JD

JUSTIS- OG BEREDSKAPSDEPARTEMENTET

Høringsnotat

Samfunnssikkerhetsavdelingen
21. desember 2018
Saksnr: 17/4816

HØRING OM UTKAST TIL LOV SOM GJENNOMFØRER NIS-DIREKTIVET I NORSK RETT

1. HØRINGSNOTATETS HOVEDINNHOLD

I dette høringsnotatet legger Justis- og beredskapsdepartementet frem et utkast til en ny lov som skal kunne gjennomføre EUs NIS-direktiv i norsk rett.[1] Høringsnotatet omhandler kun gjennomføring av de delene av direktivet som krever lovendring, i all hovedsak punkt 2 i listen under.

NIS-direktivet har som formål å styrke IKT-sikkerheten i EU. Dette skal oppnås ved at medlemsstatene gjennomfører ulike tiltak for å styrke nasjonale kapasiteter og internasjonalt samarbeid. Medlemsstatene skal:

1. Utarbeide en nasjonal strategi om IKT-sikkerhet og etablere en nasjonal enhet for håndtering av digitale sikkerhetshendelser (CSIRT).
2. Sørge for at tilbydere av samfunnsviktige tjenester og tilbydere av enkelte digitale tjenester, basert på en risikovurdering, gjennomfører hensiktsmessige og

1 Europaparlamentets og Rådets direktiv (EU) 2016/1148 av 6. juli 2016 om tiltak som skal sikre et høyt felles sikkerhetsnivå i nettverks- og informasjonssystemer i EU

forholdsmessige sikkerhetstiltak. Tjenestetilbyderne skal også varsle om alvorlige hendelser. Det skal føres tilsyn med etterlevelsen, og mangelfull etterlevelse kan sanksjoneres. Direktivet stiller strengere krav til tilbydere av samfunnsviktige tjenester enn til tilbydere av digitale tjenester.[2]

3. Peke ut minst en nasjonal myndighet som skal overvåke den nasjonale gjennomføringen av direktivet.
4. Sørge for deltakelse i de to internasjonale samarbeidsgruppene som etableres under direktivet. En samarbeidsgruppe for strategisk styring og forvaltning av direktivet (NIS cooperation group) og et nettverk av nasjonale responsmiljøer (NIS CSIRT network) som skal samarbeide om håndtering av digitale sikkerhetshendelser.

Direktivet er foreløpig ikke tatt inn i EØS-avtalen. Departementet legger imidlertid til grunn at direktivet etter hvert blir innlemmet. Dersom EØS-prosessen drar ut i tid vil departementet dessuten vurdere å foreslå tilsvarende lovbestemmelser uavhengig av EØS-prosessen. Prosessen omtales nærmere i punkt 2.

Utkast til en ny lov som gjennomfører punkt 2 i listen over følger vedlagt. Loven skal forplikte virksomheter som har en særlig viktig rolle i opprettholdelsen av et funksjonelt indre marked til å gjennomføre IKT-sikkerhetstiltak og varsle om alvorlige hendelser.

Virksomhetene faller i to kategorier. For det første *tilbydere av samfunnsviktige tjenester* innenfor samfunnssektorene energi, transport, helse, vannforsyning, bank, finansmarkedsinfrastruktur og digital infrastruktur. For det andre *tilbydere av digitale tjenester*, nærmere bestemt nettbaserte markedsplasser, nettbaserte søkemotorer og skytjenester.[3]

Virksomhetene som omfattes av loven får i hovedsak to forpliktelser. De skal gjennomføre sikkerhetstiltak som står i et rimelig forhold til den risikoen virksomheten står overfor og de skal varsle om alvorlige IKT-sikkerhetshendelser.

Det stilles strengere krav til tilbydere av samfunnsviktige tjenester enn til tilbydere av digitale tjenester. En konkretisering av kravene som stilles til sistnevnte kategori følger av Kommisjonens gjennomføringsforordning (EU) 2018/151 30. januar 2018.[4] Departementets foreløpige vurdering er at forordningen bør vedtas som forskrift til den loven som dette høringsnotatet omhandler. En slik forskrift vil i så fall bli hørt på vanlig måte på et senere tidspunkt.

---

2 For en oversikt over tilbydere av samfunnsviktige og digitale tjenester som omfattes av direktivet, se henholdsvis direktivet vedlegg II og III.

3 De to kategoriene kalles i den vedlagte uoffisielle oversettelsen av diretivet henholdsvis ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester.

4 COMMISSION IMPLEMENTING REGULATION (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact.

Myndighetene skal føre tilsyn med virksomhetene og kan gi pålegg og eventuelt gebyr ved manglende oppfyllelse av pliktene. Myndighetene skal også ta imot varsler om alvorlige IKT-sikkerhetshendelser.

Departementet mener at eksisterende myndighetsstruktur bør benyttes i størst mulig grad. Der det per i dag eksisterer sektormyndigheter, skal deres hjemler justeres slik at de er i samsvar med direktivet når det gjelder tilsyn og sanksjonering. Departementet tar videre utgangspunkt i at eksisterende myndigheter også bør føre tilsyn med virksomheter som per i dag ikke er underlagt tilsyn.

Departementet ber om at høringsinstansene kommer med innspill til forslaget til regelverk for gjennomføring av NIS-direktivet i Norge. Det understrekes at regjeringen ikke har tatt endelig stilling til om direktivet skal gjennomføres. Departementet ønsker gjennom høringsrunden å få belyst hvilke konsekvenser det vil få for norske virksomheter dersom direktivet gjennomføres i Norge.

Den videre gjennomgangen av gjeldende rett vil vise at det i mange tilfeller er vanskelig å lese ut av gjeldende lover om, og i så fall hvordan, de også inkluderer IKT-sikkerhet. Slik uklarhet eller fravær av rettslige krav om IKT-sikkerhet betyr imidlertid ikke nødvendigvis at det er for dårlig IKT-sikkerhet i en virksomhet. Det er derfor særlig interessant for departementet å få belyst hva som vil være forskjellen på IKT-sikkerhetsnivået slik det er i virksomheten per i dag, og hvilket nivå det vil bli dersom loven vedtas.

2. BAKGRUNNEN FOR HØRINGSNOTATET

Den 7. februar 2013 lanserte EU-kommisjonen EUs strategi for cybersikkerhet, *An Open, Safe and Secure Cyberspace*.[5] Som ett av flere tiltak for å nå målene i strategien lanserte Kommisjonen samtidig et forslag til direktiv om tiltak for et høyt felles sikkerhetsnivå i nettverks- og informasjonssystemer i EU (NIS-direktivet).[6] Direktivet ble vedtatt i EU 6. juli 2016, med frist for gjennomføring 10. mai 2018.

Departementet sendte direktivet på alminnelig høring i juni 2016, blant annet for å få innspill til vurderingen av Norges posisjon til direktivet. Departementet mottok rundt 40 høringssvar. Ingen av høringsinstansene uttalte at direktivet ikke er EØS-relevant eller at det ikke er akseptabelt. Rundt 13 av høringsinstansene stilte seg uttrykkelig positive til direktivet, herunder OED, NVE, HOD, Datatilsynet og Statoil. Flere av disse mente at direktivet er EØS-relevant.

---

5 https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/organized-crime-and-human-trafficking/cybercrime/docs/join_2013_1_en.pdf
6 https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-is-new/news/news/2013/docs/1_directive_20130207_en.pdf

Regjeringen besluttet i desember 2016 å anse direktivet som EØS-relevant og akseptabelt. Island har inntatt samme posisjon som Norge. Liechtenstein har foreløpig ikke inntatt en endelig posisjon. Alle EØS/EFTA-statenes posisjoner må være klarlagt før prosessen med en innlemmelse av direktivet i EØS-avtalen kan fortsette. EØS-komiteen har dermed ikke ennå tatt stilling til om – og eventuelt innen hvilken frist – direktivet skal gjennomføres i EØS/EFTA-landene.

Til tross for og delvis på grunn av usikkerheten knyttet til EØS-prosessen mener departementet det er flere grunner til å sende dette utkastet til lov på høring nå.

Det er etter departementets syn klart at direktivet er EØS-relevant og samarbeidet med EU innen IKT-sikkerhet tiltar.[7] Direktivet får direkte innvirkning på berørte virksomheters rammevilkår og det vil ikke være i tråd med EØS-avtalens intensjon om direktivet gjennomføres kun i EU og ikke i hele EØS. Departementet mener det kan legges til grunn at direktivet blir bindende for Norge.

Etter normal prosedyre får EØS/EFTA-landene i saker som denne, der det er behov for lovendringer, et halvt års frist etter beslutningen i EØS-komiteen for å gjøre nødvendige nasjonale avklaringer og få på plass nødvendig regelverk. Generelt bør arbeid med norsk regelverk for gjennomføring av EU-rettsakter settes i gang før EØS-komiteen har fattet en beslutning. Dette gjør seg særlig gjeldende i denne saken fordi NIS-direktivet er såpass omfattende.

Departementet anser direktivet for å være et godt tiltak for å styrke IKT-sikkerheten i Norge. Gjennomføring av direktivet vil for mange samfunnsviktige virksomheter innebære en styrking av arbeidet med IKT-sikkerhet. Dette vil bidra til å redusere digitale sårbarheter i den enkelte virksomhet, den enkelte sektor og samlet sett for nasjonen. En risikobasert tilnærming til sikkerhetsarbeid er et viktig skritt på veien til bedre digital sikkerhet. Krav om varsling av alvorlige digitale sikkerhetshendelser vil blant annet gi tilgang til informasjon om både trusler og sårbarhet – en kunnskap som vil bidra til enda bedre arbeid med IKT-sikkerhet i fremtiden. Nasjonal sikkerhetsmyndighet anbefalte i Sikkerhetsfaglig råd 2015 tiltak 13 at «[i]nnholdet i NIS-direktivet bør implementeres.»

Av hensyn til konkurranse er det en fordel om det er like krav til sikkerhet i hele EØS. Ulike rammevilkår i ulike deler av EØS er uheldig særlig for virksomheter som har aktivitet både i EU og EØS/EFTA-landene. Videre vil norske virksomheter kunne antas å være enklere mål for angripere dersom vi ikke har samme nivå på IKT-sikkerheten her som i EU. Et tettere samarbeid med EU-landene om IKT-sikkerhetsrelaterte spørsmål vil også være positivt for Norge.

---

7 Se blant annet EU kommisjonens forslag om styrking av mandatet til EUs byrå for nettverks- og informasjonssikkerhet (ENISA) og forslag til direktiv om IKT-sikkerhetssertifisering, COM(2017) 477.

3. FREMMED RETT - GJENNOMFØRING AV DIREKTIVET I ANDRE LAND

I Sverige trådte en ny *lag om informationssäkerhet för samhällsviktiga och digitala tjänster* i kraft 1. august 2018. Formålet med loven er å oppnå et høyt nivå på sikkerheten i nettverk og informasjonssystemer for samfunnsviktige tjenester innnenfor samfunnssektorene som omfattes av NIS-direktivet. Virksomheter som omfattes av den svenske sikkerhetsloven omfattes ikke av «NIS-loven».[8]

Loven pålegger virksomhetene som omfattes å drive systematisk og risikobasert sikkerhetsstyring, og å varsle om alvorlige hendelser. I all hovedsak gjelder loven de delene av NIS-direktivet som retter seg mot tilbydere av samfunnsviktige og digitale tjenester.

I Danmark blir NIS-direktivet implementert gjennom reguleringer i den enkelte sektor. En ny *lov om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter m.v.* trådte i kraft 10. mai 2018. Dette lovforslaget implementerer de deler av direktivet som stiller sikkerhetskrav til samtrafikkpunkter (internett exchange points). Loven gir Center for Cybersikkerhed myndighet til å fastsette minimumsregler om minimumskrav til sikkerheten i nettverk og informasjonssystemer for operatører av vesentlige internetutvekslingspunkter.

I Storbritannia trådte *The Network and Information Systems Regulations 2018* i kraft 10. mai 2018.[9] Regelverket gjelder alle direktivets krav, både de som retter seg mot tilbydere av samfunnsviktige og digitale tjenester, og krav som retter seg mot myndighetene.

4. NY LOV OM SIKKERHET I NETTVERK OG INFORMASJONSSYSTEMER

4.1 Innledning

NIS-direktivet – som andre direktiver – forplikter kun medlemsstatene. Det er dermed medlemsstatenes oppgave å sørge for at direktivets bestemmelser blir etterlevet. Det følger av EØS-avtalen art. 7 bokstav b at det overlates til nasjonale myndigheter å bestemme formen og midlene for gjennomføringen av EU-direktiver.

Der det er påkrevet av hensyn til legalitetsprinsippet eller informasjonsformål foreslår departementet lovregler. Dette gjelder først og fremst i tilfeller hvor det pålegges plikter mht. gjennomføring av sikkerhetstiltak, varsling av hendelser, tilsyn og sanksjoner. Se nærmere vedlagte utkast til lov om sikkerhet i nettverk og informasjonssystemer.

Gjennomføring av direktivets øvrige krav, det vil si plikt til å ha en nasjonal strategi for IKT-sikkerhet, et nasjonalt responsmiljø for IKT-hendelser, utpeking av en nasjonal kompetent myndighet og deltakelse i NIS samarbeidsgruppe og NIS CSIRT-nettverk,

---

8 Säkerhetsskyddslagen (1996:627) fra ikrafttredelsen, jf. 8 §, og Säkerhetsskyddslagen (2018:585) fra 1. april 2019, jf. Lag om ändring i lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

9 https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018

krever ikke lovregulering og vil følges opp av departementet parallelt med lovprosessen. Gjeldende nasjonale strategi og NSM NorCERT vil bli vurdert opp mot direktivets krav. Utpeking av en eller flere nasjonale kompetente myndigheter vil skje i dialog med aktuelle myndigheter og gjennom aktuelle tildelingsbrev.

Direktivet gir medlemsstatene rom for nasjonal tilpasning på flere områder. Direktivet setter *minimumskrav* til medlemsstatene når det gjelder både virkeområde og sikkerhetskrav. Det er for eksempel opp til den enkelte medlemsstat å inkludere flere samfunnssektorer og å stille strengere sikkerhetskrav enn det som følger av direktivet. Det er imidlertid ikke rom for å inkludere færre samfunnssektorer eller å stille mindre strenge krav.

Når det gjelder tilbydere av digitale tjenester er handlingsrommet mindre. Ifølge direktivet er denne type virksomhet grenseoverskridende av natur og tilbyderne må følgelig ha et så likt regelverk som mulig å forholde seg til i hele EU. En konkretisering av kravene som stilles til tilbydere av digitale tjenester følger i medhold av direktivet art. 16(8) av Kommisjonens gjennomføringsforordning (EU) 2018/151 30. januar 2018.[10] Departementets foreløpige vurdering er at forordningen bør vedtas som forskrift til den loven som dette høringsnotatet omhandler. En slik forskrift vil i så fall bli hørt på vanlig måte på et senere tidspunkt.

Som det fremgår av lovutkastet, foreslår departementet at lovens virkeområde, sikkerhetskrav og varslingskrav tilsvarer NIS-direktivet. Det vil si en minimumsgjennomføring av direktivet.

4.2 Nærmere om direktivet og lovutkastet

Departementet mener at direktivet bør gjennomføres i en egen ny lov om nettverk- og informasjonssystemsikkerhet. En sektorovergripende lov er best egnet til å gi felles regler om sikkerhets- og varslingskrav, både av styringshensyn og for å oppnå mest mulig lik etterlevelse. Et felles regelverk er videre best egnet til å stille IKT-sikkerhetskrav til virksomheter som per i dag ikke er underlagt noen form for sikkerhetskrav.

Det finnes i norsk rett i dag ingen tverrsektorielle eller sektorspesifikke lover som fullt ut tilsvarer NIS-direktivet. Den loven som er nærmest til å dekke direktivets krav er sikkerhetsloven. Det er imidlertid vesentlige forskjeller mellom de to regelverkene. For det første angir sikkerhetsloven og direktivet ulike formål med sikringen. Hva som er formålet er et viktig element for å kunne angi virkeområdet. For det andre handler sikkerhetsloven i første rekke om å beskytte seg mot tilsiktede handlinger. Direktivet

[10] COMMISSION IMPLEMENTING REGULATION (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact.

har ikke en slik begrensning. I tillegg er det ulikheter når det gjelder hvilket sikkerhetsnivå som kreves, varsling av hendelser, tilsynsregime og prosess for angivelse av virkeområde.

Gjennomgangen av gjeldende rett viser at det kun for noen sektorer per i dag finnes regler som tilsvarer NIS-direktivets krav. En rekke virksomheter er underlagt sikkerhetskrav av ulik art, men det er i mange tilfeller uklart om det kan tolkes slik at det stilles krav om IKT-sikkerhet. Et felles IKT-sikkerhetsregelverk vil kunne fjerne slik tvil. Om det ikke følger IKT-sikkerhetskrav av sektorregelverket, så vil det følge av en ny IKT-sikkerhetslov. Dette er hovedbegrunnelsen for lovutkastet § 5.

Kravene som stilles til virksomhetene skal bidra til å nå to hovedmål – styrket forebyggende sikkerhet og styrket beredskap til å håndtere hendelser. Krav om en risikobasert tilnærming til arbeidet med IKT-sikkerhet i samfunnsviktige virksomheter skal styrke sikkerheten både i den enkelte virksomhet og i samfunnet. Dette skal sikre tjenestens tilgjengelighet.

Formålet med varsling av alvorlige hendelser kan deles opp i flere delmål. Varslene skal bidra til generell bedring av hendelseshåndteringen. Kravet om varsling vil kunne ha en oppdragende effekt gjennom at virksomhetene utarbeider planer for varsling. I tillegg vil varslene gjøre tilsynsmyndigheter eller hendelsehåndteringsmiljøer i stand til å bistå i virksomhetens hendelseshåndtering. Varslene skal videre samlet danne et viktig grunnlag for videre utvikling av arbeidet med IKT-sikkerhet, både i Norge og i Europa. Varslene skal bidra til sentrale myndigheters oversikt over den nasjonale sikkerhetstilstanden. Systematisk varsling skal også bidra til å kunne se viktige sammenhenger mellom hendelser i ulike sektorer, nasjonalt og internasjonalt.

Lovutkastet gjennomgås i detalj i de følgende kapitlene.

5. LOVENS FORMÅL OG VIRKEOMRÅDE

5.1 Gjeldende rett

Det finnes i norsk rett i dag ingen lover som fullt ut tilsvarer NIS-direktivet. Blant de lovene som finnes, har *lov om nasjonal sikkerhet* flest fellestrekk med NIS-direktivet.[11] Formålet med sikkerhetsloven er å ivareta nasjonale sikkerhetsinteresser gjennom å sikre grunnleggende nasjonale funksjoner.

Noe forenklet gjelder sikkerhetsloven for virksomheter som har avgjørende betydning for *grunnleggende nasjonale funksjoner*. Dette er «tjenester, produksjon og andre former for virksomhet som er av en slik betydning at et helt eller delvis bortfall av funksjonen vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser.» Departementene skal innenfor sine ansvarsområder fatte vedtak om at loven helt eller

[11] Se nærmere Prop. 153 L (2016-2017) Lov om nasjonal sikkerhet (sikkerhetsloven).

delvis skal gjelde for virksomheter som enten behandler sikkerhetsgradert informasjon, råder over informasjon, informasjonssystemer, objekter eller infrastruktur som har avgjørende betydning for grunnleggende nasjonale funksjoner, eller driver aktivitet som har avgjørende betydning for grunnleggende nasjonale funksjoner.

I tillegg gjelder sikkerhetsloven for statlige, fylkeskommunale og kommunale organer og leverandører av varer eller tjenester i forbindelse med sikkerhetsgraderte anskaffelser.

Lov 25. juni 2010 nr. 45 om kommunal beredskapsplikt, sivile beskyttelsestiltak og Sivilforsvaret (sivilbeskyttelsesloven) har også som formål å beskytte kritisk infrastruktur. Loven er likevel ikke relevant i denne sammenheng da virkeområdet og plikter som følger av loven er av en annen art enn lovutkastet.

Personopplysningsregelverket gjelder i praksis for de aller fleste, om ikke alle, virksomheter. Formålet er å beskytte personopplysninger, og behandlingsansvarlige og databehandlere er derfor pålagt plikter om blant annet sikring av personopplysningene. For å ivareta informasjonens konfidensialitet, integritet og tilgjengelighet må informasjonssystemene som behandler personopplysningene sikres. Hvorvidt dette er de samme informasjonssystemene som skal sikres etter det nye lovutkastet, og dermed om personopplysningsregelverket er relevant i denne sammenheng, blir drøftet nærmere i kapittel 7. Der gjennomgås også forvaltningsloven og eforvaltningsforskriften.

Det finnes en rekke sektorspesifikke regelverk som på ulik måte og i ulikt omfang stiller krav om sikkerhet til virksomheter som omfattes av NIS-direktivet. Relevant sektorregelverk gjennomgås nærmere i de påfølgende kapitlene om lovutkastets forskjellige deler.

5.2 Direktivet

Direktivets krav retter seg mot virksomheter som leverer tjenester som er viktige for et velfungerende samfunn og næringsliv. Virksomhetene er delt i to hovedkategorier, tilbydere av samfunnsviktige tjenester (operator of essential service, se art. 4(4)) og tilbydere av digitale tjenester (digital service provider, se art. 4(6)). Alle tjenestene er listet opp i direktivets vedlegg II og vedlegg III.

Direktivet legger opp til at gjennomføringen av direktivet, hva gjelder virkeområdet, skal skje i to omganger, jf. art. 24. Direktivet trådte i kraft 9. mai 2018. Fristen for å identifisere tilbydere av samfunnsviktige tjenester er 9. november 2018. Formålet er at medlemsstatene skal ha en mest mulig lik tilnærming til identifiseringsprosessen.

NIS-direktivet gjelder ikke for virksomheter som er omfattet av EUROPAPARLAMENTS- OG RÅDSDIREKTIV 2002/21/EF av 7. mars 2002 om felles rammeregler for elektroniske kommunikasjonsnett og -tjenester (rammedirektivet), §§ 13 a og 13 b. Direktivet er innlemmet i EØS-avtalen, og bestemmelsene er i praksis gjennomført i norsk rett gjennom ekomregelverket. Direktivet har likevel et noe snevrere virkeområde enn det norske ekomregelverket.

NIS-direktivet gjelder ikke for virksomheter som er omfattet av EUROPAPARLAMENTS- OG RÅDSFORORDNING (EU) nr. 910/2014 av 23. juli 2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked og om oppheving av direktiv 1999/93/EF. Forordningen er gjennomført i norsk rett gjennom lov 15. juni 2018 nr. 44 om elektroniske tillitstjenester.

NIS-direktivet skal ikke legge begrensninger på medlemsstatenes muligheter til å iverksette tiltak for å ivareta essensielle statsfunksjoner, særlig nasjonal sikkerhet og opprettholdelse av lov og orden, herunder adgangen til å etterforske, oppdage og iretteføre kriminelle handlinger, jf. art. 1(6).

Det følger videre av art. 1(7) et lex specialis-unntak for virksomheter som er underlagt sektorspesifikt EU-regelverk. Dersom slikt regelverk stiller krav om sikkerhet og varsling som har effekt som minst tilsvarer direktivets krav, skal sektorregelverket anvendes. Etter fortalepunkt (9) er det kun det aktuelle regelverket og hvordan det er implementert nasjonalt som skal tas i betraktning ved vurderingen av om bestemmelsen kommer til anvendelse.

Dersom regelen kommer til anvendelse er den aktuelle sektoren eller de virksomhetene som er underlagt regelverket unntatt fra direktivet. Det skal da ikke gjenomføres en identifikasjonsprosess for denne sektoren. Anvendelsen av bestemmelsen skal rapporteres til EU-kommisjonen.

I fortalepunkt (10) trekkes vanntransportsektoren frem som en mulig kandidat der art. 1(7) kommer til anvendelse. Det står der at:

> [S]ecurity requirements for companies, ships, port facilities, ports and vessel traffic services under Union legal acts cover all operations, including radio and telecommunication systems, computer systems and networks. Part of the mandatory procedures to be followed includes the reporting of all incidents and should therefore be considered as lex specialis, in so far as those requirements are at least equivalent to the corresponding provisions of this Directive.

I fortalepunkt (12) og (13) trekkes sektorene bank og finansmarkedsinfrastruktur frem som mulige lex specialis-kandidater og medlemslandene oppfordres til å vurdere om regelen kommer til anvendelse. Kommisjonen har selv fulgt opp dette i COM(2017) 476, der tre konkrete regelverk vurderes nærmere; 1) Payment Service Directive 2; 2) Regulation (EU) 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories, og 3) Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU, bør betraktes som lex specialis.

Det konkluderes med at regelverk 1) oppfyller både sikkerhets- og varslingskravene som følger av direktivet, mens regelverk 2) og 3) oppfyller direktivets sikkerhetskrav.

Etter kommisjonens vurdering finnes det ikke regelverk for tilbydere av digitale tjenester som kan betraktes som lex specialis.

5.2.1 Behandling av personopplysninger

Direktivet art. 2(1) bestemmer at personopplysninger som behandles i henhold til direktivet, skal behandles i samsvar med direktiv 95/46/EF.12 Videre følger det av art. 2(2) at personopplysninger som behandles av «Unionens institusjoner og organer i henhold til dette direktiv, skal behandles i samsvar med forordning (EF) nr. 45/2001.»[13]

5.2.2 Tilbydere av samfunnsviktige tjenester

Det følger av art. 5(2) at en virksomhet skal anses som tilbyder av en samfunnsviktig tjeneste dersom tre kumulative kriterier er oppfylt. De tre kriteriene følger av henholdsvis art. 5(2)(a) til (c). Kriteriene kommer til uttrykk i lovutkastet § 4 første ledd nr. 1.

Det første kriteriet, jf. art. 5(2)(a), er at virksomheten må tilby en tjeneste som er viktig for opprettholdelsen av kritiske samfunnsmessige eller økonomiske aktiviteter. I henhold til fortalepunkt (20) er det tilstrekkelig å fastslå at virksomheten leverer en slik tjeneste som er opplistet i direktivet vedlegg II. Det er kun den delen av virksomheten som leverer den aktuelle tjenesten som omfattes. For eksempel vil trafikkstyringen på en stor flyplass omfattes, mens butikkområdet ikke omfattes. Vedlegg II lister opp følgende samfunnssektorer:

- Energi (elektrisitet, olje og gass)
- Transport (luft, jernbane, sjø og vei)
- Helse (helsetjenester)
- Bank
- Finansmarkedsinfrastruktur
- Drikkevannsforsyning og -distribusjon
- Digital infrastruktur
    - IXP – internet exchange point
    - DNS – domain name server service provider
    - TLD – top level domain name registries

Se direktivet vedlegg II for nærmere spesifisering av hvilke tjenester som omfattes.

