikring av konfidensialitet

Det skal treffes tiltak mot uautorisert innsyn i opplysninger i SIS

Sikkerhetstiltakene skal også hindre uautorisert innsyn i annen informasjon med betydning for informasjonssikkerheten.

Lagringsmedium som inneholder opplysninger fra SIS, skal merkes slik at behovet for konfidensialitet fremgår.

Dersom lagringsmediet ikke lenger benyttes for behandling av slike opplysninger, skal opplysningene slettes fra lagringsmediet.

§ 7-12. Sikring av tilgjengelighet

Det skal treffes tiltak for å sikre tilgang til opplysninger hvor tilgjengelighet er nødvendig.

Sikkerhetstiltakene skal også sikre tilgang til annen informasjon med betydning for informasjonssikkerheten.

Alternativ behandling skal forberedes for de tilfeller informasjonssystemet er utilgjengelig for normal bruk.

Det skal opprettes kopier av opplysninger og annen informasjon som er nødvendig for gjenoppretting av normal bruk.

§ 7-13. Sikring av integritet

Det skal treffes tiltak mot uautorisert endring av opplysninger i SIS der integritet er nødvendig.

Sikkerhetstiltakene skal også hindre uautorisert endring av annen informasjon med betydning for informasjonssikkerheten.

Det skal treffes tiltak mot ødeleggende programvare.

§ 7-14. Sikkerhetstiltak

Sikkerhetstiltak skal hindre uautorisert bruk av informasjonssystemet, og gjøre det mulig å oppdage forsøk på slik bruk.

Forsøk på uautorisert bruk av informasjonssystemet skal registreres.

Sikkerhetstiltak skal omfatte tiltak som ikke kan påvirkes eller omgås av medarbeiderne, og ikke være begrenset til handlinger som den enkelte forutsettes å utføre.

Sikkerhetstiltak skal dokumenteres.

§ 7-15. Sikkerhet hos andre virksomheter

Den registeransvarlige eller de myndigheter som har tilgang til SIS skal bare overføre opplysninger elektronisk til kommunikasjonsparter som tilfredsstiller kravene i dette kapitlet.

Leverandører som gjennomfører sikkerhetstiltak eller annen bruk av informasjonssystemet, på vegne av den registeransvarlige, skal tilfredsstille kravene i dette kapitlet.

Den registeransvarlige skal etablere klare ansvars- og myndighetsforhold overfor kommunikasjonsparter og leverandører. Ansvars- og myndighetsforhold skal beskrives i særskilt avtale eller instruks.

Den registeransvarlige skal ha kunnskap om sikkerhetsstrategien hos slike virksomheter, og jevnlig forsikre seg om at strategien gir tilfredsstillende informasjonssikkerhet som resultat.

§ 7-16. Dokumentasjon

Rutiner for bruk av informasjonssystemet og annen informasjon med betydning for informasjonssikkerheten, skal dokumenteres.

Dokumentasjon skal lagres i minimum 5 år fra det tidspunkt dokumentet ble erstattet med ny gjeldende utgave.

Registrering av autorisert bruk av informasjonssystemet og av forsøk på uautorisert bruk, skal lagres minimum 3 måneder. Registreringer av alle hendelser med betydning for informasjonssikkerheten skal lagres i minimum 3 måneder.

Forskrift om tinglysning (JD)

§ 25. Datasikkerhet

Den som har ansvaret for driften av en tinglysningsdatabase, skal påse at databasen blir håndtert og oppbevart på en sikkerhetsmessig forsvarlig måte - herunder at det jevnlig tas sikkerhetskopier av databasen.

Departementet kan utarbeide nærmere instruks for tilgang til registrene og sikkerhetsrutinene ved tinglysningsmyndigheten og Løsøreregisteret.

Det skal ikke tas andre kopier av tinglysningsdatabasene enn det som følger av denne paragraf og § 20, § 21 og § 24.

Den som har ansvaret for driften av en tinglysningsdatabase, må påse at behandlingen av registeropplysningene inngår i institusjonens beredskaps- eller kriseplan.