---

[12] Europaparlaments- og rådsdirektiv 95/46/EF av 24. oktober 1995 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger.
[13] Europaparlaments- og rådsforordning (EF) nr. 45/2001 av 18. desember 2000 om personvern i forbindelse med behandling av personopplysninger i Fellesskapets institusjoner og organer og om fri utveksling av slike opplysninger.

Det andre kriteriet, jf. art. 5(2)(b), er at tjenesteleveransen må være avhengig av nettverk og informasjonssystemer. Begrepet *nettverk og informasjonssystemer* defineres i art. 4(1), og benyttes i lovutkastet § 4 første ledd nr. 3:

a. elektronisk kommunikasjonsnett, jf. lov 4. juli 2003 nr. 83 om elektronisk kommunikasjon (ekomloven) § 1-5 nr. 2
b. en enhet eller en gruppe av sammenkoblede eller beslektede enheter, der en eller flere enheter behandler digitale data automatisk ved hjelp av et program
c. digitale data som lagres, behandles, innhentes eller overføres ved hjelp av elementer som nevnt i bokstav a) eller b) for at dataene skal kunne driftes, vernes, beskyttes eller vedlikeholdes.

Det tredje kriteriet, jf. art. 5(2)(c), er at en hendelse i virksomhetens nettverk og informasjonssystemer ville hatt vesentlig forstyrrende virkning på leveransen av den samfunnsviktige tjenesten. Som det fremgår av punktene under er vurderingstemaet her tjenesteleveranse i en samfunnssammenheng, og ikke virksomhetens tjenesteleveranse isolert sett. Det er altså spørsmål om i hvilken grad det går utover samfunnets tilgang på en viss tjeneste, at den aktuelle virksomheten ikke leverer sitt bidrag til totalen som normalt.

Ved vurderingen av vesentligheten av en sikkerhetshendelses forstyrrende effekt skal både tverrsektorielle og sektorspesifikke momenter tas i betraktning. Art. 6 oppstiller en ikke uttømmende liste med tverrsektorielle momenter som skal vurderes:

- antall brukere som baserer seg på tjenesten
- andre vedlegg II-sektorers avhengighet av tjenesten
- omfanget og varigheten av hendelsers mulige virkning på økonomiske og samfunnsmessige aktiviteter og samfunnssikkerhet
- virksomhetens markedsandel
- geografisk område som kan rammes av hendelsen
- viktigheten av virksomhetens bidrag til leveranse av tjenesten, med tanke på alternative tjenestetilbydere

Begrepet *betydelig forstyrrende effekt* defineres i lovutkastet § 4 første ledd nr. 6.

Det endelige virkeområdet for direktivet skal fastlegges gjennom en identifiseringsprosess i regi av hver enkelt medlemsstat. Det er opp til medlemsstatene hvordan denne prosessen gjennomføres, så lenge direktivets krav om å opprette en liste over alle operatører av essensielle tjenester oppfylles. Det er for eksempel ikke krav om at det fattes enkeltvedtak om identifisering eller utpeking av hver enkelt virksomhet. Listen skal oppdateres jevnlig og minst hvert andre år.

Det er opp til medlemsstatene å definere flere samfunnssektorer og tjenester som samfunnsviktige enn det som følger av direktivet. Se blant annet fortalepunkt (23).

5.2.3 Tilbydere av digitale tjenester

Den andre kategorien virksomheter omfatter tilbydere av nettbaserte markedsplasser, nettbaserte søkemotorer og skytjenester, i det videre betegnet tilbydere av digitale tjenester eller DSP (digital service providers).

Det følger av direktivet art. 4(5) at med digital tjeneste menes tjenester som nevnes i NIS-direktivet vedlegg III. Videre henvises det til definisjonen av tjenester i Europaparlaments- og rådsdirektiv (EU) 2015/1535 av 9. september 2015 om en informasjonsprosedyre for tekniske regler og standarder og informasjonssamfunnstjenester (kodifisering) art. 1(1)(b):

> 'service' means any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. (…)

I vedlegg I til nevnte direktiv er det inntatt en veiledende liste over tjenester som ikke omfattes av definisjonen.

Det materielle innholdet i direktiv (EU) 2015/1535 tilsvarer innholdet i direktiv 98/34/EF[14], endret ved direktiv 98/48/EF[15]. Bestemmelsene er gjennomført i lov 17. desember 2004 nr. 101 om europeisk meldeplikt for tekniske regler m.m. (EØS-høringsloven). I § 4 nr. 5 menes med *informasjonssamfunnstjeneste* «enhver tjeneste som vanligvis ytes mot vederlag og som formidles elektronisk over avstand og etter individuell anmodning fra en tjenestemottaker».[16] Også her henvises det til en liste over tjenester som ikke omfattes av definisjonen.

De tre digitale tjenestene som omfattes av NIS-direktivet defineres i art. 4(17), 4(18) og 4(19).

En nettbasert markedsplass (online marketplace) er en digital tjeneste som gjør det mulig for forbrukere og næringsdrivende å inngå nettbaserte salgs- eller tjenesteavtaler med næringsdrivende, enten på nettstedet til den nettbaserte markedsplassen eller på nettstedet til en næringsdrivende som bruker datatjenester som leveres av den nettbaserte markedsplassen. Applikasjonsbutikker trekkes i fortalepunkt (15) frem som en type butikk som faller inn i denne kategorien.

En nettbasert søkemotor (online search engine) er en digital tjeneste som gjør det mulig for brukere å foreta søk på i prinsippet alle nettsteder på et bestemt språk, på grunnlag av en forespørsel om et hvilket som helst emne i form av et nøkkelord, en setning eller

---

[14] Europaparlaments- og rådsdirektiv 98/34/EF av 22. juni 1998 om en informasjonsprosedyre for standarder og tekniske forskrifter

[15] EUROPAPARLAMENTS- OG RÅDSDIREKTIV 98/48/EF av 20. juli 1998 om endring av direktiv 98/34/EF om en informasjonsprosedyre for standarder og tekniske forskrifter.

[16] I direktivet defineres begrepet *tjeneste* med blant annet begrepet *Information Society service*, mens loven definerer begrepet *informasjonssamfunnstjeneste.* Dette innebærer ikke en realitetsforskjell.

andre inndata, og som viser lenker hvor det er mulig å finne informasjon om det forespurte innholdet.

En skytjeneste (cloud computing service) er en digital tjeneste som gir tilgang til en skalerbar og fleksibel samling av delbare databehandlingsressurser.

I følge art. 16(11) omfattes ikke mikrovirksomheter og små virksomheter, jf. Kommisjonsrekommandasjon 2003/361/EF av 6. mai 2003 om definisjonen av mikroforetak og små og mellomstore bedrifter.[17] Det vil si at virksomheter som har færre enn 50 ansatte og som har en årlig omsetning eller årlig samlet balanse som ikke overstiger 10 millioner euro ikke omfattes av direktivet. Se for øvrig rekommandasjonen for nærmere bestemmelser om hvilke virksomheter som omfattes.

Det skal ikke foretas en identifisering av tilbydere av digitale tjenester, i motsetning til ordningen for tilbydere av samfunnsviktige tjenester.

For denne kategorien skal det være like regler i hele EU, jf. fortalepunkt (49). Det er derfor ikke noe nasjonalt handlingsrom hva gjelder definisjon av de digitale tjenestene eller sikkerhets- og varslingskrav, med unntak av de føringer som er gitt i art. 1(6), jf. art. 16(10). Dette har blant annet sammenheng med at aktiviteten er grenseoverskridende av natur, se nærmere fortalepunkt (57). Av samme grunn har kommisjonen i medhold av art. 16(8) utarbeidet et gjennomføringsregelverk som konkretiserer direktivets krav om sikkerhet og varsling. Se nærmere om forholdet mellom de to kategoriene i fortalepunkt (49) og (57). Bestemmelsene hindrer imidlertid ikke den enkelte tilbyder fra å iverksette strengere sikkerhetstiltak enn det som følger av direktivet. Det følger dessuten av fortalepunkt (54) at offentlige virksomheter står fritt til gjennom kontrakt å kreve at tilbydere av digitale tjenester har et høyere sikkerhetsnivå enn det som følger av direktivet.

Det følger videre av fortalepunkt (58) at direktivet ikke utelukker medlemsstatene fra å stille krav om sikkerhet og varsling til virksomheter som ikke faller inn under direktivets definisjon av tilbydere av digitale tjenester.

5.3 Departementets vurdering

5.3.1 Innledning

I norsk rett har vi verken lov eller forskrift med formål og virkeområde som tilsvarer NIS-direktivet. Vi står imidlertid ikke overfor et lovtomt rom da flere gjeldende tverrsektorielle og sektorspesifikke lover og forskrifter i stiller på ulikt vis setter krav til IKT-sikkerhet og varsling av uønskede hendelser. Samtidig er det klart at en rekke av de aktuelle virksomhetene per i dag ikke er omfattet av krav til IKT-sikkerhet og varsling.

[17] Høring om en mulig revisjon av rekommandasjonen ble startet av EU-kommisjonen 6. februar 2018.

Med et slikt rettskildebilde som bakteppe, mener departementet at det er behov for en lov som tilsvarer direktivets formål og virkeområde. Forslag til formålsbestemmelse er tatt inn i lovutkastet § 1.

Et alternativ kunne vært å endre sektorlovgivning slik at det ble klart at det stilles krav i tråd med NIS-direktivet. Videre måtte det blitt utformet nye lovregler for de virksomhetene som ikke er omfattet av relevant sektorregelverk. Departementet har funnet en slik tilnærming mindre hensiktsmessig, og viser for øvrig til den nærmere drøftingen av dette i kapittel 4.

I tråd med direktivet art. 1(3) foreslår departementet i lovutkastet § 2 femte ledd et uttrykkelig unntak for virksomheter som omfattes av lov om elektroniske tillitstjenester.

Det følger av direktivet art. 1(3) også at virksomheter som er omfattet av kravene i rammedirektivet art. 13a og art. 13b. Departementet ser ikke behov for en bestemmelse om dette i loven da ekomsektoren ikke er nevnt i lovutkastet § 2 første ledd.

EU-kommisjonens kommunikasjon «Making the most of NIS» nyanserer unntaket for «ekom-virksomheter» noe.[18] Det følger av kommunikasjonen punkt 5.2 at dersom virksomheten i tillegg tilbyr digitale tjenester, jf. direktivet vedlegg III eller samfunnsviktige tjenester, jf. direktivet vedlegg II, punkt 7, så må virksomheten når det gjelder disse tjenestene forholde seg til bestemmelsene i direktivet. Departementet legger til grunn EU-kommisjonens forståelse av direktivet.

Departementet har vurdert om lex specialis-regelen i direktivet art. 1(7) kommer til anvendelse. EU-kommisjonens vurderinger i COM(2017) 476 danner utgangspunktet for denne vurderingen. Slik departementet forstår kommunikasjonen er det kun virksomheter som omfattes av Payment Service Directive 2, som faller inn under NIS-direktivet art. 1(7). Departementet ser for øvrig ikke at det er annet regelverk som passer inn under lex-specialis-regelen, men vil gjerne ha innspill fra høringsinstansene angående dette. Regelen kommer til uttrykk i lovutkastet § 2 fjerde ledd.

Avhengig om virksomheten faller i kategorien tilbydere av samfunnsviktige tjenester eller tilbyder av digitale tjenester, er det ulike fremgangsmåter for å avgjøre om virksomheten faktisk omfattes av direktivet. I det følgende omhandles først tilbydere av samfunnsviktige tjenester, og deretter tilbydere av digitale tjenester.

---

[18] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union, COM(2017) 476 final/2

5.3.2 Behandling av personopplysninger

NIS-direktivet art. 2(1) regulerer behandling av personopplysninger, og viser til direktiv 95/46/EF, som ble opphevet ved vedtakelsen av forordning (EU) nr. 2016/679 (generell personvernforordning).

Personopplysninger som behandles i henhold til direktivet skal behandles i samsvar med de til enhver tid gjeldende personopplysningsregler, nå den generelle personvernforordningen. Det innebærer at virksomheter som omfattes av det vedlagte lovutkastet, skal behandle personopplysninger i tråd med personopplysningsloven. Adgangen til å behandle personopplysninger kommer til uttrykk i lovutkastet § 6, som også gjelder for behandling av særlige kategorier av personopplysninger, jf. personvernforordningen art. 9 nr. 2 bokstav g.

5.3.3 Tilbydere av samfunnsviktige tjenester

Lovens virkeområde er angitt i lovutkastet § 2. Hva som menes med henholdsvis tilbydere av samfunnsviktige tjenester og tilbydere av digitale tjenester følger av definisjonsbestemmelsen i lovutkastet § 4 første ledd nr. 1 og 2. Definisjonen peker til NIS-direktivet vedlegg II som inneholder en nærmere angivelse av hvilke tjenester som omfattes.

Departementet foreslår at lovutkastets virkeområde skal tilsvare direktivets. Luftfartstilsynet (LT) har imidlertid i forbindelse med utarbeidelse av dette høringsnotatet og høringen av selve direktivet som ble gjennomført sommeren 2016, foreslått at flere tjenesteleverandører innen luftfarten bør omfattes av lovutkastet. I følge direktivet vedlegg II, som viser til rammeforordningen[19] art. 2(1), er det kun flygekontrolltjeneste som omfattes. Etter LTs syn er det for snevert, og de viser til at flygekontrolltjenesten er helt avhengig av systemleveranser for å være i stand til å yte tjenester. På denne bakgrunn ber departementet om at relevante høringsinstanser vurderer om lovens virkeområde bør utvides til å gjelde for flysikringstjeneste, jf. rammeforordningen art. 2(4), som omfatter både lufttrafikktjeneste og systemleveranser.

Et ytterligere vilkår i definisjonen er at en hendelse vil kunne få betydelig forstyrrende effekt på tjenesteleveransen. Vilkåret tilsvarer direktivet art. 6 og er definert i lovutkastet § 4 nr. 6. Vurderingstemaet er hvilken samfunnseffekt en hendelse i virksomheten kan få. Det er dermed ikke bare spørsmål om en hendelse helt eller delvis kan slå ut den enkelte virksomhetens tjenesteleveranse. Dette er et viktig moment for direktivets og dermed også lovutkastets virkeområde. Det er meningen å omfatte de virksomheter som er så viktig for samfunnet at en hendelse hos virksomheten får negativ effekt for samfunnet.

---

[19] Europaparlaments- og rådsforordning (EF) nr. 549/2004 av 10. mars 2004 om fastsettelse av rammeregler for opprettelse av et felles europeisk luftrom (rammeforordningen).

Departementet ser at det etter en vurdering av de nevnte momentene som oppstilles i lovutkastet, fremdeles kan være uklart om en virksomhet er omfattet av loven. Dels for å gi aktuelle virksomheter bedre veiledning, og dels for å oppfylle direktivets krav om identifisering av tilbydere av samfunnsviktige tjenester, har departementet gitt Nasjonal sikkerhetsmyndighet i oppdrag å utarbeide mer konkrete vilkår for hvilke virksomheter som skal omfattes. Der det er mulig skal det utarbeides terskelverdier innenfor hver enkelt sektor. Berørte sektormyndigheter og andre aktuelle aktører skal involveres i arbeidet. Departementet ser for seg at en slik liste tas inn i en forskrift til den foreslåtte loven, jf. forskriftshjemmelen i lovutkastet § 4 siste ledd. Departementet mener at dette vil gjøre virksomhetenes egne vurderinger av om de faller innunder direktivet enklere.

Dette arbeidet er ikke ferdigstilt ved utsendelse av dette høringsnotatet. Identifiseringsprosessen pågår nå i EU-landene. Departementet vil, i tråd med føringene i direktivet art. 24, arbeide for at den norske identifiseringsprosessen blir mest mulig lik som ellers i EØS.

Inntil videre henviser departementet til tilsvarende arbeid i Sverige og Storbritannia.[20] [21] Blant de to landene er Sverige mest likt Norge, og departementet mener at listen som er utarbeidet av den svenske Myndigheten för samhällsskydd och beredskap (MSB) gir en relativt god pekepinn på hvilke virksomheter som i Norge kan komme til å omfattes. Til illustrasjon følger et utdrag fra den svenske listen:

> Olja:
> 1. Tjänster avseende import, export, produktion, raffinering eller bearbetning av flytande bränslen och drivmedel som hanterar minst 3 miljoner ton/år.
> 2. Lagrings- och depåtjänster med lagringskapacitet på minst 20 000 m3. Depåområden där flera leverantörer har cisterner med gemensam lastnings-/ lossningsutrustning ska betraktas som en tjänst vid beräkning av volym.
> 3. Tjänster för distribution, överföring och tillhandahållande av ledningar för flytande bränslen och drivmedel med kapacitet för 3 miljoner ton/år.
>
> Järnvägstransport
> 1. Infrastrukturförvaltare järnväg enligt definitionen i artikel 3.2 i Europaparlamentets och rådets direktiv 2012/34/EU om inrättande av ett gemensamt europeiskt järnvägsområde. Med betydande störning avses störningar i verksamhet vars huvudspår överstiger 200 spårkilometer som leverantören förvaltar och/eller bedriver trafikledning på.

---

[20] Redovisning av vissa vidtagna åtgärder för att förbereda genomförandet av NIS-direktivet, 12.01.2018, Deluppdrag A, https://www.msb.se/Upload/Nyheter_press/Pressmeddelanden/MSB%20Regeringsuppdrag%20F%c3%b6rbereda%20inf%c3%b6rande%20av%20NIS%20180115%20.pdf

[21] The Network and Information Systems Regulations 2018, Schedule 2, https://www.legislation.gov.uk/uksi/2018/506/made

2. Särskild trafikledning, trafikutövning och/eller spårinnehav avseende tunnelbana enligt lagen om säkerhet vid tunnelbana och spårväg (1990:1157).
3. Särskild trafikledning, trafikutövning och/eller spårinnehav avseende spårvägar överskridande 100km banlängd och årligen transporterar mer än 400 000 personkilometer enligt lagen om säkerhet vid tunnelbana och spårväg (1990:1157).

Finansmarknadsinfrastruktur
1. Tjänster avseende sådana handelsplatser som avses i 4 art 24 p direktiv Europaparlamentets och rådets direktiv 2014/65/EU med en sammanlagd omsättning om minst 1 miljard kr/år eller med över 30% av handelsvolymen i marknaden.

Hälso- och sjukvårdssektorn
1. hälso- och sjukvårdsverksamhet som omfattas av hälso- och sjukvårdslagen (2017:30), tandvårdslagen (1985:125) eller detaljhandel med läkemedel enligt lagen (2009:366) om handel med läkemedel, och som:
a) omfattar minst 20 000 patientbesök per år, eller
b) minst 20 000 expedieringar per år, eller
c) har ett upptagningsområde där avståndet till likvärdig tjänst uppgår till minst 200 km.

Det følger av den nye sikkerhetsloven § 1-3 at det skal fattes vedtak om hvilke virksomheter som (utover sikkerhetsloven § 1-2) faller innunder lovens virkeområde. Departementet foreslår ikke en tilsvarende prosess for virksomheter som faller innunder virkeområdet til den loven som omhandles i dette høringsnotatet. Det knytter seg en del kostnader til en slik utpekingsprosess, som etter departementets syn ikke veies opp av nyttevirkninger i dette tilfellet. Det legges altså opp til en mer tradisjonell fremgangsmåte ved at den enkelte virksomhet selv må vurdere om den omfattes av lovutkastet, se nærmere lovutkastet §§ 2 og 4.

5.3.4 Tilbydere av digitale tjenester

Når det gjelder tilbydere av digitale tjenester legger direktivet opp til en noe mer tradisjonell angivelse av virkeområde. «Tilbyder av digitale tjenester» og «digitale tjenester» er definert i direktivet, men utover dette gis det ikke nærmere føringer for hva som skal anses for å være tilbydere av digitale tjenester. På dette området er det i enda større grad hensikten å få ensartede regler i hele EU, både hva gjelder virkeområde og sikkerhets- og varslingsplikter. De aktuelle virksomhetene må dermed vurdere om de er omfattet utifra lovutkastets bestemmelser. *Tilbydere av digitale tjenester* defineres i lovutkastet § 4 første ledd nr. 7 til nr. 9.

Tilbyderen av en digital markedsplass legger til rette for at kjøper og selger ved hjelp av markedsplassen kommer i kontakt med flere selgere og kjøpere på samme sted. Markedsplassen kan således sammenlignes med et kjøpesenter. Dette innebærer blant

annet at nettbaserte markedsplasser ikke omfatter nettbutikker der den næringsdrivendes egne varer tilbys.

For nærmere informasjon om tilbydere av digitale tjenester, viser departementet til EU-kommisjonens kommunikasjon «Making the most of NIS» og den svenske Myndigheten för samhällsskydd och beredskap (MSB) utredning av visse forhold knyttet til NIS-direktivet.[22] [23]

I tråd med direktivet art. 16(11) foreslår departementet i lovutkastet § 2 andre ledd tredje punktum at loven ikke skal gjelde for tilbydere av digitale tjenester som er mikrovirksomheter og små virksomheter, slik dette er definert i Kommisjonsrekommandasjon 2003/361/EF av 6. mai 2003. Det vil si at virksomheter som har færre enn 50 ansatte og som har en årlig omsetning eller årlig samlet balanse som ikke overstiger 10 millioner euro ikke omfattes av direktivet.

Departementet tar sikte på å definere mikrovirksomheter og små virksomheter nærmere i forskrift.

Se nærmere om virkeområdet i kapittel 12.

6. LOVENS GEOGRAFISKE VIRKEOMRÅDE

6.1 Gjeldende rett

Som nevnt under punkt 5.1 er det i norsk lovgivning i dag ikke ett samlet regelverk som innholdsmessig tilsvarer den foreslåtte loven om nettverk- og informasjonssystemsikkerhet. Eksisterende tverrsektorielt og sektorspesifikt regelverk om IKT-sikkerhet er for øvrig heller ikke samlet sett dekkende for den foreslåtte lovens innhold.

Gjeldende sikkerhetslov gjelder for Svalbard og Jan Mayen i den utstrekning Kongen bestemmer, jf. sikkerhetsloven § 2 åttende ledd. I ny sikkerhetslov § 1-2 fjerde ledd er forskriftskompetansen utvidet til også å gjelde bilandene. For øvrig er det ikke egne bestemmelser om lovens geografiske virkeområde.

Det geografiske virkeområdet til den nye personopplysningsloven følger av § 4, hvor det heter i første ledd at «[l]oven og personvernforordningen gjelder for behandling av

---

[22] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union, COM(2017) 476 final/2

[23] Redovisning av vissa vidtagna åtgärder för att förbereda genomförandet av NIS-direktivet, 12.01.2018, Deluppdrag B, https://www.msb.se/Upload/Nyheter_press/Pressmeddelanden/MSB%20Regeringsuppdrag%20F%c3%b6rbereda%20inf%c3%b6rande%20av%20NIS%20180115%20.pdf

personopplysninger som utføres i forbindelse med aktivitetene ved virksomheten til en behandlingsansvarlig eller en databehandler i Norge, uavhengig av om behandlingen finner sted i EØS eller ikke.». Som etter sikkerhetsloven kan Kongen i forskrift gi nærmere bestemmelser om lovens anvendelse på Svalbard og Jan Mayen. Det vises for øvrig til Prop. 56 LS (2017-2018) punkt 5.5.

Når det gjelder sektorregelverk, ser departementet ikke behov for en utførlig gjennomgang av det geografiske virkeområdet til alt sektorregelverket. Dette er ikke nødvendig for å kunne ta stilling til hvilket geografiske virkeområde den foreslåtte loven skal ha. For de fleste regelverk er det tilstrekkelig å fastslå at de gjelder på norsk territorium. Det varierer om regelverket gjelder for Svalbard, Jan Mayen og i bilandene.

Et særlig tilfelle i denne sammenheng er imidlertid petroleumsloven. Det følger av § 1-4 første ledd første punktum at loven kommer til anvendelse på petroleumsvirksomhet knyttet til undersjøiske petroleumsforekomster underlagt norsk jurisdiksjon. Med dette menes i første rekke petroleumsforekomster i undergrunnen på norsk kontinentalsokkel. *Petroleumsvirksomheten* som er knyttet til petroleumsforekomsten er ikke geografisk avgrenset.

6.2 Direktivet

6.2.1 Tilbydere av samfunnsviktige tjenester

Direktivet gjelder EUs medlemsstater og for virksomheter som er etablert på medlemsstatenes territorium. For øvrig er det ikke særlige bestemmelser om geografisk virkeområde.

6.2.2 Tilbydere av digitale tjenester

For tilbydere av digitale tjenester gir direktivet bestemmelser om det geografiske virkeområdet. Det følger av direktivet art. 18 (1) og (2) at en tilbyder av digitale tjenester anses å være underlagt jurisdiksjonen i den medlemsstat hvor den har sitt hovedforetak. Videre anses virksomheten å ha sitt hovedforetak der den har sitt hovedkontor. Tilbydere som ikke er etablert i Unionen, men som tilbyr digitale tjenester i Unionen, skal utpeke en representant i Unionen. Representanten skal være etablert i en av medlemsstatene hvor tjenestene tilbys. Tilbyderen av digitale tjenester skal anses som underlagt jurisdiksjonen til medlemsstaten hvor representanten er etablert.

6.3 Departementets vurdering

Som utgangspunkt vil direktivets geografiske virkeområde tilsvare EØS-avtalens virkeområde. Det vil si at direktivet vil gjelde på norsk territorium, jf. EØS-avtalen art. 126. Ut i fra en tradisjonell folkerettslig tilnærming betyr dette at EØS-avtalen gjelder det geografiske området hvor det utøves suverenitet, det vil si på landjorden,

territorialfarvannet og luftrommet. Kontinentalsokkelen, den økonomiske sonen og den tilstøtende sonen omfattes ikke.

Svalbard, Jan Mayen og bilandene er underlagt norsk suverenitet, men står likevel i en særstilling. Departementet foreslår at det bør fastsettes i forskrift om og eventuelt i hvilken utstrekning lovutkastet også skal gjelde for Svalbard og Jan Mayen, og i bilandene. Se lovutkastet § 3.

Departementet foreslår at direktivet art. 18(1) og (2) om jurisdiksjon gjennomføres i lovtukastet § 2 andre og tredje ledd. Det er avgjørende for jurisdiksjon hvor en virksomhet har sitt hovedkontor. Dersom for eksempel en bedrift har sitt hovedkontor i Irland er det gjennomføringen av direktivet i Irland som er bestemmende for om virksomheten har oppfylt sine plikter. I praksis skal det være likt, se blant annet tidligere nevnte gjennomføringsforordning som gjelder for tilbydere av digitale tjenester. Tanken er imidlertid at hver virksomhet ikke skal trenge å forholde seg til mer enn ett lands regelverk på dette området.

For tilbydere av digitale tjenester som ikke er etablert i EØS, men som tilbyr tjenester i EØS, følger det av direktivet art. 18(2) at tilbyderen må oppnevne en representant i EU. Representanten må være etablert i ett av EU-landene der tjenesten tilbys. Regelen er tatt inn i lovutkastet § 2 tredje ledd.

7. HVA SKAL SIKRES OG HVORDAN SKAL DET SIKRES

Dette kapittelet om sikkerhetskrav har gjennomgående to hovedelementer. For det første en angivelse av hvilke nettverk og informasjonssystemer som skal sikres. For det andre hvilke krav som stilles til sikringen av de aktuelle nettverkene og informasjonssystemene.

7.1 Gjeldende rett

7.1.1 Tverrsektorielt

Gjeldende *sikkerhetslov* stiller krav om sikring av informasjonssystemer som behandler sikkerhetsgradert informasjon. Det er informasjon som potensielt kan skade Norges eller alliertes sikkerhet, forholdet til fremmede makter eller andre vitale nasjonale sikkerhetsinteresser dersom informasjonen blir kjent for uvedkommende, jf. sikkerhetsloven § 11. Det er her først og fremst tale om å beskytte informasjonens konfidensialitet.

Den nye sikkerhetsloven stiller krav om sikring av informasjonssystemer som behandler skjermingsverdig informasjon eller som i seg selv har avgjørende betydning for grunnleggende nasjonale funksjoner, kalt *skjermingsverdige informasjonssystemer*, jf. § 6-1. Den nye sikkerhetsloven omfatter dermed flere systemer enn gjeldende sikkerhetslov. I Prop. 153 L (2016-2017) legges det til grunn at skjermingsverdige informasjonssystemer kan utpekes som skjermingsverdig objekt eller infrastruktur.

Et informasjonssystem anses å ha avgjørende betydning for grunnleggende nasjonale funksjoner dersom bortfall eller svekkelse av systemets funksjonalitet vil svekke den grunnleggende nasjonale funksjonen det inngår i eller understøtter. Med *grunnleggende nasjonale funksjoner* menes tjenester, produksjon og andre former for virksomhet som er av en slik betydning at et helt eller delvis bortfall av funksjonen vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser.

Begge lovene, med tilhørende forskrifter, stiller relativt tydelige og omfattende krav til styringen av sikkerheten i virksomheten, herunder informasjonssystemsikkerheten. Departementet legger til grunn at sikkerhetskravene mer enn oppfyller direktivets krav, og henviser derfor til Prop. 153 L (2016-2017) Lov om nasjonal sikkerhet for en nærmere beskrivelse av kravene.

Etter *personopplysningsloven* § 1 gjelder personvernforordningen som norsk lov. Personopplysningsloven inneholder ikke nasjonale bestemmelser om sikkerhet ved behandlingen av personopplysninger. Personvernforordningen art. 5(1) (f) og art. 32 er de viktigste sikkerhetsbestemmelsene. De må imidlertid ses i sammenheng med andre bestemmelser, slik som for eksempel art. 24. Se for øvrig fortalepunkt 39 og 83.

Begrepet *informasjonssystem* brukes ikke i bestemmelsen. Likevel fremgår det klart av sammenhengen at når det brukes informasjonssystemer til å behandle personopplysninger, så må disse sikres.

Det gjøres i lovens forarbeider punkt 16.4.2 nærmere rede for forordningens regler om sikkerhet, se Prop. 56 LS (2017-2018) Lov om behandling av personopplysninger (personopplysningsloven):

> «Forordningens regler om informasjonssikkerhet følger av artikkel 32. Bestemmelsen fastslår at både den behandlingsansvarlige og databehandleren plikter å «gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen», jf. artikkel 32 nr. 1. Eksempler på slike tiltak fremgår av bokstav a til d. En angivelse av sentrale elementer i risikovurderingen følger av artikkel 32 nr. 2. Overholdelse av godkjente atferdsnormer etter artikkel 40 eller en godkjent sertifiseringsmekanisme etter artikkel 42 kan brukes som en faktor for å påvise at kravene til informasjonssikkerhet er oppfylt, jf. artikkel 32 nr. 3. Etter artikkel 32 nr. 4 skal den behandlingsansvarlige og databehandleren sikre at enhver som handler på vegne av den behandlingsansvarlige eller databehandleren bare behandler opplysninger etter instruks fra den behandlingsansvarlige, med mindre unionsretten eller medlemsstatenes rett pålegger en plikt til behandling.»

I forbindelse med høringen av den nye personopplysningsloven uttalte departementet om sikkerhetsbestemmelsene at:[24]

[24] https://www.regjeringen.no/contentassets/c907cd2776264a6486b8dd3ee00a4e3d/horingsnotat–ny-personopplysningslov–gjennomforing-av-personvernforordningen-i-norsk-rett.pdf, punkt 13.5.3.

> Etter departementets vurdering vil imidlertid anvendelse av reglene i artikkel 32 trolig lang på vei gi samme resultat som gjeldende regler slik de er formulert i personopplysningsloven § 13 og personopplysningsforskriften kapittel 2.

Datatilsynet har utarbeidet en veileder om Internkontroll og informasjonssikkerhet, som blant annet tar for seg risikovurderinger knyttet til informasjonssystemer.[25]

Lov 10. februar 1967 nr. 10 om behandlingsmåten i forvaltningssaker (*forvaltningsloven*) gjelder den virksomhet som drives av forvaltningsorganer, det vil si et hvert organ for stat eller kommune. Lovens hovedformål er å sikre riktige forvaltningsvedtak.

Etter § 15a tredje ledd kan Kongen gi forskrift om blant annet signering, autentisering, sikring av integritet og konfidensialitet.

Forskrift 25. juni 2004 nr. 988 om elektronisk kommunikasjon med og i forvaltningen (*eForvaltningsforskriften*), som er fastsatt med hjemmel i forvaltningsloven § 15 a, gjelder for elektronisk kommunikasjon med forvaltningen og for elektronisk saksbehandling og kommunikasjon i forvaltningen. Formålet med forskriften er å legge til rette for sikker og effektiv bruk av elektronisk kommunikasjon med og i forvaltningen.

Det følger av forskriften § 1 at:

> 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.

Bestemmelsen får dermed anvendelse på informasjonssystemer som brukes til saksbehandling og kommunikasjon med og i forvaltningen. På samme måte som at det ikke er enkelt å trekke et skarpt skille mellom et forvaltningsorgans saksbehandling og tjenesteproduksjon, er det heller ikke uten videre enkelt å trekke en skarp grense for hvilke informasjonssystemer forskriften gjelder for.

Sikkerhetskravene følger av eForvaltningsforskriften kapittel 3, Styring og kontroll med informasjonssikkerheten. § 15 *Internkontroll på informasjonssikkerhetsområdet* stiller krav om nettopp internkontroll. Etter første og andre ledd skal det etableres mål og strategi for informasjonssikkerheten og et tilfredsstillende system for internkontroll. Det stilles ikke eksplisitte krav om for eksempel tekniske og organisatoriske tiltak.

[25] https://www.datatilsynet.no/regelverk-og-verktoy/veiledere/internkontroll-og-informasjonssikkerhet/?id=11147, 17. august 2018.

7.1.2 Sektor – energi – elektrisitet

For elektrisitetssektoren gjelder lov 29. juni 1990 nr. 50 om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m. (energiloven). § 9-3 omhandler beredskapstiltak med plikt til å sørge for effektiv sikring og beredskap og iverksette tiltak for å forebygge, håndtere og begrense virkningene av ekstraordinære situasjoner.

Loven hjemler forskrift 12. juli 2012 nr. 1157 om forebyggende sikkerhet og beredskap i energiforsyningen (beredskapsforskriften). Forskriften skal «sikre at energiforsyningen opprettholdes og at normal forsyning gjenopprettes på en effektiv og sikker måte i og etter ekstraordinære situasjoner for å redusere de samfunnsmessige konsekvensene», jf. § 1-1. Ifølge § 1-2 gjelder den forebygging, håndtering og begrensning av virkningene av ekstraordinære situasjoner som kan skade eller hindre produksjon, omforming, overføring og fordeling av elektrisk energi eller fjernvarme. I høringsdokument 2017/6 Forslag til endringer i beredskapsforskriften, Krav til IKT-sikkerhet m.m. foreslår NVE at forskriften også skal gjelde for omsetning av elektrisk energi eller fjernvarme.

Det følger av forskriften § 1-3 at den gjelder for virksomheter som etter § 3-3 eller vedtak er enheter i Kraftforsyningens beredskapsorganisasjon (KBO). NVE foreslår i høringsdokumentet at forskriften skal gjelde for «de virksomheter som helt eller delvis eier eller driver anlegg eller system som er eller kan bli av vesentlig betydning for produksjon, omforming, overføring, omsetning eller fordeling av elektrisk energi eller fjernvarme.» I det følgende legger departementet virkeområdet slik det fremgår av høringsdokumentet til grunn.

Det følger av loven § 9-2 og forskriften §§ 3-3 og 5-1 at virksomhetene plikter å sikre systemene og å ha beredskap for å håndtere ekstraordinære hendelser og sikre videre drift. Forskriften kapittel 6 omhandler krav til sikring av informasjon og informasjonssystemer. I forslaget til endring av beredskapsforskriften § 6-9 stilles det krav til å sikre digitale informasjonssystemer. Beredskapsforskriften kap 7 stiller mer detaljerte krav til beskyttelse av styresystemene i kraftforsyningen.

7.1.3 Sektor – energi – olje

Dette kapittelet er delt opp i to underkapitler, oljeproduksjon og drivstofforsyning.

Oljeproduksjon
Lov 19. juni 2015 nr. 65 om petroleumsvirksomhet (petroleumsloven) kommer i henhold til § 1-4 «til anvendelse på petroleumsvirksomhet knyttet til undersjøiske petroleumsforekomster underlagt norsk jurisdiksjon. Loven gjelder også petroleumsvirksomhet i og utenfor riket og norsk kontinentalsokkel når det følger av folkeretten eller av overenskomst med fremmed stat.» Med petroleumsvirksomhet menes all virksomhet knyttet til undersjøiske petroleumsforekomster, herunder undersøkelse, leteboring, utvinning, transport, utnyttelse og avslutning samt planlegging av slike aktiviteter, likevel ikke transport av petroleum i bulk med skip.

Petroleumsloven hjemler, sammen med en rekke andre lover, særlig fire forskrifter som har betydning for sikkerheten i petroleumssektoren.

Forskrift 12. februar 2010 nr. 158 om helse, miljø og sikkerhet i petroleumsvirksomheten og på enkelte landanlegg (rammeforskriften) gjelder i henhold til § 2 for petroleumsvirksomhet, slik som dette er definert i petroleumsloven, og for annen virksomhet på landanlegg. Formålet med forskriften er blant annet å oppnå systematisk gjennomføring av tiltak for å oppfylle kravene og nå målene som er gitt i helse-, miljø- og sikkerhetslovgivningen, herunder petroleumsloven.

Forskrift 29. april 2010 nr. 634 om utforming og utrustning av innretninger med mer i petroleumsvirksomheten (innretningsforskriften) gjelder i henhold til § 1 for petroleumsvirksomhet til havs, med de unntak som følger av rammeforskriften § 4.

Forskrift 29. april 2010 nr. 613 om utføring av aktiviteter i petroleumsvirksomheten (aktivitetsforskriften) gjelder i henhold til § 1 for petroleumsvirksomhet til havs, med de unntak som følger av rammeforskriften § 4.

Forskrift 29. april 2010 nr. 611 om styring og opplysningsplikt i petroleumsvirksomheten og på enkelte landanlegg (styringsforskriften) har samme virkeområde som petroleumsloven og gjelder i henhold til § 1 for petroleumsvirksomhet, og for annen virksomhet på landanlegg. Med de unntak som følger av rammeforskriften § 4.

Norsk Olje og gass har utarbeidet retningslinjer om krav til sikkerhet for IKT-baserte prosesskontroll-, sikkerhets- og støttesystemer.[26] Formålet med retningslinjene er å styrke den generelle informasjonssikkerheten i offshore industrien og derigjennom forbedre sikkerheten ved og regulariteten til operasjoner på norsk kontinentalsokkel.

Petroleumsloven § 10-1 setter krav til forsvarlig petroleumsvirksomhet. Blant annet skal petroleumsvirksomheten ivareta hensynet til sikkerhet for de økonomiske verdier som innretninger og fartøyer representerer. I dette ligger også et krav om sikring av driftstilgjengelighet.

Det følger av særmerknaden til bestemmelsen at sikkerhetsbegrepet skal tolkes vidt:

> Begrepet omfatter tiltak til forebyggelse av skader på personell, miljø og økonomiske verdier, herunder tiltak for opprettholdelse av produksjons- og transportregularitet (driftstilgjengelighet). Tiltakene må innrettes slik at tilløp til skader kan motvirkes, tåles eller avbøtes. Tiltakene skal motvirke både mindre skader, større ulykker og katastrofer. Spesielt mht driftstilgjengelighet kan det være aktuelt med langsiktige, forebyggende tiltak som ikke nødvendigvis er rettet mot konkrete skader. Disse hensynene er nå ivaretatt gjennom endringen i lovteksten.

[26] Retningslinje 104, Anbefalte retningslinjer krav til informasjonssikkerhetsnivå i IKT-baserte prosesskontroll-, sikkerhets- og støttesystemer, Norsk olje & gass.

Virksomheter innen petroleumssektoren er underlagt et helhetlig sikkerhetsregelverk. Kravene er funksjonelle og angir sjelden et spesifikt nivå for oppfyllelse. Det angis gjennom henvisninger til standarder i de enkelte veiledningene til forskriftsbestemmelsene. Selve systemet for dette følger av rammeforskriften § 24.

Sikkerhetsregelverket er omfattende, og det følgende er et utdrag av de mest relevante reglene.

Etter styringsforskriften § 7 skal den ansvarlige fastsette og videreutvikle mål og strategier for å forbedre helse, miljø og sikkerhet. Operatøren skal sikre at det er samsvar mellom kortsiktige og langsiktige må på ulike områder, på ulike nivå og mellom ulike deltakere i virksomheten. Målene skal uttrykkes slik at det er mulig å ta stilling til graden av måloppnåelse.

Det følger av styringsforskriften § 17 at det skal utføres risikoanalyser som gir et nyansert og mest mulig helhetlig bilde av risikoen forbundet med virksomheten. Risikoanalysene skal blant annet identifiser og analysere risikoreduserende tiltak, jf. rammeforskriften § 11 og styringsforskriften §§ 4 og 5.

Styringsforskriften § 4 bestemmer at ved reduksjon av risiko som nevnt i rammeforskriften § 11, skal den ansvarlige velge tekniske, operasjonelle og organisatoriske løsninger som reduserer sannsynligheten for at det oppstår skade, feil og fare- og ulykkessituasjoner.

Når det gjelder hendelseshåndtering, følger det av styringsforskriften § 17 blant annet at det skal gjennomføres beredskapsanalyser. Det følger videre av aktivitetsforskriften § 76 at det skal utarbeides beredskapsplaner som til enhver tid beskriver beredskapen og inneholder aksjonsplaner for de definerte fare- og ulykkessituasjonene. Planer for beredskap mot akutt forurensning skal dokumentere hvilke beredskapsressurser som inngår, responstider og ytelse og kapasitet i forhold til miljørisiko- og beredskapsanalysenes forutsetninger. Aktuelle bekjempelsesmetoder skal være beskrevet i beredskapsplanen. Aktivitetsforskriften § 77 setter krav til den faktiske håndteringen av fare- og ulykkessituasjoner.

Det er ikke uten videre klart at krav om sikring av nettverk og informasjonssystemer kan tolkes inn i disse generelt utformede kravene om sikkerhet. Dermed er det heller ikke klart hvilke nettverk og informasjonssystemer som eventuelt skal sikres, eller hvordan de skal sikres.

Drivstofforsyning
For de delene av oljevirksomheten som ikke omfattes av petroleumsloven, det vil si raffinering, behandling, lagring og transport av olje, også kalt drivstofforsyningen, finnes det ikke relevant sektorspesifikt regelverk med sikringskrav som tilsvarer lovutkastet.

7.1.4 Sektor – energi – gass

Regelverket som er beskrevet over om oljesektoren gjelder også for produksjon av gass, jf. petroleumsloven.

Lov om 28. juni 2002 nr. 61 om felles regler for det indre marked for naturgass (naturgassloven) og tilhørende naturgassforskrift har ikke relevante bestemmelser om sikkerhet.

7.1.5 Sektor – transport – luft

Lov 11. juni 1993 nr. 101 om luftfart (luftfartsloven) regulerer både sivil og militær luftfart. Blant annet reguleres landingsplasser og flysikringstjenesten. Loven hjemler blant annet forskrift 22. desember 2014 nr. 1902 om felles krav for yting av flysikringstjenester, som i § 2 bestemmer at EØS-avtalen vedlegg XIII kap. VI nr. 66xc (gjennomføringsforordning (EU) nr. 1035/2011 om felles krav til yting av flysikringstjenester, endret ved gjennomføringsforordning (EU) nr. 923/2012 og gjennomføringsforordning (EU) nr. 448/2014), gjelder som forskrift med de tilpasninger som følger av vedlegg XIII, protokoll 1 til avtalen og avtalen for øvrig.

Det finnes i varierende grad regelverk om IKT-sikkerhet i luftfarten. Flysikringstjenesten kan sies å ha kommet lengst. I gjennomføringsforordning nr. 1035/2011 stilles det krav om at tjenesteleverandør skal ha et «Security Management System» (SEMS). SEMS skal, i henhold til retningslinjer blant annet fra EUROCONTROL, ta utgangspunkt i leverandørens risikovurdering og tiltak skal innføres for å sikre data. Sikkerhetsstyringssystemet skal inneholde blant annet vurdering og håndtering av risiko og plan for håndtering av hendelser. Det stilles i denne forbindelse eksplisitt krav til sikring av driftsdata.

Det følger videre av vedlegg I til gjennomføringsforordning (EU) nr. 1035/2011 punkt 1 at ytere av flysikringstjenester «skal kunne yte sine tjenester på en sikker, effektiv, kontinuerlig og bærekraftig måte som er forenlig med enhver rimelig samlet etterspørsel etter et gitt luftrom. For dette formål skal de ha tilstrekkelig teknisk og driftsmessig kapasitet og sakkunnskap.»

Det ligger her indirekte et krav om å sikre relevante informasjonssystemer. Regelverket gir ikke nærmere anvisning på hvordan sikringen skal skje.

Det pågår relevant regelverksarbeid i regi av EASA (European Aviation Safety Agency). Direktoratet ønsker et helhetlig fokus på Cyber security/IKT-sikkerhet i luftfarten, og nytt regelverk vil omfatte både lufthavner, flyselskap og flysikringstjenesten. Et slikt felleseuropeisk regelverk vil følgelig dekke flere aktører enn NIS-direktivet. Blant annet vil ikke de nye reglene være begrenset til «operators of essential services». I tillegg er det et uttalt mål at de nye reglene som et minimum skal tilsvare krav etter NIS-direktivet, slik at alle innen luftfarten som er omfattet av NIS-direktivet, vil innfri kravene ved å rette seg etter reglene gitt av EASA. Regelverket antas å kunne tre i kraft i løpet av 2020.

FNs luftfartsorganisasjon, ICAO, har vedtatt en folkerettslig bindende standard som krever at luftfartsaktører gjennomfører risikovurderinger, identifiserer sine kritiske systemer og innfører tiltak for å sikre disse. Standarden trådte i kraft i november 2018.

7.1.6 Sektor – transport – jernbane

Lov 11. juni 1991 nr. 100 om anlegg og drift av jernbane, herunder sporvei, tunnelbane og forstadsbane m.m. (jernbaneloven) § 6a gir departementet hjemmel til å fastsette forskrift om sikring mot tilsiktede uønskede handlinger, herunder bestemmelser om kriseledelse, om taushetsplikt og om hvilke virksomheter som skal omfattes av forskriften. Hjemmelen inkluderer også IKT-sikkerhet uten at dette er nevnt særskilt, jf. Prop. 107 L (2014-2015) om endringer i jernbaneloven (sikring mot tilsiktede uønskede handlinger), jf. Innst. 311 L (2014-2015).

Samferdselsdepartementet har delegert til Statens jernbanetilsyn å fastsette forskrifter etter loven. Formålet med forskrift 1. juli 2015 nr. 848 om sikring på jernbane (sikringsforskriften) er å pålegge jernbanevirksomheter å arbeide systematisk og proaktivt for å unngå tilsiktede uønskede handlinger og begrense konsekvensene av dem. De virksomheter som er omfattet av forskriften er jernbanevirksomheter på det nasjonale jernbanenettet samt jernbanevirksomheter som driver tunnelbane (omfatter ca. 10 virksomheter), og er rettet mot terror og sabotasje, og trussel om dette samt hærverk og tyveri med særlig stor skadepotensiale, inkludert IKT- sikkerhet.

Sikringsforskriften stiller krav til styringssystemer, herunder ansvar for oppgaver som utføres av leverandører, krav til dokumentasjon, taushetsplikt, prosedyrer, ansvarsforhold, beredskap, kompetansekrav, opplæring mv. Virksomhetene skal utarbeide risikovurderinger og det stilles krav om hvordan disse skal følges opp og oppdateres. Videre stilles det krav om systematisk gjennomføring av revisjoner, oppfølging av uønskede hendelser, beredskapsøvelser og oppfølging av avvik.

Forskrift 11. april 2011 nr. 389 om sikkerhetsstyring for jernbanevirksomheter på det nasjonale jernbanenettet (sikkerhetsstyringsforskriften) er også fastsatt med hjemmel i jerbaneloven. Forskriften gjelder for jernbanevirksomheter på det nasjonale jernbanenettet, og har som formål at de skal arbeide systematisk og proaktivt slik at det etablerte sikkerhetsnivået på jernbanen opprettholdes og i den grad det er nødvendig forbedres, samt at jernbaneulykker, alvorlige jernbanehendelser og jernbanehendelser unngås.

Det følger ikke av forskriften om IKT-sikkerhet skal innfortolkes i kravene.

Innenfor rammene av forskrift 16. juni 2010 nr. 820 om samtrafikkevnen i jernbanesystemet (samtrafikkforskriften) er det krav til visse systemers driftsstabilitet og tilgjengelighet og tilhørende tekniske spesifikasjoner for samtrafikkevne (TSIer).

7.1.7 Sektor – transport – vann

Dette kapittelet er delt opp i to underkapitler, havneanlegg og havner og skipsfart.

Havneanlegg og havner

Lov 19. juni 2015 nr. 65 om havner og farvann (*havne- og farvannsloven*) skal legge til rette for god fremkommelighet, trygg ferdsel og forsvarlig bruk og forvaltning av farvannet i samsvar med allmenne hensyn og hensynet til fiskeriene og andre næringer. Loven skal også legge til rette for effektiv og sikker havnevirksomhet som ledd i sjøtransport og kombinerte transporter samt for effektiv og konkurransedyktig sjøtransport av personer og gods innenfor nasjonale og internasjonale transportnettverk. Med havnevirksomhet menes tjenesteyting, myndighetsutøvelse og annen offentlig forvaltning som retter seg mot fartøy, gods eller passasjerer i havnen. Loven hjemler særlig to relevante forskrifter.

Forskrift 29. mai 2013 nr. 538 om *sikring av havneanlegg* gjelder for havneanlegg som betjener passasjerskip og lasteskip med bruttotonnasje 500 eller mer og enkelte flyttbare boreinnretninger, som er i internasjonal fart. Formålet er å bedre sikkerheten for fartøyer som brukes i internasjonal handel og nasjonal skipsfart, samt tilhørende havneanlegg, mot trusselen fra forsettlige ulovlige handlinger.

Forskrift 29. mai 2013 nr. 539 om *sikring av havner* gjelder for havner der det ligger ett eller flere havneanlegg som er omfattet av en godkjent sikringsplan for havneanlegg i henhold til havneanleggssikringsforskriften. Havnesikringsforskriften skal forebygge og hindre sikringshendelser som kan skade havner, havneanlegg eller skip som anløper disse. Forskriften skal også styrke sikringen i de områder av havnen som ikke er omfattet av havneanleggssikringsforskriften, og underbygge de sikringstiltakene som er iverksatt i medhold av denne.

Det følger av forskrift om sikring av havneanlegg § 10 andre ledd at «[p]å bakgrunn av en sårbarhetsvurdering skal det utarbeides en sikringsplan for hvert anlegg.» I henhold til ISPS-koden del A 15.3 skal sårbarhetsvurderingen inneholde følgende deler:

1. identifisering og vurdering av viktige eiendeler og infrastruktur som det er viktig å beskytte,
2. identifisering av mulige trusler mot eiendelene og infrastrukturen og sannsynligheten for at de skal oppstå, med det formål å fastsette og prioritere sikkerhetstiltakene,
3. identifisering, utvelging og prioritering av mottiltak og endringer av framgangsmåter, og hvor effektive disse er for å redusere sårbarheten, og
4. identifisering av svakheter, herunder menneskelige faktorer, i infrastrukturen, politikken og framgangsmåtene.

I henhold til ISPS-koden del A 16.3 skal sikringsplanen inneholde en rekke konkrete prosedyrer og tiltak for å håndtere risiko og for å varsle om hendelser.

§ 8 bestemmer at det er eier av havneanlegget som er ansvarlig for at oppgaver og forpliktelsene overholdes.

Forskrift om sikring av havner § 9 andre ledd sier at «[p]å bakgrunn av en sårbarhetsvurdering skal det utarbeides en sikringsplan.» Krav til sårbarhetsvurderingen og sikringsplanens følger av henholdsvis vedlegg 1 og 2.