Forskrift om offentleg arkin (KKD)

§ 4-9. Vern mot skadeverk, innbrot og ulovleg tilgjenge

Bygningsdelar som avgrensar arkivlokalet, skal vere utforma slik at arkivmaterialet er fullgodt sikra mot innbrot og mot at uvedkomande elles kan sleppe inn.

Spesialrom for arkiv skal vere sikra med særskild innbrotsalarm. Kontorrom der ein har arkiv, skal gå inn i det ordinære tryggingssopplegget for bygningen.

Offentlege organ skal ha reglar for kven som har tilgjenge til arkivlokale.

Forskrift om kart og stedfestet informasjon i plan- og byggesaksbehandlingen (MD)

§ 11. Datasikkerhet

Den som har ansvaret for driften av offentlig kartgrunnlag og planarkiv, skal påse at disse blir håndtert og oppbevart på en sikkerhetsmessig forsvarlig måte, herunder at det jevnlig tas sikkerhetskopier av databaser.

Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften) (MOD)

Hele forskriften

Forskrift om behandling av personopplysninger (personopplysningsforskriften) (MOD)

Kap 2 og 8

Forskrift om registrering av foretak (NHD)

§ 10. Datasikkerhet

Det tas regelmessig sikkerhetskopi av det som er registrert i Foretaksregisterets database. Databehandlingen må dessuten tilrettelegges på en slik måte at kvaliteten av lagrede og avgitte opplysninger er tilstrekkelig god og slik at den blir mest mulig robust mot uønskede

hendelser. Uhell, misbruk, feil og øvrige trusler mot datasikkerheten skal søkes avdekket og avverget så effektivt som mulig.

Forskrift om føringen av grunneiendoms-, adresse- og bygningsregisteret (GAB-registeret) (MD)

§ 10. Informasjonssikkerhet, taushetsplikt, mv.

Enhver som i stillings medfør eller i medhold av disse bestemmelsene har anledning til å gjøre seg kjent med opplysninger i GAB om noens personlige forhold, er pliktig til å bevare taushet om det vedkommende får kjennskap til. Opplysninger underlagt taushetsplikt må oppbevares på en forsvarlig måte slik at ingen uvedkommende får adgang til dem.

Den som har ansvaret for driften av en GAB-database skal påse at databasen blir håndtert og oppbevart på en sikkerhetsmessig forsvarlig måte, herunder at det jevnlig tas sikkerhetskopier av databasen. Statens kartverk fastsetter nærmere instruks for tilgang til registrene og sikkerhetsrutiner, herunder for lagring og makulering av opplysninger fra GAB.

Statens kartverk, kommuner som fører opplysninger i GAB, databehandler og distributør skal utøve forebyggende sikkerhetstjeneste for GAB i henhold til lov om forebyggende sikkerhetstjeneste. Personopplysningslovens bestemmelser om informasjonssikkerhet og internkontroll gjelder tilsvarende.

Forskrift om elektronisk signatur (NHD)

Flere viktige bestemmelser

Forskrift om beredskap i kraftforsyningen (OED)

Kapittel 6. Informasjonssikkerhet

§ 6-1. Generelt

Alle enheter i KBO skal foreta en løpende helhetlig vurdering av informasjonssikkerheten. Nødvendige tiltak og rutiner skal etableres og vedlikeholdes.

Informasjonssikkerheten i kraftforsyningen skal omfatte konfidensialitet, integritet og tilgjengelighet av informasjon og ressurs. Dette skal gjelde følgende områder:

- a) Sensitiv informasjon om kraftforsyningen som kan brukes til å hindre eller skade kraftforsyningens funksjoner,
- b) alle systemer og enheter som ivaretar viktige driftskontrollfunksjoner - herunder både informasjonsbehandling og kommunikasjon - for henholdsvis: driftssikkerhet, overvåking, styring, vedlikehold og feilretting av kraftsystem, anlegg og vassdragsregulering for kraftproduksjon,
- c) administrative og merkantile systemer som behandler sensitiv informasjon, eller har betydning for driften av kraftforsyningen.