Vedlegg 1 sier at sårbarhetsvurderingen blant annet skal inneholde «identifisering og vurdering av viktige eiendeler og infrastruktur som det er viktig å beskytte» og «identifisering av mulige trusler mot eiendelene og infrastrukturen og sannsynligheten for at de skal oppstå, med det formål å fastsette og prioritere sikringstiltakene». Sårbarhetsvurderingen skal også «fastslå de særlige kjennetegnene for de enkelte delområdene, f.eks. plassering, adgang, strømforsyning, kommunikasjonssystem, eierforhold, brukere og andre elementer som vurderes som relevante for sikringen» og tiltak for forebygging og tiltak for skadebegrensning og skadereduksjon. Det stilles også krav om å beskytte fortrolige opplysninger knyttet til sikring.

Vedlegg 2 sier at sikringsplanen blant annet skal inneholde tekniske og organisatoriske tiltak. Planen skal også inneholde «klare krav til havnens sikringsleder og/eller til havnens sikringsmyndighet om å rapportere alle sikringshendelser.»

Det er ikke uten videre klart om reglene innebærer sikring av informasjonssystemer. Sikring av informasjonssystemer nevnes ikke særskilt, men utelates heller ikke.

Skipsfart

Lov 16. februar 2007 nr. 9 om skipssikkerhet (*skipssikkerhetsloven*) skal trygge liv og helse, miljø og materielle verdier ved å legge til rette for god skipssikkerhet og sikkerhetsstyring, herunder hindre forurensing fra skip, sikre et fullt forsvarlig arbeidsmiljø og trygge arbeidsforhold om bord på skipet, samt et godt og tidsmessig tilsyn.

Det følger av skipssikkerhetsloven § 7 første ledd at «[r]ederiet skal sørge for å etablere, gjennomføre og videreutvikle et dokumenterbart og verifiserbart sikkerhetsstyringssystem i rederiets organisasjon og på det enkelte skip, for å kartlegge og kontrollere risiko samt sikre etterlevelse av krav fastsatt i eller i medhold av lov eller i sikkerhetsstyringssystemet selv. Sikkerhetsstyringssystemets innhold, omfang og dokumentasjon skal være tilpasset behovet til rederiet og den aktiviteten det driver.»

Loven hjemler forskrift 5. september 2014 nr. 1191 om sikkerhetsstyringssystem for norske skip og flyttbare innretninger. Forskriften gjelder for lasteskip og fiskefartøy med bruttotonnasje 500 eller mer, og for flyttbare innretninger, samt roro-passasjerskip og passasjerskip som bruker drivstoff med lavt flammepunkt, passasjerskip i utenriksfart og dessuten passasjerskip i innenriksfart som er sertifisert for mer enn 100 passasjerer.

Forskriften gjennomfører den internasjonale norm for sikkerhetsstyring (ISM-koden) i norsk rett. ISM-koden stiller krav til sikkerhetsstyringssystemet for både det enkelte skip og rederiorganisasjonen. Koden fastsetter blant annet krav til intern- og eksternrevisjoner, håndtering av avvik og sertifisering av skip så vel som rederi. Sikkerhetsstyring skal etter ISM-koden være et system under utvikling, med prosesser for kontinuerlig forbedring. Sikkerhetsstyringssystemet skal bidra til å styre aktivitetene om bord på skipet, i rederiorganisasjonen på land og kommunikasjonen mellom skip og rederi på en systematisk måte. Formålet med regelverket er å sikre at rederier opprettholder et høyt sikkerhetsnivå på alle nivåer i organisasjonen.

Regelverket har i dag ingen eksplisitte krav om digital- eller nettverkssikkerhet. Kravene til sikkerhetsstyring er imidlertid generelt utformet og passer også for vurdering og håndtering av slik risiko. Dette legges til grunn i ISM-koden at alle identifiserte risikoer for skip, personell og miljø, skal vurderes og at det skal innføres egnet vern. Dette kan også omfatte risikovurderinger og tiltak knyttet til digital sikkerhet.

International Maritime Organization (IMO) har vedtatt resolusjon MSC.428(98) som angir at rederiene senest innen første årlige revisjon etter 1. januar 2021 skal innarbeide vurdering og håndtering av risiko knyttet til sikkerhet i nettverk og digitale løsninger som en del av sikkerhetsstyringssystemet. Bakgrunnen for resolusjonen er at disse risikoene faller inn under operasjonelle trusler som allerede dekkes av ISM, og som sikrer at dette blir gjort. Det er med andre ord lagt til grunn i IMO at ISM-regelverket også omfatter informasjonsteknologiske problemstillinger.

7.1.8 Sektor – transport – vei

Det foreligger per i dag ingen lov- eller forskriftsregulering som stiller krav til IKT-sikkerhet på området trafikkstyring. I stedet gjelder interne retningslinjer som definerer rutiner for bruk, drift og utvikling av automasjonsnettet og SCADA-systemet, samt tilhørende nettverk. Vegdirektoratet sørger sammen med regionene i Statens vegvesen for en hensiktsmessig samordning, der krav og rutiner videreutvikles i takt med endringer i omgivelsene og inngår i etatens kvalitetssystem.

7.1.9 Sektor – bank

Lov 10. april 2015 nr. 17 om finansforetak og finanskonsern (*finansforetaksloven*) gjelder for finansforetak, herunder banker og kredittforetak. Formålet med loven er å bidra til finansiell stabilitet, herunder at finansforetak virker på en hensiktsmessig og betryggende måte. Med finansiell stabilitet menes at det finansielle systemet er robust nok til å motta og utbetale innskudd og andre tilbakebetalingspliktige midler fra allmennheten, formidle finansiering, utføre betalinger og omfordele risiko på en tilfredsstillende måte. Loven gjelder ikke for Norges Bank, jf. § 1-6. Norges Bank omfattes ikke av NIS-direktivets virkeområde.

Forskrift 21. mai 2003 nr. 630 om bruk av informasjons- og kommunikasjonsteknologi (IKT-forskriften) gjelder for foretak under tilsyn, herunder banker, kredittforetak og regulerte markeder. Etter § 1 andre ledd omfatter forskriften «IKT-systemer som er av betydning for foretakets virksomhet.»

Det heter i § 2 første ledd at foretaket «skal fastsette overordnede mål, strategier og sikkerhetskrav for IKT-virksomheten», og at det «skal foreligge beskrivelse av den enkelte prosess og hvordan ansvaret for administrasjon, anskaffelse, utvikling, drift, systemvedlikehold, sikring av informasjon og avvikling utføres på en betryggende måte.» Forskriften stiller videre blant annet krav til sikring av informasjon og informasjonssystemer, og hvor det i den sammenheng også henvises til personvernregelverket. Forskriften inneholder krav når det gjelder planlegging og ledelse, utarbeidelse av risikoanalyser og varsling av uønskede hendelser. IKT-forskriften er referanseregelverket for Finanstilsynet i arbeidet med tilsyn av foretakenes bruk av IKT.

For blant annet banker og kredittforetak er det gitt nærmere regler om risikostyring og internkontroll i forskrift 22. august 2014 nr. 1097 om kapitalkrav og nasjonal tilpasning av CRR/CRD IV (CRR/CRD IV-forskriften). Det følger blant annet av § 27 at det skal etableres retningslinjer for operasjonell risiko som skal omfatte beredskapsplaner for å sikre at driften kan videreføres og tap begrenses ved alvorlige driftsforstyrrelser.

Lov 17. desember 1999 nr. 95 om betalingssystemer m.v. har som formål å bidra til at systemer for betalingstjenester innrettes og drives slik at hensynet til sikker og effektiv betaling og til rasjonell og samordnet utførelse av betalingstjenester ivaretas. Loven hjemler forskrift 17. desember 2015 nr. 1731 om systemer for betalingstjenester, som gjelder for blant annet banker og kredittinstitusjoner.

Det reviderte betalingstjenestedirektivet (PSD 2) inkluderer blant annet bestemmelser om både risikoanalyser, sikkerhet og hendelsesrapportering.[27] Det europeiske banktilsynet EBA har utarbeidet retningslinjer både for operasjonell- og sikkerhetsrisiko og for rapportering av hendelser. PSD 2 stiller blant annet krav til rapportering av hendelser til andre berørte medlemsstater.

I tidlig utkast til revidert direktiv var det direkte henvisninger til NIS-direktivets foreslåtte bestemmelser om operasjonell- og sikkerhetsrisiko og hendelsesrapportering. I det fastsatte direktivet er begge områdene imidlertid inntatt som egne bestemmelser. Forslag til innarbeidelse av direktivet i norsk rett har vært på høring, men regelverket er per i dag ikke fastsatt.

[27] Europaparlaments- og rådsdirektiv (EU) 2015/2366 av 25. november 2015 om betalingstjenester i det indre marked om endring av direktiv 2002/65/EF, 2013/36/EU og 2009/110/EF og forordning (EU) nr. 1093/2010, og oppheving av direktiv 2007/64/EF

7.1.10 Sektor – finansmarkedsinfrastruktur

Lov 29. juni 2007 nr. 74 om regulerte markeder (*børsloven*) gjelder for regulerte markeder og skal legge til rette for effektivitet, velordnede og tillitvekkende markeder for finansielle instrumenter. Børsloven har bestemmelser om taushetsplikt (§ 14). I dette ligger det indirekte et krav på regulerte markeder at markedene har et kontrollsystem som sikrer at innsyn i taushetsbelagt informasjon er avgrenset i størst mulig grad (need to know) og at tilganger til slik informasjon blir kontrollert.

IKT-forskriften, omtalt ovenfor, gjelder som nevnt også for regulerte markeder.

Lov 29. juni 2007 nr. 75 om verdipapirhandel (*verdipapirhandelloven*) gjelder for regulerte markeder og skal legge til rette for sikker, ordnet og effektiv handel i finansielle instrumenter. Lov om verdipapirhandel har bestemmelser når det gjelder innsideinformasjon, taushetsplikt og tilbørlig informasjonshåndtering. I dette ligger det indirekte et krav på foretakene at de har et kontrollsystem som sikrer at innsyn i taushetsbelagt informasjon er avgrenset i størst mulig grad (need to know) og at tilganger til slik informasjon blir kontrollert.

Forskrift 22. september 2008 nr. 1080 om risikostyring og internkontroll gjelder for andre foretak under tilsyn enn finansforetak. Blant annet gjelder regelverket for regulerte markeder.

I Finanstilsynets veiledning til Forskrift om risikostyring og internkontroll heter det at:

> "Prinsippene for risikostyring og internkontroll bør kortfattet angi hvordan foretaket skal vektlegge forhold av betydning for å sikre forsvarlig drift, som rollefordelingen mellom styret, administrasjonen og andre kontrollerende funksjoner, organisatoriske forhold, systemmessige forhold, samt hvordan myndighet eventuelt skal delegeres".
> […]
> "Styret må påse at det blir etablert og gjennomført tiltak for å korrigere eller redusere de svakheter som blir funnet, og at hensynet til risikostyring og internkontroll inngår i vurderingen ved beslutninger om vesentlige endringer i virksomheten. Daglig leder må sørge for at styret er tilstrekkelig orientert om hovedtrekkene i foretakets risikostyring og internkontroll. Hvor omfattende denne rapporteringen skal være, hva som skal rapporteres når og hvordan, bør framgå av styrets prinsipper.»

7.1.11 Sektor – helsetjenester

Lov 20. juni 2014 nr. 42 om behandling av helseopplysninger ved ytelse av helsehjelp (*pasientjournalloven*) gjelder all behandling av helseopplysninger som er nødvendig for å yte, administrere eller kvalitetssikre helsehjelp til enkeltpersoner. Lovens formål er at behandling av helseopplysninger skal skje på en måte som gir pasienter og brukere helsehjelp av god kvalitet ved at relevante og nødvendige opplysninger på en rask og

effektiv måte blir tilgjengelige for helsepersonell, samtidig som vernet mot at opplysninger gis til uvedkommende ivaretas, og sikrer pasienters og brukeres personvern, pasientsikkerhet og rett til informasjon og medvirkning.

Det følger av pasientjournalloven § 22 første ledd at den «dataansvarlige og databehandleren skal gjennomføre tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen, jf. personvernforordningen artikkel 32. Den dataansvarlige og databehandleren skal blant annet sørge for tilgangsstyring, logging og etterfølgende kontroll.» Krav om internkontroll følger av § 23.

Loven 20. juni 2014 nr. 43 om helseregistre og behandling av helseopplysninger (*helseregisterloven*) gjelder for behandling av helseopplysninger til statistikk, helseanalyser, forskning, kvalitetsforbedring, planlegging, styring og beredskap i helse- og omsorgsforvaltningen og helse- og omsorgstjenesten. Formålet med loven er å legge til rette for innsamling og annen behandling av helseopplysninger for å fremme helse, forebygge sykdom og skade og gi bedre helse- og omsorgstjenester. Loven skal sikre at behandlingen foretas på en etisk forsvarlig måte, ivaretar den enkeltes personvern og brukes til individets og samfunnets beste.

Det følger av helseregisterloven § 21 at den «dataansvarlige og databehandleren skal gjennomføre tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen, jf. personvernforordningen artikkel 32. Den dataansvarlige og databehandleren skal blant annet sørge for tilgangsstyring, logging og etterfølgende kontroll. I registre som er etablert med hjemmel i §§ 10 eller 11, skal direkte personidentifiserende kjennetegn lagres kryptert.» Krav om internkontroll følger av § 22.

Idet de to lovene viser direkte til personvernforordningen art. 32, vil avgrensningen av hvilke informasjonssystemer som skal sikres, og hvilke krav som stilles til sikkerheten følge av denne bestemmelsen. Det vises til nærmere omtale i kapittel 5.1 og 7.1.1.

Formålet med lov 21. juni 2017 nr. 89 om helsemessig og sosial beredskap (*helseberedskapsloven*) er å «verne befolkningens liv og helse og bidra til at nødvendig helsehjelp, helse- og omsorgstjenester og sosiale tjenester kan tilbys befolkningen under krig og ved kriser og katastrofer i fredstid. For å ivareta lovens formål, skal virksomheter loven omfatter kunne fortsette og om nødvendig legge om og utvide driften under krig og ved kriser og katastrofer i fredstid, på basis av den daglige tjeneste, oppdaterte planverk og regelmessige øvelser, slik det er bestemt i eller i medhold av loven.»

Det er ingen særlige krav om IKT-sikkerhet. Kravene følger derfor av personvernforordningen art. 32.

Det følger av lov 30. mars 1984 nr. 15 om statlig tilsyn med helse- og omsorgstjenesten m.m. (*helsetilsynsloven*) § 1 blant annet at Statens helsetilsyn har det overordnede faglige tilsyn med helse- og omsorgstjenesten i landet.

Loven hjemler forskrift 28. oktober 2016 nr. 1250 om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten. Formålet med forskriften er å bidra til faglig forsvarlige helse- og omsorgstjenester, kvalitetsforbedring og pasient- og brukersikkerhet, og at øvrige krav i helse- og omsorgslovgivningen etterleves. I forskriften presiseres det at den som har det overordnede ansvaret for virksomheten skal sørge for at det etableres og gjennomføres systematisk styring av virksomhetens aktiviteter (styringssystem). Videre presiseres plikten til å dokumentere, planlegge, gjennomføre, evaluere og korrigere.

Her er det heller ingen særlige krav om IKT-sikkerhet. Kravene følger derfor av personvernforordningen art. 32.

Norm for informasjonssikkerhet i helse- og omsorgssektoren (Normen) er en bransjenorm som nær sagt hele helse- og omsorgstjenesten er forpliktet til å rette seg etter, blant annet som følge av avtaler, eksempelvis avtalen som inngås når en virksomhet blir tilknyttet Helsenettet. Normen ble formelt lansert 7. september 2006, og har i dag sitt organisatoriske knutepunkt og sekretariat hos Direktoratet for e-helse. Normen skal bidra til å etablere mekanismer hvor virksomhetene kan ha gjensidig tillit til at behandling av helse- og personopplysninger gjennomføres på et forsvarlig sikkerhetsnivå.

Normen stiller krav som detaljerer og supplerer gjeldende regelverk. Normen setter en rekke konkrete krav for sikring av pasient- og personopplysninger, herunder at det skal gjennomføres en risikovurdering og at det skal fastsettes nivå for akseptabel risiko, tekniske og organisatoriske tiltak og prosedyrer for avvikshåndtering.

Normen er imidlertid ikke heldekkende. Helseregisterloven, personopplysningsloven og øvrig regelverk stiller enkelte krav til behandling av helse- og personopplysninger utover det som er tema for Normen.

Siden det stort sett er personopplysningsloven og helselovgivningens fokus på sikring av helseopplysninger som er grunnlaget for det meste av informasjonssikkerhetsarbeidet i sektoren i dag, kan det være behov for at virksomhetene utvider omfanget av risikostyring og sikkerhetstiltak til også å omfatte annen kritisk infrastruktur. Et eksempel kan være byggteknisk infrastruktur og en del medisinsk-teknisk utstyr.

7.1.12 Sektor – forsyning og distribusjon av drikkevann

Forskrift 22. desember 2016 nr. 1868 om vannforsyning og drikkevann (drikkevannsforskriften), fastsatt med hjemmel i blant annet matloven, er den primære forskriften som regulerer produksjon og forsyning av drikkevann.[28] Formålet med forskriften er å beskytte menneskers helse ved å stille krav om sikker levering av tilstrekkelige mengder helsemessig trygt drikkevann som er klart og uten fremtredende lukt, smak og farge. Forskriften gjennomfører rådsdirektiv 98/83/EF

[28] Lov 19. desember 2003 nr. 124 om matproduksjon og mattrygghet mv. (matloven).

(drikkevannsdirektivet) i norsk rett. Alle vannforsyningssystemer som vil kunne bli omfattet av NIS-direktivet, er omfattet av drikkevannsforskriftens krav. Det følger av § 3 bokstav m at det er vannverkseieren som har ansvaret for at kravene til vannforsyningssystemer etterleves.

Drikkevannsforskriften stiller krav til vannverkene om å kunne levere drikkevann til enhver tid, og at de skal ha forebyggende sikring og beredskap til å håndtere hendelser. Om årsaken er knyttet til svikt i nett- eller informasjonssystem, eller andre forhold, så skal mulige hendelser kartlegges og kunne håndteres.

Sikkerhetstiltakene har tradisjonelt primært vært knyttet til andre årsaker enn svikt i digital kommunikasjon, men også slike årsaker har det vært fokusert på i den senere tid. Mattilsynets veiledning av april 2017 til vannforsyningssystemene om utarbeiding av beredskapsplaner nevner derfor IKT som et område som må tas med i farekartleggingen.

Drikkevannsforskriften stiller i følgende paragrafer krav til vannforsyningssystemene om å:

- identifisere farer som må forebygges, fjernes eller reduseres til et akseptabelt nivå for å sikre levering av tilstrekkelige mengder drikkevann, jf. § 6 første ledd
- sikre at tiltak som forebygger, fjerner eller reduserer farene til et akseptabelt nivå, identifiseres og gjennomføres, jf. 6 andre ledd
- sikre at farekartleggingen og farehåndteringen er oppdatert, jf. 6 fjerde ledd
- etablere internkontroll og sikre at denne følges opp (det stilles krav om organisering og ansvarsplassering, rutiner, registreringer, avvikshåndtering og tiltak for å hindre at avvik gjentar seg samt krav om at internkontrollen holdes oppdatert), jf. § 7
- sikre at vannforsyningssystemet har, eller gjennom avtale har tilgang til, nødvendig kompetanse, jf. § 8 første ledd
- sikre at alle gis opplæring som står i forhold til arbeidsoppgavene, jf. § 8 andre ledd
- sikre at vannforsyningssystemet er utstyrt og dimensjonert samt har driftsplaner og beredskapsplaner for å kunne levere tilstrekkelige mengder drikkevann til enhver tid, jf. § 9 første ledd
- sikre at vannbehandlingsanlegget og alle relevante deler av distribusjonssystemet er tilstrekkelig fysisk sikret, og at alle styringssystemer er tilstrekkelig sikret mot uautorisert tilgang og bruk, jf. § 10
- sikre beredskapsforberedelser, oppdaterte beredskapsplaner og at det er planer for og gjennomføres øvelser jf. § 11
- varsle abonnentene straks ved mistanke om avvik fra kravene som stilles til helsemessig trygt vann som er klart og uten framtredende lukt, smak og farge jf. § 23 første ledd
- varsle Mattilsynet straks ved mistanke om avvik fra kravene som stilles til helsemessig trygt vann som er klart og uten framtredende lukt, smak og farge jf. § 24 første ledd

- på forespørsel gi Mattilsynet de opplysningene Mattilsynet ber om jf. § 24 andre ledd.

7.1.13 Sektor – digital infrastruktur – samtrafikkpunkter på internett (IXP)

Norges samtrafikkpunkter er per i dag ikke gjenstand for ekomrettslig regulering eller krav til sikkerhet. IXP er i art. 4(13) definert som: [29]

> «en nettstruktur som muliggjør sammenkopling av mer enn to uavhengige og selvstendige systemer, først og fremst for å legge til rette for samtrafikk på Internett; et IXP sørger for sammenkopling bare for selvstendige systemer; et IXP krever ikke at internettrafikk som passerer mellom to deltakende selvstendige systemer, passerer gjennom et tredje selvstendig system, og det verken endrer eller griper forstyrrende inn i slik trafikk»

7.1.14 Sektor – digital infrastruktur – tilbyder av DNS-tjeneste

Lov 4. juli 2003 nr. 83 om elektronisk kommunikasjon (ekomloven) gjelder for virksomheter knyttet til elektronisk kommunikasjon og tilhørende utstyr, herunder tilbydere av tilgang til internett. Lovens formål er å sikre brukerne i hele landet gode, rimelige og fremtidsrettede elektroniske kommunikasjonstjenester, gjennom effektiv bruk av samfunnets ressurser ved å legge til rette for bærekraftig konkurranse, samt stimulere til næringsutvikling og innovasjon.

Loven hjemler forskrift 16. februar 2004 nr. 401 om elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste (ekomforskriften). Forskriften gjelder rettigheter og plikter for tilgang for tilbydere og andre brukere til elektronisk kommunikasjonsnett og tilbud av elektronisk kommunikasjonstjeneste.

Regelverk som stiller krav til IKT-sikkerhet for ekomaktørene er i hovedsak ekomloven kapittel 2 og spesielt ekomloven §§ 2-7, 2-9 og 2-10 og ekomforskriften kapittel 8.

Etter ekomloven § 2-7 har en tilbyder plikt til å gjennomføre nødvendige sikkerhetstiltak til vern av kommunikasjon i egne elektroniske kommunikasjonsnett og -tjenester. Trafikkdata skal slettes eller anonymiseres så snart de ikke lenger er nødvendige for kommunikasjons- eller faktureringsformål, med mindre noe annet er bestemt i eller i medhold av lov. Annen behandling av trafikkdata krever samtykke fra brukeren.

Ekomloven § 2-10 sier at tilbyder skal tilby ekomnett og -tjeneste med forsvarlig sikkerhet for brukerne i fred, krise og krig, og opprettholde nødvendig beredskap. Myndigheten kan gjennom vedtak eller forskrift presisere hva som er forsvarlig sikkerhet og nødvendig beredskap.

I ekomforskriften § 8-2 har tilbydere en plikt til å utarbeide og vedlikeholde beredskapsplaner. Det forutsettes at det ligger dokumenterte risiko- og

[29] IXP er nærmere definert i direktivet fortalepunkt 18 og EU-kommisjonens kommunikasjon COM(2017) 476 final/2 Vedlegg I s. 20.

sårbarhetsvurderinger til grunn for disse beredskapsplanene. Det fremkommer også av § 8-2 at tilbyder på forespørsel skal delta på beredskapsøvelser arrangert av myndigheten.

I gjenopprettingsfasen etter utfall plikter tilbydere, etter ekomforskriften § 8-4, å prioritere hensynet til sluttbrukere med ansvar for liv og helse, foran kommersielle hensyn. Myndigheten kan i særlige tilfeller pålegge tilbyder å prioritere andre viktige samfunnsaktører. Dette er situasjoner hvor offentlige interesser tilsier en annen rekkefølge i gjenopprettingen enn det som fremkommer ovenfor. Tilbydere skal uten ubegrunnet opphold varsle Nkom om hendelser som vesentlig kan redusere eller har redusert tilgjengeligheten til ekomtjenester.

Norske registrarer er ikke underlagt ekomloven og heller ikke annet sektorregelverk som stiller krav om IKT-sikkerhet eller varsling av IKT-sikkerhetshendelser.[30]

7.1.15 Sektor – digital infrastruktur – registerenheter for toppdomener

Forskrift 1. august 2003 nr. 990 om domenenavn under norske landkodetoppdomener (domeneforskriften), er fastsatt med hjemmel i ekomloven. Formålet med forskriften er å fastlegge offentligrettslige rammebetingelser for virksomhet som tildeler domenenavn under norske landkodetoppdomener.

De rettslige rammene for sikkerhet og robusthet for norske landkodetoppdomener følger av domeneforskriften §§ 3 og 6 om henholdsvis tildelingsregler og sikkerhetskopi. Registerenheter er ikke tilbydere i ekomlovens forstand, og reglene om sikkerhet i ekomloven og ekomforskriften gjelder derfor ikke for registerenheter. De er heller ikke underlagt annet sektorspesifikt regelverk som stiller krav om IKT-sikkerhet.

7.2 Direktivet

7.2.1 Tilbydere av samfunnsviktige tjenester

Sikkerhetskravene følger av art. 14(1) og (2). Virksomhetene skal sikre de nettverk og informasjonssystemer som de bruker for å levere den samfunnsviktige tjenesten. Virksomheten skal treffe tekniske og organisatoriske tiltak som er hensiktsmessige og står i et rimelig forhold til risikoen som knytter seg til nettverkene og informasjonssystemene. For å sikre opprettholdelse av tjenesteleveransen, skal virksomheten treffe tiltak som er egnet til å forebygge og redusere virkningen av hendelser som truer sikkerheten i virksomhetens IKT-systemer. Ved vurderingen av hvilke tiltak som skal treffes skal det tas hensyn til den tekniske utviklingen.

Litt forenklet sagt oppstiller direktivet et krav om å vurdere sikkerhetsrisikoen som knytter seg til de IKT-systemene som brukes for å levere samfunnsviktige tjenester. Virksomheten skal så treffe tiltak som er egnet til å redusere denne risikoen.

---

[30] En registrar er en forhandler som har en avtale om å tilby domenetjenester, norid.no, 21. august 2018.

Nærmere om hva som ligger i dette er bare til en viss grad omhandlet i fortalen. Det gir ikke særlig veiledning utover det som allerede følger av direktivbestemmelsene. Det fremgår av fortalepunkt (44) blant annet at landene gjennom innføring av passende lovgivningstiltak og frivillige bransjenormer skal fremme en risikostyringskultur som inkluderer risikovurdering og gjennomføring av proporsjonale sikkerhetstiltak. I fortalepunkt (46) står det at risikostyringstiltak omfatter tiltak for å identifisere risikoer for hendelser, med sikte på å forebygge, avdekke og håndtere hendelser og begrense skaden.

NIS-samarbeidsgruppen utarbeider retningslinjer for hva som ligger i sikkerhetskravet.[31]

Etter art. 3 står medlemslandene fritt til å stille strengere sikkerhetskrav enn det som følger av direktivet. Overfor tilbydere av digitale tjenester er det ikke tilsvarende nasjonalt handlingsrom, jf. art. 16(10).

7.2.2 Tilbydere av digitale tjenester

Sikkerhetskravene følger av art. 16. Virksomheten skal sikre nettverk og informasjonssystemer den bruker for å levere tjenesten. Videre skal virksomheten ha en risikobasert tilnærming til sikkerhetsarbeidet. Den skal iverksette sikkerhetstiltak som står i et rimelig forhold til risikoen virksomheten står overfor. Det skal også iverksettes tiltak for å forebygge og minimere virkningen av hendelser i nettverk og informasjonssystemer, med særlig henblikk på opprettholdelse av tjenesteleveransen. Sikkerhetstiltakene skal også ta hensyn til følgende fem elementer:

1. Informasjonssystemsikkerhet og fysisk sikkerhet
2. Hendelseshåndtering
3. Opprettholdelse av tjenesteleveranser
4. Overvåkning, revisjon og testing
5. Etterlevelse av internasjonale standarder

Alle de fem punktene er nærmere spesifisert i EU kommisjonens gjennomføringsforordning fastsatt i medhold av direktivet art. 16(8) (CIR 2018/151).

Det går tydelig frem av fortalen til direktivet at det skal stilles lavere sikkerhetskrav til disse tjenestene da de anses noe mindre viktige enn de samfunnsviktige tjenestene. Det følger dessuten av fortalepunkt (49) at blant annet på grunn digitale tjenesters grensekryssende natur, bør de være underlagt et regelverk som er harmonisert i hele EU. Dette er ivaretatt gjennom gjennomføringsforordningen, som etterlater lite rom for nasjonale tilpasninger.

[31] COM(2017) 476 final/2 Vedlegg I s. 30.

7.3 Departementets vurdering

Gjeldende rett stiller i varierende grad og på ulikt vis krav om sikring av informasjonssystemer. Sikkerhetskravene som stilles faller i to hovedkategorier. Det stilles sikkerhetskrav i tilknytning til en aktivitet, for eksempel jernbanevirksomhet, og det stilles krav om sikring av en viss type informasjon, for eksempel personopplysninger.

Ved vurderingen av forholdet mellom gjeldende rett og kravene som følger av NIS-direktivet, må det også ses hen til hvilke informasjonssystemer som skal sikres.

Som det vil fremgå av de følgende vurderingene mener departementet at det er behov for bestemmelser som stiller krav om IKT-sikkerhet til virksomhetene som omfattes av lovutkastet. Se nærmere lovutkastet §§ 7 og 9.

Den første kategorien sikkerhetskrav følger, i tillegg til sikkerhetsloven, gjerne av sektorspesifikt regelverk, slik som for eksempel petroleumsloven, energiloven og jernbaneloven. Utførelse av de ulike aktivitetene kan ikke gjøres uten fare for personer som utfører arbeidet, som drar nytte av tjenesten eller omgivelsene. I mange tilfeller er dette bakgrunnen for at det er utarbeidet sikkerhetskrav knyttet til aktiviteten.

Det er et uttalt formål med lovutkastet at de samfunnsviktige og digitale tjenestene faktisk blir levert. Det er direkte sammenheng mellom formålsbestemmelsen og sikkerhetskravene, for å gjøre det tydeligere hva som er poenget med sikringen og hvilke nettverk og informasjonssystemer som skal sikres.

Det går tydelig frem av *sikkerhetsloven* hva som er formålet med sikringen, hva som skal sikres og hvordan sikringen skal skje. Sikkerhetskravene som følger av sikkerhetsloven er mer enn dekkende for lovutkastets sikkerhetskrav.

De to regelverkene har imidlertid ulik tilnærming til hvilke informasjonssystemer som skal sikres. Mens sikkerhetsloven stiller krav til sikring av skjermingsverdige informasjonssystemer, stiller direktivet krav til sikring av nettverk og informasjonssystemer som de bruker for å levere den samfunnsviktige tjenesten. Det kan være sammenfall mellom de to tilnærmingene, men det trenger ikke å være det. Virksomhetene som omfattes av begge regelverkene må derfor foreta konkrete vurderinger av hvert enkelt regelverk for å vurdere hvilke informasjonssystemer som skal sikres etter hvilket regelverk.

Beredskapsforskriften, som gjelder for elektrisitetssektoren, stiller tydelige krav til IKT-sikkerhet. Det fremgår også klart frem at formålet med sikringen er å opprettholde energiforsyningen. Legges det til grunn at endringsforslagene etter hvert blir vedtatt, er det departementets vurdering at gjeldende regelverk stiller minst tilsvarende sikkerhetskrav som lovutkastet.

Videre vurderer departementet sikkerhetskravene som gjelder for jernbanesektoren og drikkevannssektoren å være dekkende for lovutkastets krav.

Etter departementets vurdering er det ikke helt klart om gjeldende rett for øvrig stiller tilstrekkelige sikkerhetskrav. Det stilles gjerne ikke eksplisitte krav om sikring av informasjonssystemer. Ofte går det verken av formål eller sikkerhetskrav tydelig frem at selve tjenesteleveransen er et viktig hensyn. Formål og sikkerhetskrav er såpass generelt utformet at det likevel ikke kan utelukkes at loven eller forskriften implisitt stiller krav om IKT-sikkerhet. Ut i fra gjeldende regelverk er det dermed uklart om informasjonssystemene som skal sikres etter den nye loven, allerede er sikret, og om de er sikret godt nok.

Spørsmålet er i hvor stor grad samfunnsutvikling og ny teknologi kan innfortolkes i allerede vedtatt regelverk. Departementet har ikke gått inn i denne relativt omfattende oppgaven, men slår fast at det knytter seg en del usikkerhet til om gjeldende regelverk er dekkende for lovutkastet. I mange tilfeller er det klart at det ikke er dekkende. Problemstillingen berøres også i kapittelet om økonomiske og administrative konsekvenser.

Den andre kategorien sikkerhetskrav handler om sikring av en bestemt type informasjon. Eksempelvis følger det av blant annet personopplysningsloven, pasientjournalloven og helseregisterloven, at personopplysninger skal sikres. De to sistnevnte lovene viser direkte til personvernforordningen, og de tre regelverkene har dermed likelydende sikkerhetskrav.

Ved vurderingen av kravene om informasjonssikring er relevante, må det først vurderes hvilket informasjonssystem som brukes til hva. At en virksomhet er underlagt krav om informasjonssikkerhet, for eksempel i henhold til personopplysningsloven, er ikke nødvendigvis relevant. Det må vurderes i hvilken grad det enkelte informasjonssystem er sikret. Er det snakk om et informasjonssystem som ikke behandler personopplysninger, så er det vel grunn til å anta at systemet heller ikke er sikret i henhold til personopplysningsloven.

I noen tilfeller kan det imidlertid være slik at et informasjonssystem brukes til både å levere en samfunnsviktig eller digital tjeneste, og til å behandle personopplysninger. Dette kan for eksempel være en virksomhets saksbehandlingssystem, eller kontorstøttesystem. Slike informasjonssystemer skal sikres i henhold til både personopplysningsloven og lovutkastet. Da vil det være relevant å vurdere om sikkerhetstiltakene som er iverksatt i henhold til personopplysningslovene tilfredsstiller kravene som følger av lovutkastet.

Sikkerhetskravene etter henholdsvis personopplysningsloven og lovutkastet har mye til felles. Det stilles i begge tilfeller krav om risikovurdering og iverksetting av tekniske og organisatoriske tiltak, som står i et rimelig forhold til den sikkerhetsrisikoen en står overfor. Det nasjonale cybersenteret i Storbritannia (NCSC) har publisert veiledninger til både NIS-direktivet og personvernforordningen. En sammenstilling av veiledningene

viser at innholdet i sikkerhetskravene etter de to ulike regelverkene er tilnærmet like.[32] [33]

Selv om begge kravene gir anvisning på tilvarende metodikk for sikring, er det imidlertid ingen automatikk i at etterlevelse av det ene kravet samtidig er etterlevelse av det andre kravet. Formålene med sikring er ulike. Personopplysningsloven bestemmer at personopplysninger skal sikres. Lovutkastet sier at systemets funksjonalitet skal sikres. Ett eksempel på sikkerhetstiltak, som ikke nødvendigvis er veldig praktisk, men som nevnes for å illustrere ulikhetene, er utstrakt bruk av kryptering. Dette kan være et godt tiltak for å sikre personopplysninger samtidig som det kan være hemmende for funksjonaliteten til systemet.

Virksomheten må foreta en konkret vurdering av sikringsbehovet for hvert enkelt system. Hva som er formålet med sikringen kan ha betydning for hvilke sikkerhetstiltak som bør iverksettes og hvordan disse skal innrettes. I noen tilfeller kan det være fullt samsvar mellom tiltakene som skal iverksettes etter de to regelverkene. I andre tilfeller vil det måtte iverksettes annen sikring på grunn av kravene i lovutkastet enn etter personopplysningsloven.

Generelt gir lovutkastet anvisning på en viss metodikk for sikring av et informasjonssystems funksjonalitet. Personopplysningsloven kan sies å anvende en slik metodikk på et spesifikt felt, nemlig sikring av personopplysninger. Departementet vil likevel anta at dersom man etterlever kravene som følger av personopplysningsloven, vil man, når det gjelder den typen informasjonssystemer vi her omtaler, ha kommet langt på vei til etterlevelse også av sikkerhetskravene som følger av lovutkastet.

Som nevnt tidligere har departementet ved utforming av bestemmelsen om sikkerhetskrav ment å fange opp det samme som direktivets krav. Direktivet konkretiserer i liten grad sikkerhetskravet utover det som følger av bestemmelsen. Generelt mener departementet at «NSMs grunnprinsipper for IKT-sikkerhet» gir god veiledning i grunnleggende IKT-sikkerhet.[34] Denne vil være et godt utgangspunkt for å ha tilstrekkelig god digital sikkerhet i virksomheten. Det er viktig å se IKT-sikkerhet i sammenheng med virksomhetens mer generelle sikkerhetsstyringssystem og virksomhetens overordnede styringssystem.

Når det gjelder bestemmelsens tredje ledd som handler om hendelseshåndtering, viser departementet til *Rammeverk for håndtering IKT-sikkerhetshendelser*, se nærmere punkt 9.1. Selv om virksomheten ikke er i primærmålgruppen for rapporten, så er det likevel gode råd som virksomheten kan dra nytte av.

Utover den generelle føringen i direktivet om at det skal stilles noe mindre strenge krav til tilbydere av digitale tjenester, gis det ikke særlige føringer på hvor store forskjeller det

[32] https://www.ncsc.gov.uk/guidance/gdpr-security-outcomes
[33] https://www.ncsc.gov.uk/content/files/NIS%20Guidance%20Collection%201.0.pdf
[34] https://nsm.stat.no/globalassets/dokumenter/nsm_grunnprinsipper_ikt-sikkerhet_enkeltside_3008.pdf

er snakk om eller hva dette betyr i praksis. Kravene som stilles om sikkerhet til tilbydere av digitale tjenester er, i tråd med direktivet, konkretisert i lovutkastet § 8 andre ledd. Kravene er ytterligere konkretisert i EU-kommisjonens gjennomføringsforordning. De samme kravene vil komme til å gjelde i Norge.

Når det gjelder utformingen av sikkerhetskrav er det store forskjeller mellom gjeldende rett og det som følger av direktivet. Selv om enkelte regelverk til dels kan ha relativt like sikkerhetskrav, mener departementet det likevel er mest hensiktsmessig at det i lovutkastet stilles likelydende krav om IKT-sikkerhet som skal gjelde for alle virksomheter som omfattes av lovutkastet.

Det følger av lovutkastet § 5 *Forholdet til andre lover*, at i den grad tilstrekkelig sikkerhet oppnås gjennom gjeldende regelverk eller praksis, vil direktivet ikke medføre endringer. I motsatt fall vil virksomheten måtte følge direktivets sikkerhetskrav.

8. VARSLINGSKRAV

8.1 Gjeldende rett

8.1.1 Tverrsektorielt

Ifølge *sikkerhetsloven* (2018) § 4-5 skal virksomheten varsle sikkerhetsmyndigheten og sektormyndigheten dersom den har blitt rammet av eller det er begrunnet mistanke om at sikkerhetstruende virksomhet har rammet eller vil kunne ramme virksomheten. Sikkerhetstruende virksomhet er i loven definert som tilsiktede handlinger som direkte eller indirekte kan skade nasjonale sikkerhetsinteresser. Etter andre ledd er det også varslingsplikt selv om ikke egen virksomhet er truet, men «dersom den får kunnskap om en planlagt eller pågående aktivitet som kan medføre en ikke ubetydelig risiko for at nasjonale sikkerhetsinteresser blir truet.»

§ 4-5 første ledd bokstav c bestemmer at det også skal varsles om alvorlige brudd på krav til sikkerhet som følger av loven for øvrig. Hva som er årsaken til sikkerhetsbruddet har ikke betydning, hvilket innebærer at også ikke tilsiktede sikkerhetsbrudd skal varsles.

Det følger av særmerknaden til bestemmelsen at «[e]n forutsetning for at myndighetene skal kunne ha oversikt over sikkerhetstilstanden i de ulike samfunnssektorene, er at myndighetene får rettidig og tilstrekkelig informasjon om hendelser av betydning». Verken loven eller forskriftene konkretiserer ytterligere hva slags informasjon varselet skal inneholde.

I *personopplysningsloven* følger det av personvernforordningen art. 33(1) at brudd på personopplysningssikkerheten skal varsles til tilsynsmyndigheten. Brudd på personopplysningssikkerheten er i art 4 nr. 12 definert som «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».

Art. 33(3) angir hva varselet skal inneholde av opplysninger. Behandlingsansvarlig skal varsle senest 72 timer etter å ha fått kjennskap til bruddet.

eForvaltningsforskriften stiller ikke krav om at virksomheten skal varsle om brudd på sikkerhetskravene i forskriften § 15.

8.1.2 Sektor – energi – elektrisitet

Beredskapsforskriften § 2-6 gir varsling og rapporteringsplikt fra virksomhetene til beredskapsmyndigheten for alle ekstraordinære situasjoner. Varselet skal kortfattet beskrive hendelsen, forventet gjenoppretting og kontaktperson. Det er foreslått å splitte denne bestemmelsen i to, en for varsling når noe ekstraordinært skjer og en for rapportering etter at hendelsen er over, jf. forslag til §§ 2-5 og 2-6.

I forslaget § 6-9 er det lagt opp til at «[v]irksomheten skal varsle uønskede hendelser i sine digitale informasjonssystemer til det sektorvise responsmiljøet.»

8.1.3 Sektor – energi – olje

Oljeproduksjon
Etter styringsforskriften § 29 skal operatøren sikre varsling til Petroleumstilsynet ved fare- og ulykkessituasjoner som har ført til, eller under ubetydelig endrede omstendigheter kunne ha ført til død, alvorlig og akutt skade, akutt livstruende sykdom, alvorlig svekking eller bortfall av sikkerhetsrelaterte funksjoner eller barrierer, slik at innretningens eller landanleggets integritet er i fare eller ved akutt forurensning. Veiledningen til bestemmelsen presiserer at dette også gjelder «situasjoner der normal drift av kontroll- eller sikkerhetssystemer blir forstyrret av arbeid som ikke er planlagt (IKT-hendelse).»

Petroleumstilsynet har utarbeidet et standard skjema for varsling av hendelser, hvor det blant annet skal fylles inn tidspunkt for hendelsen, hvem som var involvert, hendelsesforløp og skadeomfang.

Drivstofforsyning
For de delene av oljevirksomheten som ikke omfattes av petroleumsloven, det vil si raffinering, behandling, lagring og transport av olje, også kalt drivstofforsyningen, finnes det ikke relevant sektorspesifikt regelverk som ivaretar varslingskravet i lovutkastet.

8.1.4 Sektor – energi – gass

Regelverket som er beskrevet i avsnittet over om oljesektoren, gjelder for petroleumsvirksomhet, og dermed også for deler av den norske gassvirksomheten.

Naturgassloven har ikke krav om varsling av hendelser.

8.1.5 Sektor – transport – luft

Det fremgår ikke eksplisitte krav om varsling av sikkerhetshendelser i det gjeldende regelverket. Det legges likevel til grunn at luftfarten har et omfattende rapporteringssystem hvor alle hendelser som har betydning for flysikkerheten i utgangspunktet skal rapporteres. Hendelser innen IKT-sikkerhet skal også rapporteres, i den grad de har betydning for flysikkerheten.

8.1.6 Sektor – transport – jernbane

Sikringsforskriften stiller krav til at jernbanevirksomheter skal ha styringssystem som dekker sikring, inkludert IKT-sikkerhet. Krav om systemer omfatter også etterlevelse og praktisering av bestemmelsene i systemet. Det stilles krav om at virksomhetene skal sikre at nødvendige tiltak blir satt i verk raskest mulig, og beredskapen skal blant annet omfatte beredskapsplanverk med tydelig rollefordeling, varslingslister og innsatsplaner.

8.1.7 Sektor – transport – vann

Forskrift om sikring av havner § 6 bestemmer at sikringshendelser skal varsles til Kystverket. Med sikringshendelse menes «[e]n mistenkelig handling eller omstendighet som utgjør en trussel mot et skip, et havneanlegg eller en havn.»

Det følger av ISM-koden punkt 9.1 at sikkerhetsstyringssystemet skal omfatte framgangsmåter som sikrer avvik, ulykker og farlige situasjoner rapporteres til selskapet, undersøkes og analyseres med det formål å forbedre sikkerheten og hindringen av forurensning.

8.1.8 Sektor – transport – vei

Som nevnt i punkt 7.1.8 foreligger det per i dag ingen lov- eller forskriftsregulering som stiller krav til IKT-sikkerhet på området trafikkstyring.

8.1.9 Sektor – bank

IKT-forskriften § 9 Avviks- og endringshåndtering sier at "Avvik som medfører vesentlig reduksjon i funksjonalitet som følge av brudd på konfidensialitet (beskyttelse av data), integritet (sikring mot uautoriserte endringer) eller tilgjengelighet til IKT-systemer og/eller data skal rapporteres til Finanstilsynet. Rapporteringen skal normalt omfatte hendelser som foretaket selv kategoriserer til alvorlighetsgrad svært alvorlig eller kritisk, men kan også omfatte andre avvik dersom disse avdekker spesielle sårbarheter i applikasjon, arkitektur, infrastruktur eller forsvarsverk".

Finanstilsynet har i høringsnotatet om forslag til gjennomføring av PSD2 i norsk rett foreslått mindre endringer i IKT-forskriften § 9. Videre legger Finanstilsynet til grunn en revidering av Rundskriv 15/2009: Rapportering av IKT-hendelser til Kredittilsynet, der retningslinjer for hendelsesrapportering utarbeidet av EBA (det europeiske banktilsynet) generelt vil bli lagt til grunn. Her stilles det blant annet krav til form og angivelse av grensekryssende konsekvenser.

Det fremgår av Rundskriv 15/2009 at "dersom samme hendelse rammer flere banker som samarbeider, kan bankene rapportere med én felles melding", noe som også følger av retningslinjene for hendelseshåndtering utarbeidet av EBA. NIS-direktivet inneholder ikke tilsvarende bestemmelse og det legges derfor grunn at en slik praksis ikke vil være i brudd med direktivet.

Lov 10. april 2015 nr. 17 om finansforetak og finanskonsern (*finansforetaksloven*) gjelder for finansforetak, herunder banker og kredittforetak. Formålet med loven er å bidra til finansiell stabilitet, herunder at finansforetak virker på en hensiktsmessig og betryggende måte. Med finansiell stabilitet menes at det finansielle systemet er robust nok til å motta og utbetale innskudd og andre tilbakebetalingspliktige midler fra allmennheten, formidle finansiering, utføre betalinger og omfordele risiko på en tilfredsstillende måte. Loven gjelder ikke for Norges Bank, jf. § 1-6.

For kredittinstitusjoner er det gitt nærmere regler om risikostyring og internkontroll i forskrift 22. august 2014 nr. 1097 om kapitalkrav og nasjonal tilpasning av CRR/CRD IV (CRR/CRD IV-forskriften).

Forskrift 21. mai 2003 nr. 630 om bruk av informasjons- og kommunikasjonsteknologi (IKT-forskriften) gjelder for foretak under tilsyn, herunder banker, kredittforetak og regulerte markeder.

Formålet med lov 17. desember 1999 nr. 95 om betalingssystemer m.v. kapittel 3 er å bidra til at systemer for betalingstjenester innrettes og drives slik at hensynet til sikker og effektiv betaling og til rasjonell og samordnet utførelse av betalingstjenester ivaretas.

Loven hjemler forskrift 17. desember 2015 nr. 1731 om systemer for betalingstjenester, som gjelder for blant annet banker og kredittinstitusjoner.

Det reviderte betalingstjenestedirektivet (PSD 2) inkluderer blant annet bestemmelser om både risikoanalyser, sikkerhet og hendelsesrapportering.[35] Det europeiske banktilsynet EBA har utarbeidet retningslinjer både for operasjonell- og sikkerhetsrisiko og for rapportering av hendelser. PSD 2 stiller blant annet krav til rapportering av hendelser til andre berørte medlemsstater.

I tidlig utkast til revidert direktiv var det direkte henvisninger til NIS-direktivets foreslåtte bestemmelser om operasjonell- og sikkerhetsrisiko og hendelsesrapportering. I det fastsatte direktivet er begge områdene imidlertid inntatt som egne bestemmelser. Forslag til innarbeidelse av direktivet i norsk rett har vært på høring, men regelverket er per i dag ikke fastsatt.

---

[35] Europaparlaments- og rådsdirektiv (EU) 2015/2366 av 25. november 2015 om betalingstjenester i det indre marked om endring av direktiv 2002/65/EF, 2013/36/EU og 2009/110/EF og forordning (EU) nr. 1093/2010, og oppheving av direktiv 2007/64/EF

8.1.10 Sektor – finansmarkedsinfrastruktur

Se beskrivelse av varsling etter IKT-forskriften over om banksektoren. Dersom den foreslåtte endringen i IKT-forskriften § 9, på bakgrunn av PSD 2, blir vedtatt, vil endringen også gjelde for denne sektoren.

8.1.11 Sektor – helsetjenester

Det følger av forskrift til personopplysningsloven § 2-6 at bruk av informasjonssystemer som er i strid med fastlagte rutiner, og sikkerhetsbrudd, skal behandles som avvik. Dersom avviket har medført uautorisert utlevering av personopplysninger hvor konfidensialitet er nødvendig, skal Datatilsynet varsles.

Etter normen punkt 6.3 skal Datatilsynet varsles dersom det har blitt foretatt en uautorisert utlevering av helse- og personopplysninger.

Det følger av helseberedskapsloven § 2- 3 at virksomheter loven omfatter, plikter å varsle om forhold innen helse- og omsorgstjenesten eller sosialtjenesten som kan gi grunnlag for tiltak etter denne lov. Varsel gis til departementet eller den myndighet departementet bestemmer.

I helse- og omsorgssektoren er det for øvrig en rekke bestemmelser med krav om å varsle uønskede hendelser. Disse hendelsene er imidlertid primært relatert til personskade og/eller bivirkninger ved pasientbehandlingen.

8.1.12 Sektor – forsyning og distribusjon av drikkevann

Som angitt i punkt 7.1.12 over skal Mattilsynet og abonnentene varsles ved avvik i vannkvaliteten. Andre avvik er ikke varslingspliktige til Mattilsynet. Varsling knyttet til svikt i elektroniske komponenter eller signaloverføringer er følgelig ikke spesifikt varslingspliktig etter drikkevannsforskriften med mindre de medfører avvik i vannkvaliteten.

8.1.13 Sektor – digital infrastruktur – samtrafikkpunkter på internett (IXP)

Norges samtrafikkpunkter er per i dag ikke gjenstand for ekomrettslig regulering eller krav til varsling.

8.1.14 Sektor – digital infrastruktur – tilbydere av DNS-tjeneste

Etter ekomloven § 2-7 fjerde ledd plikter tilbyder å varsle myndighetene straks dersom det foreligger særlig risiko for brudd på sikkerheten eller sikkerhetsbrudd som har krenket personvernet til abonnent eller bruker.

Etter ekomforskriften § 8-5 skal tilbyder «varsle Nasjonal kommunikasjonsmyndighet om hendelser som vesentlig kan redusere eller har redusert tilgjengeligheten til elektroniske kommunikasjonstjenester.»

Norske registrarer er som nevnt ikke underlagt sektorregelverk som stiller krav om IKT-sikkerhet eller varsling av IKT-sikkerhetshendelser.

8.1.15 Sektor – digital infrastruktur – registerenheter for toppdomener

Det gjelder per i dag ingen varslingskrav for registerenhetene.

8.2 Direktivet

8.2.1 Tilbydere av samfunnsviktige tjenester

Det følger av art. 14(3) at tilbydere av samfunnsviktige tjenester skal varsle tilsynsmyndigheten eller CSIRTen om hendelser som har betydelig innvirkning på opprettholdelsen av tjenesteleveransen.

I art. 4(7) defineres en «hendelse» som «ethvert tilfelle av reell negativ virkning på sikkerheten i nettverk og informasjonssystemer». Med begrepet «sikkerheten i nettverk og informasjonssystemer» menes «den evnen nett eller informasjonssystemer har til å tåle, på et gitt tillitsnivå, enhver handling som går ut over tilgjengeligheten, autentisiteten, integriteten eller tilliten til lagrede eller overførte eller behandlede data eller tilknyttede tjenester som tilbys eller er tilgjengelige via slike nett- og informasjonssystemer, jf. art. 4(2).[36]

Det ligger i begrepet «ethvert tilfelle» at årsaken til hendelsen er irrelevant. Det som betyr noe er om tjenesteleveransen er redusert. Sett hen til nevnte definisjoner kan det imidlertid ikke bare vurderes om tjenestens tilgjengelighet er berørt. Hendelser som har negativ innvirkning på autensiteten, integritet eller konfidensialiteten til data eller relaterte tjenester, kan potensielt utløse en varslingsplikt. NIS-samarbeidsgruppen utarbeider retningslinjer for hva som ligger i sikkerhetskravet. [37]

Ved vurderingen av om innvirkningen har vært betydelig skal det legges vekt på antall brukere av tjenesten som påvirkes, hendelsens varighet og størrelsen på det geografiske området som berøres av hendelsen. Varselet skal dessuten inneholde nok opplysninger til at det kan fastslås om hendelsen har virkninger utover Norges grenser.