Alle enheter i KBO skal utpeke en egen datakyndig IT-sikkerhetsleder. Denne skal bistå enhetens leder med informasjonssikkerheten. IT-anlegg skal plasseres slik at mulighetene for skade blir minst mulig.

§ 6-2. *Beskyttelse av informasjon*

Sensitiv informasjon om kraftforsyningen skal ikke offentliggjøres.

På følgende områder skal sensitiv informasjon til enhver tid avskjermes effektivt for uvedkommende:

- a) Driftskontrollsystemer (oversikter over system, sikkerhetstiltak, sårbarhet og liknende),
- b) detaljerte oversikter (kraftsystem, kart, tabeller og liknende) over sentral- og regionalnett hvor status over transformatorytelser eller kraftlinjer med spenningsnivå og/eller overføringskapasitet er angitt,
- c) oversikter over fordelingsnett som leverer kraft til viktige forsvarsanlegg og andre beredskaps- og samfunnsviktige virksomheter,
- d) sikrings- og sikkerhetstiltak,
- e) beredskapsrom/kommandoplasser,
- f) detaljerte analyser av sårbarhet som følge av påført skade,
- g) oversikter over reservemateriellagre og reparasjonsmuligheter.

Herunder skal det vurderes hvilken informasjon som er viktig eller sensitiv for drift og sikkerhet. Det skal identifiseres hvor sensitiv informasjon befinner seg og hvem som er rettmessige brukere av denne informasjonen.

For denne informasjonen skal det etableres en effektiv tilgangskontroll slik at kun rettmessige brukere har tilgang til informasjon og ressurser. Kommunikasjon skal beskyttes mot avlytting og manipulering av uvedkommende. Det skal utarbeides og implementeres sikkerhetsinstruks og gjennomføres tiltak og rutiner for å ivareta ovennevnte.

Norges vassdrags- og energidirektorat kan treffe vedtak om at informasjon om kraftforsyningen skal sikkerhetsgraderes og behandles i henhold til bestemmelsene i sikkerhetsloven.

§ 6-3. *Sikkerhetskopier*

Det skal til enhver tid foreligge oppdaterte sikkerhetskopier av informasjon og programvare som er av betydning for kraftforsyningens drift og sikkerhet. Herunder skal all nødvendig informasjon og programvare sikres med fjernlagring av sikkerhetskopier.

Nødvendig dokumentasjon om kraftsystem og anlegg som lagres på datamedia skal også foreligge som utskrifter. Disse skal oppdateres årlig og oppbevares på et sikkert sted.

§ 6-4. *Særlige krav til driftskontrollsystemer*

Driftskontrollsystemer omfatter driftssentraler, sambandsanlegg og øvrige anlegg og komponenter som ivaretar driftskontrollfunksjoner.

a) *Planer og dokumentasjon*

Alle enheter i KBO skal til en hver tid ha oppdatert dokumentasjon over de eksisterende og planlagte driftskontrollsystemer.

b) *Tilgangskontroll*

Alle driftskontrollsystemer skal ha kontrollordninger som effektivt beskytter mot intern og ekstern uautorisert fysisk og elektronisk tilgang og spredning av ondsinnet programvare og liknende.

c) *System sikkerhet*

Driftskontrollsystem i klasse 2 skal utføres med redundans frem til det enkelte kraftforsyningsanlegg i klasse 2 og 3 slik at ikke viktige funksjoner tapes på grunn av feil eller enkelt hendelse.

Driftskontrollsystem i klasse 3 skal utføres med full redundans i hele systemet frem til det enkelte kraftforsyningsanlegg i klasse 2 og 3, og til andre relevante driftskontrollsystemer i klasse 2 og 3, slik at en feil eller enkelt hendelse ikke kan sette viktige funksjoner ut av drift. Redundansen skal utføres med fysisk og elektronisk separering.

Driftskontrollsystemet skal utføres så robust at funksjon også opprettholdes under store og langvarige påkjenninger. Driftskontrollsystemer i klasse 3 skal kunne fungere uavhengig av offentlige nett og teletjenester.