Varsling av hendelser skal ikke medføre utvidet ansvar for tjenestetilbyderen. I fortalepunkt (57) trekkes det frem at ved eventuell offentliggjøring av hendelser må hensyn til publikums behov for informasjon veies opp mot mulige omdømme- og kommersielle konsekvenser for den som er rammet av hendelsen. I denne sammenheng må myndighetene ta særlig hensyn til behovet for å holde informasjon om produktsårbarheter hemmelig frem til det foreligger en tilstrekkelig god løsning på problemet.

[36] Definisjonen er hentet fra den uoffisielle norske oversettelsen av direktivet.
[37] COM(2017) 476 final/2 Vedlegg I s. 31.

Det følger av fortalepunkt (47) at kompetente myndigheter skal kunne utstede nasjonale retningslinjer om når og på hvilken måte tilbydere av samfunnsviktige tjenester skal varsle om hendelser.

8.2.2 Tilbydere av digitale tjenester

Det følger av art. 14(3) at tilbydere av digitale tjenester skal varsle tilsynsmyndigheten eller CSIRTen om hendelser som har betydelig innvirkning på opprettholdelsen av tjenesteleveransen.

Omtalen over av definisjonene av begrepene «hendelse» og «sikkerheten i nettverk og informasjonssystemer» er relevant også her.

Ved vurderingen av om innvirkningen på tjenesteleveransen har vært betydelig skal det legges vekt på fem forhold, hvorav tre er de samme som for samfunnsviktige tjenester. Det skal legges vekt på antall brukere av tjenesten, hendelsens varighet, den geografiske spredningen, omfanget av manglende funksjonalitet og omfanget av innvirkningene på økonomisk og samfunnsmessig aktivitet. Alle de fem punktene er nærmere spesifisert i EU-kommisjonens gjennomføringsregelverk fastsatt i medhold av direktivet art. 16(8) (CIR 2018/151).[38]

Som art. 14(3) avsluttes også art. 16(3) med at varsling av hendelser ikke skal medføre utvidet ansvar for tjenestetilbyderen.

8.3 Departementets vurdering

Etter *sikkerhetsloven* skal det varsles om hendelser som direkte eller indirekte kan skade nasjonale sikkerhetsinteresser. Etter NIS-direktivet skal det varsles om hendelser som har betydelig innvirkning på opprettholdelsen av tjenesteleveransen.

Virksomheter som er omfattet av sikkerhetsloven skal varsle om hendelser allerede dersom det er begrunnet mistanke om en hendelse. I tillegg er det tilstrekkelig at det er fare for indirekte skade. Etter direktivet skal det varsles først etter at det er klart at hendelsen har hatt betydelig innvirkning på opprettholdelsen av tjenesteleveransen. Terskelen for varsling etter sikkerhetsloven er således lavere enn etter lovutkastet, og så langt er sikkerhetsloven dekkende for NIS-direktivet.

Vurderingstemaet for varsling etter de to regelverkene er imidlertid ulikt utformet. Det innebærer at virksomheten i hvert tilfelle må vurdere om det skal varsles etter bare ett eller begge regelverkene. Varslingsplikten som følger av sikkerhetsloven § 4-5 bokstav a

[38] COMMISSION IMPLEMENTING REGULATION (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact.

og b begrenser seg til å handle om tilsiktede handlinger. Bokstav c har ikke en slik begrensning, men handler i stedet om alvorlige brudd på sikkerhetskravene i loven kapittel 5, 6 eller 7.

Varsling etter *personopplysningsloven* skiller seg fra NIS-direktivet på flere måter. Ikke bare skal det varsles til andre myndigheter, det skal også varsles om andre forhold. Det er klart at varslingsreglene som følger av personopplysningsloven ikke er dekkende for kravene som følger av NIS-direktivet. Ettersom det er ulike krav kan det hende at hendelser skal varsles i henhold til begge regelverkene. Hendelser som varsles i henhold til lovutkastet, men som også innebærer brudd på personopplysningssikkerheten, skal også varsles i henhold til personopplysningsloven.

Dersom forslaget til ny beredskapsforskrift etter hvert blir vedtatt, blir varslingsreglene som gjelder for elektrisitetssektoren dekkende for NIS-direktivets krav. Varslingsreglene som gjelder for sektorene bank og finansmarkedsinfrastruktur, inkludert forslag til endringer i IKT-forskriften, er dekkende for NIS-direktivets krav. Tilbydere av DNS-tjenester er også underlagt varslingskrav som tilsvarer NIS-direktivets krav.

Det gjelder en rekke krav om varsling i jernbanesektoren. Det er imidlertid ikke klart om det følger av gjeldende regelverk om det per i dag varsles om den type hendelser som skal varsles etter lovutkastet.

For øvrig stiller ikke gjeldende lover og forskrifter varslingskrav som tilsvarer direktivet. Noen regelverk har ikke varslingskrav i det hele tatt, noen krever varsling av andre typer hendelser, noen krever varsling til andre enn myndighetene og noen er tause om varselets innhold.

Selv om enkelte lover og forskrifter har relativt like varslingskrav, mener departementet det likevel er mest hensiktsmessig at det i den foreslåtte loven stilles likelydende krav om varsling av hendelser til myndighetene. Se lovutkastet §§ 8 og 10. Det vil følge av lovutkastet § 5 *Forholdet til andre lover*, at i den grad denne typen hendelser etter gjeldende regelverk eller praksis allerede varsles til relevante myndigheter, vil direktivet ikke medføre endringer. I motsatt fall vil virksomheten måtte følge direktivets varslingskrav.

Det er flere grunner til at hendelser skal varsles til myndighetene. For det første av hensyn til den aktuelle virksomheten. Dersom denne har behov for bistand fra myndighetene til å håndtere hendelsen er det en forutsetning at det varsles til rette myndighet og at varselet inneholder nok informasjon til at det er mulig for den som blir varslet å bistå. For det andre vil sektormyndigheten få muligheten til å varsle videre til andre i samme sektor, til nasjonale myndigheter, og i enkelte tilfeller til andre land. For det tredje skal varslinger danne et nyttig kunnskapsgrunnlag for sikkerhetsmyndighetene.

Som nevnt tidligere har departementet ved utforming av bestemmelsene om varsling ment å fange opp det samme som direktivets krav. Utover det som følger av direktivet mener departementet at varslingen av hendelser i størst mulig grad bør skje i tråd med *Rammeverk for håndtering IKT-sikkerhetshendelser,* se nærmere kapittel 9.1.

Departementet har foreløpig ikke tatt endelig stilling til hvilke myndigheter som i alle tilfeller skal ta imot varsler. Det legges imidlertid opp til at eksisterende myndighetsstruktur bør benyttes i størst mulig grad. Det vil kunne variere fra sektor til sektor om det er sektormyndigheter eller responsmiljøer som skal ha oppgaven med å motta varsler etter loven. Dette vil også ha sammenheng med de andre oppgavene som skal utføres etter lovutkastet.

Utover den generelle føringen i direktivet om at det skal stilles noe mindre strenge krav til tilbydere av digitale tjenester, gis det ikke særlige føringer på hvor store forskjeller det er snakk om eller hva dette betyr i praksis. Kravene som stilles om varsling til tilbydere av digitale tjenester er som nevnt konkretisert i EU-kommisjonens gjennomføringsforordning. De samme kravene vil komme til å gjelde i Norge.

9. RESPONSMILJØER

9.1 Gjeldende rett

Det følger av *sikkerhetsloven* (2018) § 2-4 at Kongen skal utpeke en myndighet som skal drive en nasjonal responsfunksjon for alvorlige digitale angrep. Bestemmelsen gir hjemmel til å behandle personopplysninger i forbindelse med utøvelse av responsfunksjonen. Nærmere bestemmelser om responsfunksjonen følger av forskriftene til sikkerhetsloven.

Justis- og beredskapsdepartementet etablerte i 2017 sammen med Forsvarsdepartementet *Rammeverk for håndtering av IKT-sikkerhetshendelser.*[39] Det følger av rammeverket punkt 1.2 at formålet rammeverket er:

- å skape god situasjonsoversikt gjennom aggregering og koordinering av informasjon om alle relevante IKT-sikkerhetshendelser
- å effektivt håndtere alvorlige IKT-sikkerhetshendelser fra virksomhetsnivå til politisk nivå gjennom god utnyttelse av samfunnets samlede ressurser
- at Norge fremstår koordinert overfor andre land og internasjonale organisasjoner

Det følger så videre at rammeverket «beskriver en systematisk tilnærming til håndtering av IKT-sikkerhetshendelser på tvers av virksomheter og sektorer for å sikre en effektiv nasjonal sektorovergripende håndteringsevne». Rammeverket retter seg i første rekke mot offentlige og private virksomheter som har betydning for kritisk infrastruktur

[39] https://nsm.stat.no/publikasjoner/rad-og-anbefalinger/rammeverk-hendelseshandtering/

og/eller kritiske samfunnsfunksjoner,[40] sektorvise responsmiljøer,[41] myndigheter som har en rolle knyttet til håndtering av IKT-sikkerhetshendelser og departementer.

Det er først og fremst de berørte departementene som er forpliktet til å følge opp rammeverket. Rammeverket er ikke juridisk bindende overfor virksomheter i privat sektor.

9.2 Direktivet

Art. 9 sier at hver medlemsstat skal utpeke en eller flere CSIRTer (computer security incident response team - responsmiljø) som skal oppfylle kravene som følger av direktivet vedlegg I. Det stilles der krav om blant annet kommunikasjons- og infrastruktursikkerhet og at miljøet til enhver tid skal være tilgjengelig. Responsmiljøet skal blant annet overvåke hendelser på nasjonalt nivå, respondere på hendelser, bidra med analyser og situasjonsforståelse og delta i det under direktivet etablerte CSIRT-nettverket.

Responsmiljøet(ene) skal dessuten dekke minst direktivets virkeområde, jf. vedlegg II og III til direktivet, og være ansvarlig for risiko- og hendelseshåndtering.

Direktivet stiller ikke krav om mer enn ett responsmiljø eller at alle hendelser skal rapporteres direkte til responsmiljøet.

9.3 Departementets vurdering

Direktivet stiller ikke krav som nødvendiggjør lovregulering av hendelseshåndteringsmiljøer. Det vil for eksempel være innenfor det nasjonale handlingsrommet å beslutte at NSM NorCERT skal ta imot alle varsler etter loven. Det er også rom for at tilsynsmyndigheter kan ta imot varsler.

Med utgangspunkt i det systemet som per i dag finnes for håndtering av digitale angrep, jf. *Rammeverk for håndtering av IKT-sikkerhetshendelser*, så mener departementet at det bør lovfestes en hjemmel for å kunne utpeke hvilke virksomheter skal kunne ta imot varsler etter loven. For å følge opp allerede påbegynt arbeid med håndtering av hendelser bør det legges til rette for at virksomheter som omfattes av loven varsler om hendelser i de samme kanalene som allerede er opprettet. I den sammenheng mener departementet det er mest hensiktsmessig at Kongen kan utpeke både offentlige og private rettssubjekter som hendelseshåndteringsmiljøer etter loven.

Videre bør det være mulig i forskrift å bestemme nærmere hvilke krav som skal stilles til disse miljøene, slik at de kan oppfylle de forpliktelser direktivet stiller til håndtering av varsler. Det kan også bli aktuelt å gi miljøene mer konkrete hjemler for deling av

[40] DSBs rapport «Samfunnets kritiske funksjoner»(2016) redegjør for virksomheter som har betydning for kritisk infrastruktur og samfunnskritiske funksjoner.
[41] Se nærmere om sektorvise responsmiljøer i rammeverket, og i Meld. St. 38 (2016-2017), s. 29, hvor det blant annet fremgår at responsmiljøene "skal ha oversikt i egen sektor, være informasjonsknutepunkt for alle relevante virksomheter og være sektorens bindeledd mot NSM.»

informasjon seg imellom, med virksomheter de opererer på vegne av og med andre aktører som er nødvendige å kommunisere med for å håndtere hendelser på en god måte. Forslag til en bestemmelse om responsmiljøer er inntatt i lovutkastet § 11.

Departementet erkjenner at det på dette punktet foreslås regler utover minimumskravene i direktivet. Det er derfor her særlig ønskelig med innspill fra høringsinstansene. Departementet ser for øvrig for seg at IKT-sikkerhetsutvalget kan komme med anbefalinger knyttet til dette punktet.

10. TILSYNSMYNDIGHETER

10.1 Gjeldende rett

10.1.1 Tverrsektorielt

Sikkerhetsloven (2018) kapittel 3 regulerer tilsyn. Lovens hovedregel følger av § 3-1 som sier at sikkerhetsmyndigheten (i praksis Nasjonal sikkerhetsmyndighet) fører tilsyn med virksomheter som omfattes av loven. Et sektordepartement kan imidlertid i henhold til andre ledd bestemme at «myndigheter med sektoransvar som fører tilsyn med beskyttelse av informasjon, informasjonssystemer, objekter eller infrastruktur», i stedet skal føre slikt tilsyn. I praksis betyr dette at gjeldende sektormyndigheter kan føre tilsyn etter sikkerhetsloven, så fremt de har kompetanse til det.

Sikkerhetsmyndigheten skal i tillegg føre tilsyn med andre tilsynsmyndigheter, jf. § 3-1 tredje ledd. Et slikt tilsyn skal undersøke om sektormyndighetenes tilsyn etter sikkerhetsloven føres i tråd med sikkerhetslovens krav og de grunnleggende kriteriene for tilsyn som er fastsatt av sikkerhetsmyndigheten.

§ 3-2 regulerer samarbeid mellom sikkerhetsmyndigheten og andre myndigheter med tilsynsansvar. Første ledd bestemmer at det skal inngås en samarbeidsavtale og at gjennomføring av tilsyn så langt det er mulig skal samordnes med andre tilsynsmyndigheter. Etter andre ledd skal sikkerhetsmyndigheten utarbeide og utvikle grunnleggende kriterier for tilsyn og legge til rette for felles opplæring av tilsynspersonell. Når det er nødvendig kan sikkerhetsmyndigheten medvirke til forberedelse og gjennomføring av tilsyn som i utgangspunktet skal utføres av en sektormyndighet.

Etter § 3-4 kan tilsynsmyndigheten kreve tilgang til virksomhetens informasjon, informasjonssystemer, objekter og infrastruktur. Tilsynsmyndighetene har etter § 3-6 mulighet til å gi pålegg om gjennomføring av tiltak som er nødvendige for å ivareta lovens formål.

Tilsyn med anvendelsen av *personopplysningsregelverket* er relativt utførlig regulert i personvernforordningen Kapittel VI. Tilsynets oppgaver er listet opp i art. 57. I Norge vil det fortsatt være Datatilsynet som er den sentrale myndighet som skal føre tilsyn med

etterlevelse av regelverket. Datatilsynet skal både føre tilsyn, håndheve anvendelsen av reglene og behandle klager. Tilsynsmyndigheten skal også ha rådgivnings- og informasjonsoppgaver. Den skal også vedta standardkontraktsvilkår, godkjenne adferdsnormer og bindende virksomhetsregler og utarbeide kriterier for akkrediterings- og sertifiseringsoppgaver.

Etter art. 58 skal tilsynsmyndigheten ha undersøkelsesmyndighet, myndighet til å beslutte korrigerende tiltak og til å godkjenne visse typer behandlinger samt standardregler.

eForvaltningsforskriften har ikke regler om tilsyn.

10.1.2 Sektor – energi – elektrisitet

Energiloven § 10-1 bestemmer at «[d]epartementet kan gi de pålegg som er nødvendige for gjennomføringen av bestemmelser gitt i eller i medhold av denne lov. Departementet fører kontroll med at bestemmelser gitt i eller i medhold av denne lov blir overholdt.» Det følger av beredskapsforskriften § 2-10 tredje ledd at «[i]nternkontrollsystemet skal være tilrettelagt for gjennomføring av tilsyn i samsvar med de krav som er stilt.»

Norges Vassdrags- og energidirektorat fører tilsyn med de som i dag har IKT-sikkerhetskrav i beredskapsforskriften, altså nettselskaper, kraftprodusenter og fjernvarmeselskaper, men ikke med de som ikke har IKT-sikkerhetskrav fra beredskapsforskriften, rene kraftleverandører og markedsplassen Nordpool. Med oppdatert beredskapsforskrift vil de kraftleverandørene som blir å anse som "operators of essential services", og dermed underlagt beredskapsforskriften, også bli ført tilsyn med. Markedsplassen har krav gjennom IKT-forskriften FOR-2003-05-21-630 (Autoriserte markedsplasser er nevnt i IKT-forskriften § 1) og den er det finanstilsynet som følger opp.

10.1.3 Sektor – energi – olje

Petroleumsloven § 10-3 bestemmer at «[d]epartementet1 fører tilsyn med at bestemmelsene gitt i eller i medhold av denne lov blir overholdt av alle som utøver petroleumsvirksomhet som omfattes av loven. Departementet kan gi de pålegg som er nødvendige for gjennomføringen av bestemmelsene gitt i eller i medhold av denne lov.»

Petroleumstilsynet fører tilsyn med næringens håndtering av IKT-sikkerhet. I mai/juni 2017 ble det gjennomførte en tilsynskampanje med alle operatører med felt og anlegg i drift og redere med innretninger som har samsvarsuttalelse (SUT). Tilsynet rettet seg mot virksomhetenes arbeid med beskyttelse av datasystemer på anlegg og innretninger som ivaretar styring av prosessene, overvåker mulige gassutslipp eller branntilløp, samt foretar sikker nedstengning av innretninger og anlegg.

For drivstofforsyningen finnes det ikke sektorspesifikt regelverk om relevant tilsyn.

10.1.4 Sektor – energi – gass

Regelverket som er beskrevet i avsnittet over om oljesektoren, gjelder for petroleumsvirksomhet, og dermed også for deler av den norske gassvirksomheten.

Lov om 28. juni 2002 nr. 61 om felles regler for det indre marked for naturgass (naturgassloven) og tilhørende naturgassforskrift har ikke relevante bestemmelser om tilsyn.

10.1.5 Sektor – transport – luft

Flysikringsforordningen art. 4 bestemmer at for å oppnå det sertifikatet som er nødvendig for å yte flysikringstjenester, skal en organisasjon oppfylle de generelle krav til yting av flysikringstjenester som er oppført i forordningen vedlegg I og de særlige tilleggskrav som er oppført i vedlegg II til V. En utpekt myndighet skal kontrollere at organisasjonen oppfyller de felles krav før den utsteder et sertifikat til den.

Luftfartstilsynet fører tilsyn med IKT-sikkerheten. Så langt har Luftfartstilsynet hatt særlig fokus på flysikringstjenesten. Fremover skal tilsynet omfatte flere tjenester i sektoren.

10.1.6 Sektor – transport – jernbane

Statens jernbanetilsyn fører tilsyn med at bestemmelsene i sikringsforskriften overholdes, jf. jernbaneloven § 11. Blant annet skal «[e]nhver skal etter pålegg fra tilsynsmyndigheten gi de opplysninger den krever for å utføre sine oppgaver. Tilsynsmyndigheten kan bestemme i hvilken form opplysningene skal gis.» Videre skal tilsynsmyndigheten «til enhver tid ha uhindret adgang til ethvert sted som omfattes av loven.»

10.1.7 Sektor – transport – vann

Kystverket fører tilsyn med havner og havneanlegg, herunder deres oppfyllelse av sikringsregelverkene. I den utstrekning enhetens IKT-systemer er beskyttet under dette regelverket vil dette omfattes av tilsynet. Kystverket har ifølge forskrift om sikring av havneanlegg § 20 andre ledd myndighet til å gi de pålegg og treffe de vedtak som er nødvendig for gjennomføring av bestemmelsene i forskriften. Tilsvarende myndighet følger av forskrift om sikring av havner § 18.

Det følger av skipssikkerhetsloven § 41 første ledd at kongen fastsetter hvem som skal ha tilsynsmyndighet etter loven. Det skal blant annet føres tilsyn med sikkerhetsstyringssystemet, og det er plikt til å medvirke til tilsynet. Tilsyn er for øvrig inngående regulert i blant annet forskrift 22. desember 2014 nr. 1893.

10.1.8 Sektor – transport – vei

Det foreligger per i dag ingen lov- eller forskriftsregulering som stiller krav til IKT-sikkerhet på området trafikkstyring. I stedet gjelder interne retningslinjer som definerer

rutiner for bruk, drift og utvikling av automasjonsnettet og SCADA-systemet, samt tilhørende nettverk. Vegdirektoratet sørger sammen med regionene i Statens vegvesen for en hensiktsmessig samordning, der krav og rutiner videreutvikles i takt med endringer i omgivelsene og inngår i etatens kvalitetssystem.

Innen ferjetransporten er virksomheter som er underlagt krav etter forskrift om sikkerhetsstyringssystem for norske skip og flyttbare innretninger omfattet av Sjøfartsdirektoratets tilsynsmyndighet (ISM sertifisering).

10.1.9 Sektor – bank

Finanstilsynet fører tilsyn med de aktuelle virksomhetene, se lov 7. desember 1956 nr. 1 om tilsynet med finansforetak mv. (Finanstilsynsloven) § 1. Dette inkluderer tilsyn med IKT-sikkerheten i virksomhetene. Virksomhetene har medvirkningsplikt og tilsynet har påleggskompetanse.

Hvert år redegjør Finanstilsynet i en egen rapport for sitt syn når det gjelder risiko og sårbarhet innen finanssektoren knyttet til finanssektorens bruk av IKT.

10.1.10 Sektor – finansmarkedsinfrastruktur

Punktet over om banksektoren gjelder også for finansmarkedsinfrastruktur.

10.1.11 Sektor – helsetjenester

Datatilsynets oppgaver tar i hovedsak utgangspunkt i personopplysningsloven med hovedfokus på personvern, men de har i tillegg tilsynsansvar for pasientjournalloven. Tilsyn med helseregistrene vil i hovedsak også utføres av Datatilsynet.

Det finnes i dag ikke et eget sektortilsyn for informasjonssikkerhet på helseområdet. Statens helsetilsyn er øverste tilsynsmyndighet og har det overordnede faglige tilsynet med helse- og omsorgstjenestene og folkehelsearbeid, jf. helsetilsynsloven § 1. Statens helsetilsyn har myndighet til å pålegge retting av avvik, jf. § 5. Fylkesmannen er faglig underlagt Statens helsetilsyn og fører tilsyn. Helsetilsynet har fått i oppdrag å utrede roller og kompetansebehov knyttet til hvordan IKT-området skal ivaretas.

Ansvarsfordelingen mellom Statens helsetilsyn og Helsedirektoratet/Direktoratet for e-helse vil på IKT-området ikke være annerledes enn på andre områder innenfor helse- og omsorgssektoren. Helsedirektoratet og Direktoratet for e-helse er fagorganer som fortolker regelverket og normerer på området. Begge direktoratene har oppgaver med å følge med på forhold som påvirker utviklingen innenfor sine ansvarsområder, de skal bidra til at vedtatt politikk settes i verk og gi råd og veiledning overfor sentrale og lokale myndigheter, privat sektor, frivillige organisasjoner mv. Helsedirektoratet har en koordinatorrolle for sektorens innsats ved kriser. Det gjelder også hendelser som inkluderer svikt i IKT-systemer.

10.1.12 Sektor – forsyning og distribusjon av drikkevann

Mattilsynet fører i henhold til drikkevannsforskriften § 28 tilsyn med alle vannforsyningssystemer som vil kunne omfattes av NIS-direktivet. Med samme hjemmel kan Mattilsynet fatte nødvendige vedtak for å sikre etterlevelse av forskriftens krav. Det følger av forskriften § 24 andre ledd at «[d]ersom Mattilsynet ber om det, skal vannverkseieren gi Mattilsynet de opplysningene som er nødvendige for at Mattilsynet skal kunne gjennomføre sine oppgaver etter denne forskriften.» Mattilsynet har de senere årene hatt fokus på driftskontrollsystemene (DKS) til vannverkene.

10.1.13 Sektor – digital infrastruktur – samtrafikkpunkter på internett (IXP)

Norges samtrafikkpunkter er per i dag ikke gjenstand for ekomrettslig regulering eller krav til sikkerhet. For å sikre et framtidig behov for å regulere ytterligere krav til sikkerhet for andre enn tilbydere gjennomførte SD en lovendring i 2012-2013 (jf. prop. 69L side 104), som implementerte forskriftskompetanse etter ekomloven § 2-10 for andre enn tilbydere, jf. ekomloven § 2-10 femte ledd. Denne kompetansen ble innført for å kunne ta høyde for behovet for å sikre nødvendig regulering av aktører som blant annet Norid og samtrafikkpunktene på Internett (IXP). Nasjonal kommunikasjonsmyndighet fører i dag likevel ikke tilsyn med IKT-sikkerheten for samtrafikkpunktene på internett.

10.1.14 Sektor – digital infrastruktur – tilbydere av DNS-tjeneste

Nkom fører tilsyn, inkludert tilsyn med IKT-sikkerheten, for virksomheter som er tilbydere av tilgang til internett og samtidig også er tilbydere av DNS tjenester, jf. ekomloven § 10-1. Tilsynsmyndigheten kan kreve opplysninger som er nødvendige for gjennomføringen av loven eller vedtak gitt i medhold av loven. Den som er gjenstand for tilsyn har medvirkningsplikt. Myndigheten har påleggskompetanse.

10.1.15 Sektor – digital infrastruktur – registerenheter for toppdomener

Det følger av domeneforskriften § 9 at nasjonal kommunikasjonsmyndighet fører tilsyn med at bestemmelsene i forskriften overholdes, jf. ekomloven § 10-1.

10.2 Direktivet

NIS-direktivet art. 8 og 9 bestemmer at medlemsstatene skal utpeke eller etablere et nasjonalt kontaktpunkt, en eller flere kompetente myndigheter og ett eller flere hendelseshåndteringsmiljøer.