Driftskontrollsystemer i klasse 2 og 3 og annet samband av betydning for kraftforsynings drift og sikkerhet skal minimum ha to fysisk adskilte og uavhengige sambandsveier til kraftforsyningsanlegg i klasse 2 og 3.

d) *EMP- og EMI-beskyttelse*

Driftssentraler, annen kontrollutrustning og sambandsinstallasjoner i klasse 2 og 3 skal beskyttes mot elektromagnetisk puls (EMP) og elektromagnetisk interferens (EMI).

e) *Brann sikkerhet*

Automatisk brannalarm skal installeres i alle rom i den delen av bygget hvor driftssentralen med tilbehør er installert. Denne skal også varsle eventuell hjemmevakt.

f) *Beredskapsrom*

Alle driftssentraler i kontrollsystem klasse 3 skal ha beredskapsrom for ledelse og driftspersonell.

Norges vassdrags- og energidirektorat kan vedta om driftssentraler i kontrollsystem klasse 1 og 2 skal ha beredskapsrom.

Beredskapsrom skal tjene som nøddriftssentral og understøtte andre ledelsesfunksjoner i ekstraordinære situasjoner, samt gi personell beskyttelse.

§ 6-5. Mobile radionett - driftsradio

Alle enheter i KBO som er avhengig av pålitelig mobilkommunikasjon for drift, sikkerhet eller gjenoppretting av funksjon skal ha tilgang til et mobilt sambandssystem.

Dette sambandssystemet skal:

- a) Ha tilstrekkelig dekningsgrad for kraftforsyningens anlegg og drift,
- b) fungere uavhengig av funksjonssvikt i offentlige nett,
- c) ha tilstrekkelig nødstrøm ved omfattende eller langvarige strømbrudd,
- d) ha nødvendig funksjonalitet med blant annet direkte apparat til apparat kommunikasjon, gruppesending og felles oppkall, og
- e) kunne fungere som reservesamband om annet samband svikter.

§ 6-6. Relésamband - vern av kraftsystem

Kommunikasjonsbaserte vernsystemer i sentral- og regionalnett skal ha pålitelige og sikre samband som fungerer upåvirket av feiltilstander i kraftsystemet, og sørger for overføring av nødvendige signaler og meldinger mot relevante driftssentraler.

Vernsystemer skal sørge for rask og selektiv frakopling av enhet med funksjonsfeil for å begrense konsekvensen av feil i kraftforsyningssystemet.

Forskrift om Petroleumstilsynet (OED)

§ 5-1. Datasikkerhet

Registerfører skal påse at opplysninger i Petroleumsregisteret blir samlet inn, registrert, oppbevart og benyttet på en forsvarlig måte. Det skal tas sikkerhetskopier av Petroleumsregisteret.

Lov om elektronisk kommunikasjon (ekomloven)

Flere viktige bestemmelser

Forskrift om elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste (ekomforskriften) (SD)

Kapittel 8. Sikkerhet og beredskap

§ 8-1. *Plikt til å gi og ha opplysninger*

Tilbyder som:

1. leverer nødvendig elektronisk kommunikasjonstjeneste til bruker med samfunnskritisk funksjon eller
2. leverer overføringskapasitet og samtrafikk til tilbyder som omfattes av nr. 1 skal ha oversikt over egne brukere som innehar samfunnskritisk funksjon og elektronisk kommunikasjonstjeneste som er nødvendig for brukerens utførelse av slik funksjon. Med egne brukere med samfunnskritisk funksjon menes offentlig eller privat bruker som myndighetene har pålagt oppgave for videreføring av samfunnets funksjonsevne i krise- eller beredskapssituasjon, og som har kundeforhold hos tilbyder. Med krise- og beredskapssituasjon menes situasjon hvor myndighetene anser det nødvendig å innføre spesielle tiltak for å videreføre viktige samfunnsfunksjoner.

Bruker med samfunnskritisk funksjon skal informere tilbyder etter første ledd om hvilke elektronisk kommunikasjonstjenester som er nødvendige for å utføre disse funksjonene.