Den (eller de) kompetente myndigheten(e) skal i henhold til art. 8 for det første dekke hele direktivets virkeområde, jf. direktivet vedlegg II og III. Rollen som kompetent myndighet kan tildeles en eller flere eksisterende nasjonale myndigheter. Kompetent myndighet skal overvåke anvendelsen av direktivet, herunder kunne føre tilsyn med virksomhetenes etterlevelse av direktivet. Medlemsstaten skal sørge for at kompetent myndighet har tilstrekkelige ressurser og virkemidler for gjennomføring av oppgavene som tillegges dem etter direktivet.

10.2.1 Tilbydere av samfunnsviktige tjenester

Art. 15 regulerer tilsyn med *tilbydere av samfunnsviktige tjenester*. Tilsynsmyndighetene skal ha hjemler til å innhente følgende fra tilbyderne av samfunnsviktige tjenester:

a. Nødvendig informasjon for å kunne vurdere sikkerheten i deres nettverk og informasjonssystemer, herunder dokumentert sikkerhetspolicy
b. Dokumentasjon som viser effektiv gjennomføring av sikkerhetspolicyen, slik som resultater av sikkerhetsrevisjoner utført av kompetent inspektør og, i sistnevnte tilfelle, stille resultatene og den underliggende dokumentasjonen til rådighet for kompetent myndighet

Når det anmodes om slike opplysninger eller slik dokumentasjon, skal formålet med anmodningen angis og hvilke opplysninger som kreves skal presiseres. Kompetent myndighet skal i henhold til art. 15(4) samarbeide tett med personvernmyndighetene når hendelser som innebærer brudd på personopplysningsregelverket håndteres.

10.2.2 Tilbydere av digitale tjenester

Art. 17 regulerer tilsyn med *tilbydere av digitale tjenester*. Det følger av art. 17(1) at når det foreligger dokumentasjon på at en tilbyder av digitale tjenester ikke oppfyller direktivets krav, skal kompetent myndighet i ettertid ved behov gjennomføre tilsyn. Tilsynsmyndigheten kan da kreve at virksomheten

a. Gir nødvendige opplysninger for å kunne vurdere sikkerheten i nettverkene og informasjonssystemene deres, herunder en dokumentert sikkerhetspolicy
b. Utbedrer evenuelle avvik

I følge fortalepunkt (60) kan relevant informasjon komme fra eksempelvis tilbyderen selv, en annen tilsynsmyndighet (også i andre land), eller fra en bruker av tjenesten. Tilsynsmyndighetene bør derfor ikke ha en forpliktelse til å kontrollere tilbydere av digitale tjenester.

Det følger av art. 17(3) at myndigheter i ulike medlemsstater skal samarbeide og bistå hverandre ved behov i de tilfeller en virksomhet har sitt hovedforetak eller representant i én medlemsstat og sine nett- og informasjonssystemer i et annet.

10.3 Departementets vurdering

Slik som direktivets krav er utformet står medlemslandene fritt til å organisere myndigheter som skal utføre oppgaver relatert til direktivet slik de vil. For Norges del er det altså ikke nødvendig å endre på gjeldende organisering innenfor IKT-sikkerhet, for å oppfylle direktivets krav. Imidlertid må det vurderes om myndighetene har tilstrekkelige hjemler til å føre tilsyn med etterlevelse av direktivets krav til virksomhetene.

Direktivet krever at det skal føres tilsyn med at virksomhetene etterlever kravene som følger av direktivet. Det ligger i dette blant annet at tilsynsmyndighetene må ha tilgang på informasjon som virksomheten besitter.

Gjennomgangen av gjeldende rett viser at det i mange sektorer er etablert myndigheter som fører tilsyn med det gjeldende regelverket. Men som det fremgår av kapittel 7.3 er det samtidig for mange sektorer uklart om gjeldende regelverk stiller krav om nettverk og informasjonssikkerhet. Dermed er det også uklart om tilsynsmyndighetene kan føre tilsyn med IKT-sikkerheten.

For noen sektorer er det klart at gjeldende rett ikke dekker direktivets krav om tilsyn. Enten fordi det er klart at det ikke er etablert relevant sektormyndighet som fører tilsyn eller at gjeldende regler ikke stiller tilstrekkelige sikkerhetskrav.

For sektorene elektrisitet, bank, finansmarkedsinfrastruktur og drikkevann, synes det klart at gjeldende regelverk er dekkende. Samfunnsviktige nettverks- og informasjonssystemer som allerede er omfattet av sikkerhetslovens virkeområde er også underlagt en tilsynsordning som dekker NIS-direktivets krav.

Særlig fordi mange virksomheter per i dag ikke er underlagt tilsyn om IKT-sikkerhet, foreslår departementet i lovutkastet § 12 bestemmelser om tilsyn som er ment å skulle tilsvare direktivets krav. Spørsmålet om lovutforming er drøftet mer utførlig i kapittel 4.

Dette innebærer blant annet, i tråd med direktivet, at det skal være forskjellige tilsynsregimer for henholdsvis tilbydere av samfunnsviktige tjenester og tilbydere av digitale tjenester. Mens regimet som vil gjelde for tilbydere av samfunnsviktige tjenester er av mer tradisjonell karakter, vil det føres langt færre tilsyn med tilbydere av digitale tjenester, og da kun i etterkant av at det foreligger mistanke om brudd på lovens krav.

I lovutkastet § 13 foreslår departementet å gi tilsynsmyndigheten kompetanse til å pålegge den som overtrer lovens bestemmelser å bringe de ulovlige forholdene til opphør. Pålegg kan gis i tilknytning til alle typer brudd på loven, forskrifter gitt i medhold av loven eller enkeltvedtak fattet med hjemmel i loven eller forskrifter. Påleggskompetansen er ikke avgrenset til grove eller gjentatte brudd på loven. Pålegg kan gis uavhengig av lovovertrederens subjektive skyld.

Departementet foreslår i lovutkastet § 14 at tilsynsmyndigheten gis hjemmel til å ilegge tvangsmulkt. Formålet med tvangsmulkten er å sikre oppfyllelse av pålegg fastsatt i medhold av lovutkastet § 13. Vedtak om tvangsmulkt kan fastsettes samtidig med pålegget.

Tvangsmulkt kan fastsettes i tilknytning til alle pålegg om tiltak. Tvangsmulkt kan således ilegges uavhengig av subjektiv skyld og uavhengig av omfanget av overtredelsen.

Tvangsmulktens størrelse fastsettes under hensyn til hvor viktig det er at pålegget blir gjennomført og hvilke kostnader det antas å medføre. Tvangsmulkt skal fungere som et pressmiddel, og utgangspunktet er at mulkten skal være så stor at den er effektiv uten å være urimelig.

11. SANKSJONER

11.1 Gjeldende rett

11.1.1 Tverrsektorielt

Det finnes ingen sanksjonsbestemmelser i gjeldende sikkerhetslov.

Sikkerhetsloven (2018) kapittel 11 regulerer sanksjoner og straff. Tilsynsmyndigheten gis hjemmel for å fastsette tvangsmulkt og pålegge overtredelsesgebyr. Loven fastsetter ikke spesifikke beløp, men gir vurderingskriterier for fastsettelse av beløpenes størrelse. Det skal særlig legges vekt på «overtredelsens grovhet, overtredelsens varighet, utvist skyld og virksomhetens omsetning.» Forsettlige og uaktsomme overtredelser av nærmere bestemte forpliktelser er dessuten straffbelagt, jf. § 11-4.

Personopplysningsloven kapittel 7 regulerer sanksjoner og tvangsmulkt. Hovedregelen om overtredelsesgebyr er personvernforordningen art. 83, og det fremgår der i hvilke tilfeller dette kan ilegges. Det fremgår også av bestemmelsen at det kan gis gebyrer på opp til både 10 millioner euro og 20 millioner euro avhengig av overtredelsens karakter. Det følger av art. 83 at det skal foretas en konkret vurdering av hver enkelt sak ved vurdering av om overtredelsesgebyr skal ilegges og det eventuelle gebyrets størrelse.

I tillegg følger det av personopplysningsloven at Datatilsynet ogsåkan ilegge overtredelsesgebyr ved overtredelse av forordningen art. 10 om behandling av personopplysninger om straffedommer og lovovertredelser eller tilknyttede sikkerhetstiltak og art. 24 om internkontroll. Personopplysningsloven § 29 gir i tillegg Datatilsynet hjemmel til å fastsette tvangsmulkt for oppfyllelse av pålegg etter loven.

Forvaltningsloven har generelle bestemmelser om forvaltningsorganers mulighet til å ilegge administrative sanksjoner, herunder både overtredelsesgebyr og tvangsmulkt. Det er imidlertid ingen bestemmelser om sanksjonering av overtredelse av eForvaltningsforskriften.

11.1.2 Sektor – energi – elektrisitet

Energiloven §§ 10-3 og 10-7 hjemler henholdsvis tvangsmulkt og overtredelsesgebyr. Det samme gjør beredskapsforskriften §§ 8-4 og 8-5.

11.1.3 Sektor – energi – olje

Petroleumsloven § 10-16 hjemler flere tvangsmidler, herunder tvangsmulkt. Overtredelsesgebyr er ikke regulert, men i § 10-13 gis Kongen myndighet til å tilbake tillatelser som er gitt i medhold av loven.

For drivstofforsyningen finnes det ikke sektorspesifikt regelverk som regulerer sanksjoner.

11.1.4 Sektor – energi – gass

Regelverket som er beskrevet i avsnittet over om oljesektoren, gjelder for petroleumsvirksomhet, og dermed også for deler av den norske gassvirksomheten.

11.1.5 Sektor – transport – luft

Luftfartsloven §§ 13 a-4 og 13 a-5 gir hjemmel for henholdsvis å fastsette tvangsmulkt og å gi pålegg om overtredelsesgebyr i forbindelse med overtredelser av loven eller bestemmelser fastsatt med hjemmmel i loven, herunder forskrift om felles krav for yting av flysikringstjenester.

11.1.6 Sektor – transport – jernbane

Jernbaneloven § 13 hjemler tvangsmulkt ved manglende oppfylling av pålegg. § 14 gir hjemmel til å fastsette forskrift om gebyr for kontrolltiltak som gjennomføres for å sikre at loven eller vedtak i medhold av loven blir fulgt.

11.1.7 Sektor – transport – vann

Havne- og farvannsloven § 54 gir departementet hjemmel til å «gi forskrifter om gebyr for kontrolltiltak og tilsyn som gjennomføres for å sikre at loven eller vedtak i medhold av loven blir fulgt.» Etter § 58 kan «myndigheten» utferdige forelegg mot den som innen fastsatt frist unnlater å etterkomme pålegg eller forbud som er gitt med hjemmel i loven. Loven § 60, forskrift om sikring av havneanlegg § 22 og forskrift om sikring av havner § 20 hjemler tvangsmulkt.

Skipssikkerhetsloven kapittel 8 til 10 regulerer sanksjoner og straff. § 50 hjemler tvangsmulkt, § 55 hjemler overtredelsesgebyr og § 56 hjemler overtredelsesgebyr mot rederiet. Blant annet er overtredelse av § 6 om rederiets alminnelige plikter mulig grunnlag for ileggelse av overtredelsesgebyr.

Nærmere bestemmelser om overtredelsesgebyr følger av forskrift 2. juli 2007 nr. 852 om fastsettelse og gjennomføring av overtredelsesgebyr etter lov 16. februar 2007 nr. 9 om skipssikkerhet (skipssikkerhetsloven) § 55 og § 56.

11.1.8 Sektor – transport – vei

Det foreligger som nevnt per i dag ingen lov- eller forskriftsregulering som stiller krav til IKT-sikkerhet på området trafikkstyring.

11.1.9 Sektor – bank

Finanstilsynet har etter finanstilsynsloven påleggsmyndighet. Blant annet kan tilsynet gi pålegg om at foretaket skal innrette sin internkontroll etter de bestemmelser tilsynet fastsetter, jf. § 4 og om å stanse virksomhet, jf. § 4 a.

I medhold av finanstilsynsloven § 10 kan departementet bestemme at det skal betales løpende mulkt ved forsettlig eller uaktsom overtredelse av bestemmelser gitt i eller i medhold av loven.

Finansforetaksloven gir i § 22-2 departementet hjemmel til å gi pålegg og tvangsmulkt ved overtredelse av bestemmelser gitt i eller i medhold av loven. Tilsvarende hjemmel finnes i betalingssystemloven § 6-3.

11.1.10 Sektor – finansmarkedsinfrastruktur

Børsloven § 47 gir Finanstilsynet hjemmel til å gi pålegg om retting og stansing.

Verdipapirhandelloven § 16-3 gir Finanstilsynet hjemmel til å gi pålegg om retting og stansing.

11.1.11 Sektor – helsetjenester

Helsetilsynsloven § 5 gir Statens helsetilsyn adgang til å gi pålegg om å «rette på forholdene».

Pasientjournalloven §§ 27, 28 og 29 gir Datatilsynet hjemmel til henholdsvis å gi pålegg, fastsette tvangsmulkt og gi overtredelsesgebyr ved overtredelser av bestemmelser gitt i eller i medhold av loven.

Tilsvarende hjemler følger av helseregisterloven §§ 27, 28 og 29.

11.1.12 Sektor – forsyning og distribusjon av drikkevann

Mattilsynet gis i matloven § 23 myndighet til å fatte nødvendige vedtak for gjennomføring av bestemmelser gitt eller i medhold av loven. Tilsynet kan etter § 26 fastsette tvangsmulkt.

11.1.13 Sektor – digital infrastruktur – samtrafikkpunkter på internett (IXP)

Norges samtrafikkpunkter er som nevnt per i dag ikke gjenstand for ekomrettslig regulering eller krav til sikkerhet, og dermed heller ikke sanksjoner.

11.1.14 Sektor – digital infrastruktur – tilbydere av DNS-tjeneste

For å sikre at krav fastsatt i eller i medhold av ekomloven oppfylles kan Nasjonal kommunikasjonsmyndighet fastsette tvangsmulkt, jf. ekomloven § 10-7. Ved forsettlig eller uaktsom overtredelse av blant annet §§ 2-4 til 2-10, kan Nasjonal kommunikasjonsmyndighet pålegge overtredelsesgebyr.

11.1.15 Sektor – digital infrastruktur – registerenheter for toppdomener

Nasjonal kommunikasjonsmyndighet kan med hjemmel i domeneforskriften § 12 ilegge tvangsmulkt etter ekomloven § 10-7.

11.2 Direktivet

Art. 21 bestemmer at medlemsstatene skal fastsette regler om sanksjoner ved brudd på de forpliktelsene som følger av nasjonal lovgivning, som er vedtatt i henhold til direktivet. Sanksjonene skal være virkningsfulle, stå i et rimelig forhold til overtredelsen

og virke avskrekkende. Bestemmelsen skiller ikke mellom tilbydere av henholdsvis samfunnsviktige og digitale tjenester.

Bestemmelsen kommenteres ikke i fortalen til direktivet, men i en kommunikasjon fra EU-kommisjonen «Making the most of NIS».[42] Det uttales i kommunikasjonen vedlegg I punkt 3.7 at medlemsstatene i prinsippet står fritt til bestemme maksimalbeløp ved overtredelser, men at det bør være rom for en konkret vurdering av hver enkelt sak som grunnlag for å ilegge et passende gebyr. Det bør legges vekt på blant annet forholdets alvorlighetsgrad og om det er snakk om gjentakende overtredelser.

11.3 Departementets vurdering

Det er et betydelig nasjonalt handlingsrom når det gjelder utformingen av sanksjonsbestemmelsene. Det skal lovfestes sanksjonsmuligheter for myndighetene, men det er ikke et krav i direktivet at det settes et maksimumsbeløp.

Gjennomgangen av gjeldende rett viser at det er svært ulike regler i de ulike sektorene. Noen regelverk er dekkende for direktivets krav, noen er kanskje dekkende, mens andre igjen helt klart ikke er dekkende. Med dette som utgangspunkt foreslår departementet bestemmelser om sanksjonering som gjelder alle virksomhetene som omfattes av direktivet. Se nærmere lovutkastet § 15.

Sanksjonen er ment å ivareta både individual- og allmennpreventive hensyn. Mens bestemmelsene om pålegg og tvangsmulkt bare har som formål å bringe det ulovlige forholdet til opphør, vil et overtredelsesgebyr også ha som formål å hindre framtidige overtredelser. Etter departementets syn er det behov for å kunne reagere med overtredelsesgebyr både ved brudd på plikten til å sikre nettverk og informasjonssystemer, og ved brudd på plikten til å varsle om hendelser.

Sanksjonshjemmelen retter seg først og fremst mot den enkelte virksomhet som er pliktsubjekt etter loven. Departementet foreslår likevel å gi hjemmel for å ilegge fysiske personer overtredelsesgebyr da det ikke kan utelukkes at det er nødvendig i noen tilfeller. Det vil i så fall forutsette at den fysiske person har handlet uaktsomt eller forsettlig.

Departementet har vurdert, blant annet i lys av den tilsynelatende store effekten av at det i medhold av personvernforordningen kan gis relativt store bøter, om det også i denne loven bør kunne reageres med høye overtredelsesgebyrer ved overtredelse.

Det er ulike løsninger i forskjellige EU-land. I Storbritannia opereres det med maksimumsbeløp avhengig av forholdets alvorlighet. For de mest alvorlige

---

[42] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union, COM(2017) 476 final/2

overtredelsene kan det ilegges gebyr på opptil 17 millioner pund. I Sverige skal en sanksjonsavgift fastsettes til minst 5.000 og høyst 10.000.000 svenske kroner. I Danmark er det derimot ikke satt noen beløpsgrense, men kun hjemmel for å reagere med bøter ved overtredelse.

Departementet foreslår at sanksjonsbestemmelsen i loven ikke angir hvilken størrelse på gebyret som er aktuelt. Det kommer an på hva slags overtredelse det er snakk om, om det har skjedd over tid og om det er tale om gjentakende og gjenstridige handlinger. Det vil måtte bero på en konkret helhetsvurdering i hver enkelt sak hva som er et passende gebyr der også den aktuelle virksomhetens omsetning kan vektlegges. Det vil dessuten kunne variere over tid hva som er passende beløpsmessige rammer. Blant annet kan dette påvirkes av rettsutviklingen i EU. Departementet foreslår derfor at de beløpsmessige rammene fastsettes i forskrift.

12. ØKONOMISKE OG ADMINISTRATIVE KONSEKVENSER

12.1 Innledning

Departementet skal her gjøre et anslag over hvilke positive og negative konsekvenser det vil få for samfunnet, berørte virksomheter og berørte myndigheter, dersom lovutkastet blir vedtatt av Stortinget.

Det knytter seg en del usikkerhet til viktige elementer ved lovutkastet. Dette gjelder både positive og negative konsekvenser. Noe av hensikten med dette høringsnotatet er å få belyst lovutkastets mulige konsekvenser.

Hvilke virksomheter som blir omfattet av den foreslåtte loven danner et naturlig utgangspunkt for vurderingen av hvilke konsekvenser lovutkastet vil kunne få. Slik virkeområdet defineres er det de virksomhetene som er viktigst for å opprettholde et velfungerende samfunn som skal omfattes av lovutkastet. Hvor viktig en virksomhet må være for å bli omfattet beror på en skjønnsmessig vurdering. Som nevnt i kapittel 5.3 foreslår departementet å utarbeide mer konkrete vilkår for hvilke virksomheter som skal omfattes. Arbeidet er i gang, men vil ikke bli ferdigstilt innen dette høringsnotatet blir sendt ut. I påvente av dette arbeidet henviser departementet til arbeidet som er gjort av Myndigheten för samhällsskydd och beredskap. Listen gjelder svenske forhold og svenske virksomheter og dermed ikke brukes direkte på norske forhold. Departementet likevel at listen kan tjene som et foreløpig utgangspunkt for vurderingene av hvilke virksomheter som blir omfattet av det norske lovutkastet.

Med utgangspunkt i de virksomhetene som omfattes av lovutkastet, må det vurderes hvilke endringer kravene i lovutkastet vil føre til. Det som faktisk får konsekvenser er om de aktuelle virksomhetene, som følge av den nye loven, gjennomfører IKT-sikkerhetstiltak og varsler om IKT-sikkerhetshendelser, som de ikke gjør per i dag.

Inntil nå har drøftelsene i dette høringsnotatet i all hovedsak dreid seg om rent rettslige forhold og i mindre grad om faktiske forhold. Når økonomiske og administrative skal vurderes, må også de faktiske forholdene vurderes. Hvilke rettslige krav som gjelder vil imidlertid være et viktig moment i vurderingen. Samtidig er det klart at et rettslig krav om sikkerhet ikke nødvendigvis fører til god sikkerhet i en virksomhet. Motsatt betyr mangel på rettslige krav ikke nødvendigvis at det er dårlig sikkerhet i en virksomhet.

For virksomhetene er det etterlevelse av krav til sikkerhet og varsling som eventuelt vil være kostnadsdrivende. For myndighetene er det oppgaven med å føre tilsyn og å motta varsler som særlig vil være kostnadsdrivende. Slike konsekvenser gjennomgås sektorvis under.

12.2 Positive konsekvenser

Det er fastslått i en rekke dokumenter at det er behov for styrking av IKT-sikkerheten i Norge. Se blant annet Meld. St. 38 (2016-2017) IKT-sikkerhet og NOU 2015: 13 Digital sårbarhet. Gjennomføring av NIS-direktivet er etter departementets syn et viktig bidrag for å redusere digitale sårbarheter både i samfunnet og i den enkelte virksomhet. Gjennomføring av kravene i NIS-direktivet var for øvrig en av anbefalingene i NSM Sikkerhetsfaglige råd 2015.

Gjennom Mørketallsundersøkelsen 2016, foretatt av Næringslivets Sikkerhetsråd, er det innhentet fakta om IT-tilstanden i privat og offentlig næringsliv.[43] Hovedbudskapet er:

> Over en fjerdedel av norske virksomheter – 412 av 1500, eller 27% – har opplevd uønskede sikkerhetshendelser det siste året. Virksomhetene forteller at dette fører til produktivitetstap i 4 av 10 tilfeller (i form av tapte arbeidstimer), men kun 2 av 10 oppgir at de har hatt kostnader som følge av slike hendelser. Dette viser at virksomhetene mangler oversikt over hva sikkerhetshendelsene koster dem, eller undervurderer disse kostnadene. Kun 9% av virksomhetene som utsettes for angrep tar saken videre til politiet. Det tilsier at det skjuler seg betydelige mørketall, og for de kriminelle nettverk er denne typen angrep mot norske virksomheter i praksis straffefrie.

Kort sagt lever vi per i dag med for mye risiko når det gjelder IKT-sikkerhet. Da er det positivt at risikoen reduseres.

Tiltakende digitalisering av samfunnet anses som viktig for videre økonomisk vekst, i både Norge og Europa. IKT-sikkerhet er en avgjørende forutsetning for at digitaliseringen skal lykkes. Se for eksempel strategien *Digitale grep for norsk verdiskaping* fra Digital21 som nylig gjentok dette.[44] Departementet vil dessuten understreke at NIS-direktivet skal bidra til å fremme økonomisk vekst i EUs indre marked. Videre er hovedformålet med EØS-avtalen, som danner grunnlaget for

[43] https://www.nsr-org.no/moerketall/
[44] https://digital21.no/wp-content/uploads/2018/09/Digital21_strategi_2018.pdf

gjennomføring av direktivet for Norges del springer ut av EØS-avtalen, nettopp å stimulere til økonomisk vekst i hele EØS.

De viktigste tiltakene for å styrke IKT-sikkerheten som omhandles i dette høringsnotatet, retter seg først og fremst mot virksomheter som er viktige for at Norge skal kunne være et velfungerende samfunn. Dersom en slik virksomhet stanser eller vesentlig reduserer sine normale leveranser, har det konsekvenser for andre deler av samfunnet, som igjen får problemer med å gjennomføre sine leveranser.

Det første tiltaket er grunnsikring av den enkelte virksomhet. Det handler om forebyggende sikkerhetstiltak som gjør en virksomhet bedre rustet til å stå i mot angrep mot nettverk og informasjonssystemer de er avhengige av. Det andre tiltaket handler om å ha planer for håndtering av uønskede hendelser. For eksempel må en ha evne til å oppdage uregelmessigheter, og det skal iverksettes sikkerhetslogging. Det tredje tiltaket er varsling av hendelser til myndighetene.

Bedre IKT-sikkerhet har flere positive sider. For det første er det her snakk om å styrke sikkerheten knyttet til viktig infrastruktur i landet. For det andre har god grunnsikring har kriminalitetsforebyggende effekt, både for den enkelte virksomhet og for samfunnet. Norge som nasjon kan dessuten bli et mindre attraktivt sted å drive kriminell aktivitet.

For det tredje vil god IKT-sikkerhet kunne være et konkurransefortrinn. I en direkte konkurranse kan virksomheten for eksempel tilby sikker drift eller god sikring av informasjon en tar vare på på vegne av andre. Også globalt vil god IKT-sikkerhet i EØS som region kunne være en driver for å tiltrekke seg investorer.

Som nevnt i punkt 8.3 er noe av formålet med varslingskravene at myndighetene skal få bedre kunnskapsgrunnlag for å kunne forbedre arbeidet med IKT-sikkerhet. Dette vil etter hvert komme virksomheter, myndigheter og hele samfunnet til gode.

Det er viktig for norsk næringsliv og verdiskaping at direktivet også gjelder for Norge. For eksempel omfatter direktivet skytjenester. Fra norsk ståsted er det viktig at alle skytjenester innenfor EØS-området tilfredsstiller krav fra EU mht. både informasjonssikkerhet og personvern. Dette gjelder både for de norske virksomhetene som benytter skytjenester innenfor EØS-området, men det er også viktig dersom vi ønsker etablering av store, internasjonale datasentre i Norge. Det at Norge er omfattet av NIS-direktivet (og Personvernforordningen) vil være med på å redusere usikkerhet knyttet til Norge som vertsnasjon.

I tillegg til konkurransehensyn er det også av rent sikkerhetsmessige hensyn et viktig moment at Norge, i EØS-sammenheng, og at den enkelte virksomhet, i nasjonal sammenheng, faktisk gjennomfører kravene i NIS-direktivet. Angripere vil naturlig gå etter de svakeste leddene først. Når begrunnelsen for kravene delvis ligger i at alt henger sammen med alt, er det særlig viktig at alle følger opp kravene. Heri ligger også grunnen til at EU-kommisjonen kommer til å følge opp medlemslandenes etterlevelse av

direktivet, og til at det må innføres krav ved lov og at myndighetene skal føre tilsyn og får sanksjonshjemler.

NIS-direktivet utgjør en viktig brikke i realiseringen av EUs planer om et digitalt indre marked. Hvis befolkningen ikke har tillitt til de digitale tjenestene, så blir de ikke brukt. Et for lavt sikkerhetsnivå på de digitale tjenestene vil sette en effektiv stopper for den videre digitaliseringen.

12.3 Kostnader

Etter departementets syn får ikke lovutkastet nevneverdige negative konsekvenser for samfunnet som sådan. Det vil heller kunne ha en negativ effekt dersom vi velger å ikke gjennomføre dette risikoreduserende tiltaket.

For berørte virksomheter vil etterlevelse av kravene om sikkerhet og varsling kunne innebære økte kostnader. For berørte myndigheter vil lovutkastet innebære økte kostnader til gjennomføring av tilsyn og håndtering av varsler.

I forbindelse med utarbeidelse av EU-kommisjonens forslag til NIS-direktiv, gjorde Kommisjonsstaben noen beregninger av kostnader knyttet til innføring av direktivet. Selv om dette ble gjort for noen år tilbake, og at det endelige direktivet er endret noe sammenlignet med forslaget, mener departementet at beregningene kan gi en pekepinn på kostnadsnivået. Oppsummeringsvis legger Kommisjonsstaben i SWD (2013) 32 til grunn følgende kostnadsbilde for innføringen:[45]

- Sikkerhetskostnadene er beregnet til å måtte utgjøre 6,61% av en virksomhets totale IKT-budsjett
- Totalt for alle berørte virksomheter i EU, vil etterfølgelse av direktivet medføre kostnader på til sammen mellom 1 og 2 millarder euro.
- I snitt medfører direktivet økte kostnader for små og mellomstore bedrifter (10-250 ansatte) med mellom 2500 og 5000 euro.
- For energisektoren medfører direktivet ingen økte kostnader, da det antas at tilstrekkelig IKT-sikkerhet er på plass.
- Berørte virksomheter i transportsektoren må øke sin totale IKT-sikkerhetssatsing med 3 prosentpoeng
- I finanssektoren må man øke med 1,2 prosentpoeng
- I helsesektoren må man øke med 2,3 prosentpoeng
- I IKT-sektoren må man øke med 0,7 prosentpoeng
- Rapporteringskostnadene beregnes til 212 500 euro samlet for alle berørte virksomheter i EU.

Nærmere om negative konsekvenser for virksomheter som omfattes av lovutkastet følger under.

---

[45] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2013:0032:FIN:EN:PDF

Når det gjelder inndekning av økte kostnader mener departementet at kravene som følger av lovutkastet ikke er mer tyngende enn det som naturlig følger med samfunnsutviklingen. Digitaliseringen bidrar til effektivisering og økonomisk vekst. For å kunne ta del i dette er det nødvendig å investere i IKT-sikkerhet. Dette gjelder for både private og offentlige virksomheter. Private virksomheter som har en samfunnsmessig viktig rolle, har et selvstendig ansvar for å kunne levere sine tjenester. Lovutkastet krever ikke et spesielt høyt sikkerhetsnivå, men en grunnsikring. Gjennomføring av tiltak for å styrke IKT-sikkerheten vil ikke bare gagne samfunnet, men også den enkelte virksomhet.

Som nevnt over vil de fleste virksomhetene som omfattes av direktivet også være omfattet av personopplysningsloven. Departementet mener det ikke vil medføre særlige ekstra kostnader å sikre informasjonssystemer i henhold til lovutkastet, dersom systemet allerede er sikret i henhold til personopplysningsloven.

Offentlige myndigheter må som utgangspunkt kunne finne inndekning for merarbeidet som følger av lovutkastet innenfor gjeldende budsjettrammer. Skulle det ikke være tilstrekkelig vil det være opp til den enkelte sektor å finne tilstrekkelige midler enten gjennom omprioritering eller tilførsel av friske midler, som må behandles som en del av den ordinære budsjettprosessen.

Det er tidligere drøftet om gjeldende regelverk inneholder krav også til IKT-sikkerhet. Etter departementets syn er den mest naturlige tolkningen at konsekvenser av samfunnsutviklingen må tas inn i kravet om risikovurdering. En risikovurdering som foretas i 2018 eller senere og ikke inneholder vurderinger av digitale elementer, kan vanskelig sies å være fullstendig.

12.3.1 Sektor – energi – elektrisitet

Om lag 190 nettselskaper og viktige kraftprodusenter vil kunne bli omfattet av direktivet, jf. direktivet vedlegg II. Kraftprodusentene må eie produksjonsanlegg på minst 50 MVA, det vil si at selskapet som eier kun småkraftverk ikke er med.

I tillegg vil ca. 140 rene kraftleverandører kunne omfattes. For denne kategorien er det klart at kun noen få oppfyller alle tre kriteriene for hva som skal anses som tilbyder av en samfunnsviktig tjeneste, jf. lovutkastet § 4 første ledd nr. 1.

Videre vil markedsplasser for omsetning av elektrisk energi for fysisk levering, kunne omfattes av loven, men detaljene knyttet til å regulere kravene som følger av NIS-direktivet er ikke endelig fastsatt.

Som det fremgår av kapittel 7.3 og 8.3, medfører lovutkastet ikke ytterligere sikkerhetskrav sammenlignet med gjeldende rett, forutsatt at de foreslåtte endringene av beredskapsforskriften vedtas.

Ettersom gjeldende sikkerhets- og varslingskrav er dekkende for kravene som blir stilt i lovutkastet, vil dette heller ikke få negative konsekvenser for tilsynsmyndigheten i sektoren.

For elektrisitetssektoren vil lovutkastet ikke medføre negative konsekvenser.

12.3.2 Sektor – energi – olje

Oljeproduksjon

Sikkerhetskravene som følger av petroleumsloven og tilhørende forskrifter, er ganske annerledes utformet enn kravene som følger av lovutkastet. Det er i stor grad opp til virksomhetene å iverksette tilstrekkelig tiltak for å oppnå god sikkerhet. Ordlyden i gjeldende regelverk er så generell at IKT-sikkerhet gjerne kan innfortolkes. Det vil bero på virksomhetenes praksis om kravene som følger av lovutkastet innebærer kostnader for virksomhetene i denne sektoren.

Det kan i denne forbindelse nevnes at Statoil spilte inn, i forbindelse med høringen av direktivet sommeren 2016, at «Statoils styringssystem på informasjonssikring allerede [er] nært knyttet til internasjonale standarder».

Det er vanskelig å se for seg at virksomheter som driver produksjon av olje og gass på norsk sokkel vil kunne defineres som tilbydere av samfunnsviktige tjenester. Dette sammenholdt med lovens geografiske virkeområde medfører at departementer antar at lovutkastet vil få begrenset betydning for norsk oppstrøms olje- og gassproduksjon.

Drivstofforsyning
Innenfor drivstofforsyningen er noen tankanlegg utpekt som skjermingsverdige objekter etter sikkerhetsloven. Som gjennomgått tidligere vil sikkerhetslovens krav langt på vei dekke kravene i lovutkastet.

Når kravene i sikkerhetsloven etterleves er det etablert gode rutiner for sikkerhetsstyring og varsling i virksomheten. Departementet antar at etterlevelse av lovutkastets krav da ikke vil utgjøre stor kostnadsforskjell.

Det er imidlertid usikkert hvilke økonomiske og administrative konsekvenser direktivet vil få for drivstoffnæringen. Dette skyldes blant annet at noen deler av IKT-infrastrukturen kan være underlagt sikkerhetslovens krav, mens andre deler kan bli underlagt NIS-direktivet. En virksomhet kan derfor potensielt bli omfattet av begge regelverk. Både gjeldende og ny sikkerhetslov har strengere krav til sikring og varsling enn den foreslåtte IKT-sikkerhetsloven. Dette kan medføre at noen flere informasjonssystemer vil måtte sikres og at noen flere hendelser vil måtte varsles. Videre

har ikke departementet tilstrekkelig kunnskap om i hvilken grad drivstoffnæringen har etablert formaliserte rutiner for risikostyring i samsvar med lovutkastet.

For øvrige virksomheter som per i dag ikke er underlagt noen krav om sikkerhet og varsling, viser departementet til anslag som ble gjort i forbindelse med utarbeidelse av forslaget til NIS-direktivet, se innledningen til punkt 12.3.

12.3.3 Sektor – energi – gass

To virksomheter er både forsyningsforetak og operatører av distribusjonsnett, jf. direktivet vedlegg II, og faller dermed innenfor lovens virkeområde. Virksomheter som selger gass til disse kan også defineres som forsyningsforetak. Det er departementets foreløpige vurdering at disse virksomhetene ikke oppfyller kriteriene for *samfunnsviktig tjeneste.*

Virksomhetene er underlagt naturgassloven og er, som nevnt i kapittel 7.3 og 8.3, ikke underlagt krav om IKT-sikkerhet og varsling. For øvrig viser departementet til kostnadsoverslagene som er nevnt i innledningen til punkt 12.3.

12.3.4 Sektor – transport – luft

Lufthavner, luftfartsselskaper og flysikringstjenesten omfattes av NIS-direktivet vedlegg II. På generelt grunnlag legger departementet til grunn at det i første rekke er de større aktørene i sektoren som kan bli definert som *tilbydere av samfunnsviktige tjenester.* I tillegg kan enkelte vedlikeholdsvirksomheter bli omfattet.

I den grad mindre virksomheter i sektoren blir omfattet av lovutkastet, er det grunn til å anta at konsekvensene kan bli større for de mindre virksomhetene enn for de større. Sistnevnte vil mest sannsynlig ha sikkerhetstiltak på plass i større grad enn små virksomheter, gjerne drevet frem av kommersielle hensyn. Ifølge Luftfartstilsynet har alle større aktører etablert egne interne rutiner for å ivareta IKT-sikkerhet, siden dette i stor grad er knyttet til sikring av egen drift og å unngå driftsavbrudd.

Sikkerhetskravene som stilles til virksomheter innen flysikringstjenesten inneholder viktige elementer som risikovurdering og gjennomføring av risikoreduserende tiltak. Dette innebærer antakelig at etterlevelse av sikkerhetskravene i loven ikke vil medføre store merkostnader.

På grunn av det pågående regelverksarbeidet i regi av EASA, som ble nevnt i punkt 7.1.5, er det grunn til å tro at NIS-direktivet på sikt vil få liten betydning for luftfarten.

I den grad ICAO-standarden som ble nevnt i punkt 7.1.5 følges av virksomheter i sektoren, vil det antakelig ikke for dem medføre særlige merkostnader å etterleve lovutkastets sikkerhetskrav.

Luftfartstilsynet har gjennom revisjoner med fokus på ATM (Air Traffic Management) security og objektsikkerhet, hatt fokus på flysikringsområdet over flere år, og sertifiserte tjenesteytere har fulgt opp med relevante tiltak.

Departementet anslår på denne bakgrunn for det første at det er de større aktørene som i første rekke vil bli omfattet av lovutkastet, og for det andre at merkostnadene vil være begrenset i og med at det allerede er etablert rutiner for IKT-sikkerhet.

Luftfartstilsynet selv forventes å måtte føre tilsyn med utvalgte tjenesteleverandører innen luftfartssektoren iht. direktivet når dette er innført. Ytterligere behov for avklaring av sikkerhetstilstanden vedrørende IKT i luftfartssektoren forventes å påføre Luftfartstilsynet merarbeid. Disse oppgavene antas å kunne medføre økonomiske og administrative konsekvenser som per i dag ikke er nøyaktig beregnet.

12.3.5 Sektor – transport – jernbane

Aktuelle norske virksomheter er Bane NOR AS, 4 jernbaneforetak som driver persontransport, 6 jernbaneforetak som driver godstransport, og de som driver serviceanlegg, jf. jernbaneforskriften § 1-3 bokstav g. Alle virksomhetene er omfattet av jernbaneloven, sikringsforskriften og sikkerhetsstyringsforskriften. En foreløpig vurdering er at Bane NOR AS, 2 persontransportforetak og 2 godtransportforetak blir omfattet av lovutkastet.

Ettersom jernbanevirksomhetene i henhold til gjeldende regelverk er sikret mot tilsiktede hendelser, mener departementet at merkostnadene ved å etterleve kravene i lovutkastet blir små.

Videre vil lovutkastet kunne medføre noen kostnader knyttet til varsling. Siden varslingssystem er på plass vil det antakelig ikke være snakk om store merkostnader. Terskelen for å varsle om hendelser etter lovutkastet er relativt høy, og det er grunn til å tro at slike hendelser ville blitt varslet også etter dagens system.

Sett i sammenheng med kravene som følger av sikkerhetsstyringsforskfiten, legger departementet til grunn at lovutkastet ikke får særlig store økonomiske og administrative konsekvenser for de aktuelle jernbanevirksomhetene.

Jernbanetilsynet fører tilsyn med etterlevelse av både sikringsforskriften og sikkerhetsstyringsforskriften, jf. jernbaneloven § 11. Det vil kunne påløpe noen kostnader for tilsynet i tilknytning til samarbeid med andre myndigheter på dette området.

12.3.6 Sektor – transport – vann

Havneanlegg og havner

Aktuelle virksomheter er rederier, havner og havneanlegg, foretak som driver anlegg og utstyr i havn, og operatører av sjøtrafikksentraler. Her som på andre områder er det i første rekke de største aktørene som med størst sannsynlighet vil bli omfattet av lovutkastet.

I den grad gjeldende krav i sektoren omfatter IKT-sikkerhet, noe en naturlig tolkning åpner for, vil kravene etter lovutkastet ikke medføre sikringskostnader av betydning. Slik sikkerhetskravene er utformet dekker de lovutkastets sikkerhetskrav.

Gjeldende varslingsregler vil antakelig også gjelde den type alvorlige IKT-hendelser som skal varsles etter lovutkastet.

Kystverket fører tilsyn med havner og havneanlegg i henhold til deres oppfyllelse av sikringsregelverkene (ISPS-regelverket). I den utstrekning enhetens IKT-systemer er beskyttet under gjeldende regelverk vil dette omfattes av tilsynet. Per i dag har det funnet sted et begrenset antall IKT-hendelser som faller inn under ISPS-regelverket. Tilsynet etter ISPS-regelverket er risikobasert, noe som innebærer at omfanget av slikt tilsyn vil øke dersom risikoen for IKT-hendelser øker. En slik situasjon vil kunne medføre økte økonomiske og administrative kostnader for etaten.

Departementet antar på denne bakgrunn at det blir små økonomiske og administrative konsekvenser for virksomheter i denne sektoren.

Skipsfart
Det er rederiene selv og ikke det enkelte skip som skal omfattes av lovutkastet. Det er foreløpig ikke tatt noen nærmere vurdering av hvilke eller hvor mange rederier som vil kunne bli omfattet av lovutkastet.

Kravene i lovutkastet er på flere områder sammenlignbare med kravene i ISM-koden. I den grad ISM-koden gjelder også for rederiene, og ikke bare sikkerheten på det enkelte fartøy, legger departementet til grunn at det ikke knytter seg særlige merkostnader til sikkkerhetskravet som følger av lovutkastet for denne sektoren.

I alle tilfeller er det etter skipssikkerhetsloven § 7 krav om rederiene skal ha et sikkerhetsstyringssystem. Når det gjelder kvalitetskrav er det per i dag ikke særskilte krav til IKT-vurderinger, men det er fastsatt retningslinjer for oppfølging av «cyber security» som skal være tatt hensyn til i rederienes sikkerhetsstyringssystemer, som nevnt senest inne første årlige revisjon etter 1. januar 2021.

Når det gjelder varsling vil det knytte seg noen kostnader til å etablere en varslingslinje fra rederiene til myndighetene.

Sjøfartsdirektoratet fører tilsyn med rederienes sikkerhetsstyringssystem. Departementet antar dermed at lovutkastets krav om tilsyn ikke vil medføre særlige merkostnader.

12.3.7 Sektor – transport – vei

Statens vegvesen blir antakelig omfattet av lovutkastet.

Som nevnt over stilles det ikke sikkerhetskrav i gjeldende lov eller forskrift. Imidlertid er slike krav regulert av interne retningslinjer for sikkerhet, drift og forvaltning av automasjonsnettet og SCADA-systemet, og sikkerheten er håndtert internt av Statens vegvesen.

Etablering av varslingsrutiner vil ikke medføre betydelig kostnader for denne sektoren.

Det føres per i dag ikke tilsyn med Statens vegvesen. Det vil bli vurdert om Statens vegtilsyn skal pålegges oppgavene som følger av lovutkastet.

Departementets vurdering er foreløpig at etterlevelse av kravene i lovutkastet ikke vil medføre særlige merkostnader for sektoren.

12.3.8 Sektor – bank

Departementets vurdering er foreløpig at banksektorens gjeldende regelverk fullt ut dekker lovutkastets krav. For denne sektoren innebærer dermed lovutkastet ingen økonomiske og administrative kostnader.

Når det gjelder varsling så mangler dagens regelverk krav om at varselet skal inneholde nok opplysninger til at det kan fastslås om hendelsen har virkninger utover Norges grenser. Det vil kunne medføre noen kostnader å justere varslingsrutinene slik at dette blir mulig. Foreløpig ligger det likevel an til at dette blir justert gjennom endringer i rundskriv 15/2009: Rapportering av IKT-hendelser til Kredittilsynet. Dermed er det ikke det vedlagte lovutkastet som vil medføre merkostnader.

Kostnader for Finanstilsynet omtales samlet i punkt 12.3.9.

12.3.9 Sektor – finansmarkedsinfrastruktur

Gjeldende regelverk for finansmarkedsinfrastruktur dekker fullt ut lovutkastets krav når det gjelder sikring. Når det gjelder varsling så er situasjonen den samme som for banksektoren.

Kostnader for Finanstilsynet er vurdert samlet for sektorene bank og finansmarkedsinfrastruktur.

For Finanstilsynet vil lovutkastet innebære krav om å rapportere hendelser til myndigheter i andre land. Dette vil antakelig medføre noe merarbeid.

Videre blir det behov for mer samarbeid med en CSIRT. Dette kan også medføre noe merarbeid, men antakelig i mindre grad. Det samme gjelder samarbeid med Datatilsynet, som også antakelig må økes.

Samlet sett legges det til grunn at lovutkastet vil medføre kostnader for Finanstilsynet i form av 0,25 årsverk.

12.3.10 Sektor – helsetjenester

Det er om lag 17000 virksomheter som faller inn under definisjonen av tilbydere av helsetjenester. Foreløpig anslås 40 til 50 av de største virksomhetene å skulle etterleve kravene i lovutkastet. Direktoratet for e-helse, Helsedirektoratet, Folkehelseinstituttet, Statens legemiddelverk, Mattilsynet, Statens strålevern, Norsk Helsenett SF, HF / RHF, RHFenes IKT-selskaper, Private leverandører (IKT, laboratorium, etc) er eksempler på større virksomheter som vil kunne bli omfattet.

Kravene som følger av direktivet er i stor grad oppfylt i helse- og omsorgssektoren allerede, blant annet gjennom krav i sektorregelverk og i Normen. Det vurderes derfor at konsekvensene ved innføring av direktivet vil kunne være relativt begrenset, selv om ulike tiltak innenfor informasjonssikkerhetsområdet samlet vil kunne føre til økte ressurs- og kompetansebehov.

Tradisjonelt har det vært høyt fokus på konfidensialitet innen helse- og omsorgssektoren. I arbeidet med informasjonssikkerhet og pasientsikkerhet kan innføring av direktivet være med på å gi bedre balanse og forståelse for problemstillingene rundt informasjonssikkerhet. Det er positivt at tilgjengelighet i større grad kan bli rettslig regulert.

Hvis HelseCERT får en formell rolle opp mot direktivet som CSIRT og kontaktpunkt for varsling, vil dette bety en formalisering av rollen HelseCERT har i dag, og HelseCERT vil trolig måtte tilføres noe ressurser for å ivareta noe økt varsling.

12.3.11 Sektor – forsyning og distribusjon av drikkevann

Sammenlignet med Sverige, som har satt grensen på 20000 personer, bør det vurderes å sette den noe lavere i Norge, da vi har flere mindre byer og tettsteder. En grense på 10000 personer kan være mer passende for norske forhold. Det innebærer at om lag 150 vannforsyningssystemer blir omfattet av lovutkastet. Vannforsyningssystemer som leverer vann til sykehus og andre viktige virksomheter bør vurderes særskilt.

Sikkerhetskravene som følger av gjeldende regelverk dekker fullt ut lovutkastets krav. Lovutkastet vil dermed ikke medføre økte kostnader for de aktuelle virksomhetene.

Når det gjelder varsling er det imidlertid forskjeller mellom gjeldende og foreslått regelverk. Ettersom det er et varslingssystem mellom virksomhetene i

drikkevannssektoren og relevante sektormyndigheter, er det likevel grunn til å tro at det ikke er snakk om store merkostnader knyttet til de nye kravene.

Dette medfører videre at lovutkastet ikke medfører økte kostnader for Mattilsynet.

12.3.12 Sektor – digital infrastruktur – samtrafikkpunkter på internett (IXP)

Det er 6 IXPer i Norge, og alle disse blir antakelig omfattet av lovutkastet.
Selv om det ikke stilles krav til sikring i gjeldende regelverk, vil lovutkastet medføre kun begrensede kostnader for IXPene. Det er iverksatt en rekke sikkerhetstiltak som skal sørge for at tjenestene kan leveres til enhver tid. UiO har dessuten et eget hendelsesresponsteam som samarbeider med blant andre UNINETT CERT og NSM NorCERT.

Justering av varslingsrutiner kan medføre noen ekstra kostnader.

Nasjonal kommunikasjonsmyndighet, som er aktuell som tilsynsmyndighet, vil få noe økning i sine økonomiske og administrative kostnader.

12.3.13 Sektor – digital infrastruktur – tilbydere av DNS-tjeneste

Tilbydere av DNS-tjenester består av ordinære tilbydere av internett og virksomheter som har registraravtaler med Uninett Norid AS. Antakelig vil det være kun en håndfull virksomheter som må oppfylle sikkerhets- og varslingskravene i lovutkastet.

Virksomheter som er underlagt ekomregelverk, vil ikke få særlige merkostnader knyttet til lovutkastet.

Når det gjelder registrarene har Norid flere krav knyttet til stabilitet og drift i registraravtalene. Etterlevelse av lovutkastets krav vil antakelig likevel medføre økte kostnader for de aktuelle registrarene. At noe sikkerhet allerede er på plass kan tilsi at det ikke er tale om stor økning.

Nasjonal kommunikasjonsmyndighet, som er aktuell som tilsynsmyndighet, vil få noe økning i sine økonomiske og administrative kostnader.

12.3.14 Sektor – digital infrastruktur – registerenheter for toppdomener

Uninett Norid AS er aktuell til å bli omfattet av direktivet.

Gjeldende regelverk har ikke sikkerhetskrav. Det kan likevel legges til grunn at det er god sikkerhet i virksomheten og at etterlevelse av lovutkastets krav vil få begrensede økonomiske eller administrative konsekvenser.

Etablering av nye varslingsrutiner vil antakelig medføre økte kostnader.

12.3.15 Tilbydere av digitale tjenester

Direktivets definisjon av tilbydere av digitale tjenester gjør det utfordrende å komme med klare antakelser om hvor mange virksomheter som blir omfattet av det norske lovutkastet. Blant annet stemmer ikke næringskoder som det føres statistikk utifra overens med direktivets definisjon.

I Sverige har Myndigheten för samhällsskydd och beredskap (MSB) utredet spørsmålet.[46] Konklusjonen er, med flere forbehold, at det er 15 tilbydere av nettbaserte markedsplasser (hvorav flere innen finansbransen), 5 tilbydere av nettbaserte søkemotorer, og 70 tilbydere av skytjenester.

Ifølge konskvensanalysen som er gjort i Storbritannia, antas det at 3 tilbydere av nettbaserte markedsplasser, ingen tilbydere av nettbaserte søkemotorer og 169 tilbydere av skytjenester blir omfattet av de nye engelske forskriftene. [47]

Som nevnt tidligere skal tilbydere av digitale tjenester underlegges et mindre strengt sikkerhetsregime enn tilbydere av samfunnsviktige tjenester. Terskelen for hva som er et forsvarlig sikkerhetsnivå er dermed noe lavere for denne kategorien virksomheter.

For denne kategorien virksomheter er det nok særlig aktuelt å se kravene som følger av lovutkastet i sammenheng med kravene som følger av personopplysningsloven. Departementet legger til grunn at virksomheter som har sikret sine informasjonssystemer i tråd med personopplysninger, også som utgangspunkt etterlever lovutkastets krav. Departementet antar at langt de fleste virksomhetene i denne kategorien har informasjonssystemer som skal sikres etter både personopplysningsoven og det vedlagte lovutkastet. Da vil ikke sistnevnte krav medføre nevneverdige merkostnader.

Varslingskravene etter NIS-direktivet er ikke like som etter personopplysningsloven. Dette vil antakelig medføre noe økte kostnader for virksomhetene. Samtidig er det ikke grunn til å tro at det er mange hendelser som skal varsles. Konsekvensanalysen i Storbritannia konkluderer med at det i høyden er tale om 1348 varsler per år, basert på en undersøkelse blant aktuelle virksomheter. Basert på tall fra NCSC (National Cyber

---

[46] Redovisning av vissa vidtagna åtgärder för att förbereda genomförandet av NIS-direktivet, 12.01.2018, Deluppdrag B, https://www.msb.se/Upload/Nyheter_press/Pressmeddelanden/MSB%20Regeringsuppdrag%20F%c3%b6rbereda%20inf%c3%b6rande%20av%20NIS%20180115%20.pdf

[47] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/701054/Network_Information_Systems_Directive_Final_Impact_Assessment.pdf

Security Center) er det i løpet av ett år blitt registrert 39 hendelser av en slik alvorlighetsgrad at de skal varsles etter direktivet.[48]

De fleste virksomhetene vil som følge av kravene etter personopplysningsloven, allerede ha et system for varsling. Skal en hendelse varsles etter personopplysningsloven, vil det ikke knytte seg særlige merkostnader til det å skulle varsle også etter direktivet. Samlet antar departementet at varslingskostnadene vil være moderate.

VEDLEGG 1: UTKAST TIL LOV

VEDLEGG 2: NIS-DIREKTIVET

VEDLEGG 3: UOFFISIELL OVERSETTELSE AV NIS-DIREKTIVET

---

48 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/701054/Network_Information_Systems_Directive_Final_Impact_Assessment.pdf