§ 8-2. *Beredskapsplaner og øvelser*

Tilbyder etter § 8-1 første ledd skal utarbeide og vedlikeholde planer og gjennomføre tiltak for å opprettholde elektronisk kommunikasjonstjeneste som er nødvendig for

1. utførelse av egne beredskapsoppgaver
2. utførelse av de beredskapsoppgaver som egne brukere med samfunnskritiske funksjoner er pålagt i en krise- og beredskapssituasjon.

Tilbyder skal på forespørsel fra Post- og teletilsynet utlevere planer etter første ledd. Post- og teletilsynet fører tilsyn med planene og kan sette krav til innhold.

Tilbyder skal på forespørsel delta i beredskapsøvelser arrangert av myndigheten.

§ 8-3. *Nasjonal autonomi*

Tilbyder etter § 8-1 første ledd skal i krise- og beredskapssituasjon kunne opprettholde nødvendig tjenestetilbud for brukere med samfunnskritisk funksjon uten driftsstøtte og elektroniske kommunikasjonstjenester lokalisert i andre land.

Post- og teletilsynet kan i krise- og beredskapssituasjon pålegge tilbyder å utføre drift og vedlikehold av tjenestetilbudet med personell og tekniske løsninger som er lokalisert på norsk territorium.

§ 8-4. *Prioritering av tjenestetilbud*

Tilbyder etter § 8-1 første ledd skal i krise- og beredskapssituasjon gi prioritet til bruker med samfunnskritisk funksjon. Tilbyder etter § 8-1 første ledd nr. 2 skal i krise- og beredskapssituasjon gi prioritet til tilbyder etter § 8-1, første ledd nr. 1.

§ 8-5. Varsel

Tilbyder etter § 8-1 skal varsle Post- og teletilsynet om vesentlige driftsmessige og tekniske problemer som kan redusere, eller har redusert, kvaliteten på tjeneste omfattet av forskriften.

Instruks for behandling av dokumenter som trenger beskyttelse av andre grunner enn nevnt i sikkerhetsloven med forskrifter (beskyttelsesinstruksen) (SMK)

§ 10. Forsendelse

Dokumenter merket STRENGT FORTROLIG skal fortrinnsvis sendes med bud/kurér, men kan også sendes som rekommandert post. Sendes et dokument merket STRENGT FORTROLIG i posten, skal det skje i dobbelt konvolutt. Den indre konvolutt skal forsegles og påføres beskyttelsesgrad. Den ytre konvolutt skal være umerket. Forsendelse av dokumenter merket FORTROLIG kan skje på vanlig måte i umerket, lukket konvolutt.

Dokumenter merket FORTROLIG og STRENGT FORTROLIG kan sendes elektronisk, forutsatt at det er iverksatt informasjonssikkerhetstiltak jf. § 12. Ved forsendelse av dokumenter merket STRENGT FORTROLIG skal det alltid innhentes kvittering.

Hvis det ikke foreligger særlige grunner, skal forsendelsen adresseres til vedkommende institusjon og ikke til en bestemt person eller stillingshaver. Ønsker avsenderen at forsendelsen bare skal åpnes av bestemte personer, kan dokumentet sendes til en bestemt stillingsinnehaver. Mottakeren plikter i så fall å sørge for at dokumentet uten opphold blir journalisert i samsvar med § 8 foran.

§ 12. Dokumenter gradert etter denne instruksen skal så langt det passer, behandles elektronisk i samsvar med følgende regler i sikkerhetslovens forskrift om informasjonssikkerhet: § 4-36 i kapittel 4 om dokumentetsikkerhet, kapittel 5 om informasjonssystemetsikkerhet, § 6-9 fjerde ledd første punktum jf. § 6-6 i kapittel 6 om fysisk sikring mot ulovlig inntrenging og kapittel 7 om administrativ kryptosikkerhet.

Dokumenter gradert etter instruksen skal i slike tilfeller følge reglene for dokumenter gradert BEGRENSET