JD

JUSTIS- OG BEREDSKAPSDEPARTEMENTET

Høringsnotat

Samfunnssikkerhetsavdelingen
Dato: 11. september 2024
Saksnr: 24/3567
Høringsfrist: 11. desember 2024

Forslag til forskrift til digitalsikkerhetsloven (digitalsikkerhetsforskriften)

Innhold

1 Innledning ... 3
2 NIS1-direktivet ... 4
3 NIS2-direktivet ... 5
4 Lovens virkeområde ... 6
4.1 Gjeldende rett ... 6
4.2 Departementets vurderinger og forslag ... 7
4.2.1 Lovens geografiske virkeområde ... 7
4.2.2 Virkeområde for tilbydere av samfunnsviktige tjenester ... 7
4.2.3 Utpeking av virksomheter som tilbyr samfunnsviktige tjenester ... 13
4.2.4 Innmelding av samfunnsviktige tjenester ... 13
4.2.5 Unntak for små virksomheter ... 14
5 Krav til sikkerhet for samfunnsviktige tjenester ... 15
5.1 Gjeldende rett ... 15
5.2 NIS1-direktivet ... 15
5.3 Departementets vurderinger og forslag ... 16
5.3.1 Innledning ... 16
5.3.2 Krav til styringssystem for sikkerhet ... 16
5.3.3 Risikovurdering ... 17
5.3.4 Risikohåndtering ... 19
5.3.5 Sikkerhetstiltak ... 20
5.3.6 Hendelseshåndtering og beredskap ... 23
5.3.7 Oppfølgingsplikt ... 24
6 Krav til sikkerhet for tilbydere av digitale tjenester ... 25
6.1 Gjeldende rett ... 25
6.2 Gjennomføringsforordningen ... 25

6.3 Departementets vurderinger og forslag 26
7 Responsmiljøer 27
7.1 Gjeldende rett 27
7.2 Departementets vurderinger og forslag 27
8 Varsling om hendelser 28
8.1 Gjeldende rett 28
8.2 Direktivet og gjennomføringsforordningen 28
8.3 Varslingskrav i Sverige 29
8.4 Varslingsreglene i NIS2-direktivet 30
8.5 Departementets vurderinger og forslag 30
9 Tilsyn 32
9.1 Gjeldende rett 32
9.2 NIS1-direktivet 32
9.3 Departementets vurderinger og forslag 33
9.3.1 Tilsyn, opplysningsplikt og tilgang til lokaler 33
9.3.2 Særlig om deling av taushetsbelagt informasjon 34
10 Nasjonalt kontaktpunkt for sikkerhet i nettverk og informasjonssystemer 34
10.1 Gjeldende rett og direktivet 34
10.2 Departementets vurderinger og forslag 34
11 Behandling av personopplysninger 35
11.1 Gjeldende rett og NIS1-direktivet 35
11.2 Departementets vurderinger og forslag 35
12 Overtredelsesgebyr 36
12.1 Gjeldende rett 36
12.2 NIS1-direktivet 37
12.3 Departementets vurderinger og forslag 37
13 Økonomiske og administrative konsekvenser 40
Forslag til forskrift til digitalsikkerhetsloven (digitalsikkerhetsforskriften) 42

1 Innledning

Justis- og beredskapsdepartementet sender med dette på høring forslag til forskrift om digital sikkerhet (digitalsikkerhetsforskriften). Forskriftsforslaget er foreslått hjemlet i lov 20. desember 2023 nr. 108 om digital sikkerhet (digitalsikkerhetsloven), som ble vedtatt av Stortinget 12. desember 2023. I Prop. 109 LS (2022–2023) er det forutsatt at loven suppleres med forskrift. Når forskriften blir vedtatt, kan også loven settes i kraft.

Digitalsikkerhetsloven vil, sammen med forslaget til forskrift om digital sikkerhet, gjennomføre NIS1-direktivet (EU) 2016/1148 av 6. juli 2016 og gjennomføringsforordning (EU) 2018/151 av 30. januar 2018 i norsk rett.

Formålet med digitalsikkerhetsloven er å bidra til å sikre grunnleggende krav til digital sikkerhet i virksomheter med særlig betydning for samfunnet ved å forebygge, avdekke og motvirke uønskede hendelser i nettverk og informasjonssystemer som brukes for å levere samfunnsviktige tjenester og digitale tjenester. Loven stiller overordnede krav til digital sikkerhet og varsling ved hendelser som virker betydelig inn på tjenesteleveransen, og angir virkeområdet i form av hvilke sektorer den gjelder for. Loven gjelder tilbydere av samfunnsviktige tjenester og tilbydere av digitale tjenester slik disse er definert i digitalsikkerhetsloven §§ 6 og 9.

Forslag til forskrift om digital sikkerhet presiserer virkeområdet for tilbydere av samfunnsviktige tjenester, og det foreslås at det i særlige tilfeller kan fattes enkeltvedtak om at loven også skal gjelde andre tilbydere av samfunnsviktige tjenester. Det legges opp til at slik utpeking i så fall kan gjøres av sektormyndigheten. Tilbyder av samfunnsviktig tjeneste pålegges en plikt til å melde inn til tilsynsmyndigheten kontaktinformasjon, tjeneste og samfunnssektor, hvilke andre land tjenesten tilbys fra og berørt geografisk område, samt endringer i det nevnte. Se nærmere om dette i punkt 4.

Det foreslås å forskriftsfeste at tilbyder av samfunnsviktig tjeneste skal etablere og vedlikeholde et styringssystem for digital sikkerhet, som beskriver virksomhetens sikkerhetsarbeid, og at dette skal være en del av virksomhetens styringssystem. Styringssystemet for digital sikkerhet vil omfatte både digitale, fysiske og personelle sikkerhetstiltak. Risikostyring skal inngå som en del av styringssystemet og skal sikre at virksomheten oppfyller lovpålagte krav. Styringssystemet skal dokumenteres og jevnlig kontrolleres med sikte på revisjon. Virksomhetens leder har det overordnede ansvaret. Videre foreslås det at styringssystemet skal gjøres kjent for virksomhetens ansatte og underleverandører, og at leverandører og andre som utfører arbeid for eller på vegne av virksomheten skal følges opp med at sikkerhetskravene etterleves. Krav til sikkerhet for samfunnsviktige tjenester er omtalt i punkt 5.

Krav til tilbydere av digitale tjenester er gitt i Kommisjonens gjennomføringsforordning (EU) 2018/151 av 30. januar 2018 om fastsettelse av regler for anvendelse av europaparlaments- og rådsdirektiv (EU) 2016/1148. Forordningen gir ytterligere spesifisering av de elementene som tilbydere av digitale tjenester skal ta hensyn til for å håndtere risikoene knyttet til sikkerheten i nettverk og informasjonssystemer, og av kriteriene for å avgjøre om en hendelse har en betydelig innvirkning. Det foreslås at denne gjelder som forskrift. Tilbydere av digitale tjenester som er små og mellomstore virksomheter foreslås unntatt fra

krav til sikkerhet og varsling, se punkt 4.2.5. Krav til sikkerhet for tilbydere av digitale tjenester behandles i punkt 6.

For tilbydere av samfunnsviktige tjenester og tilbydere av digitale tjenester foreslås det en varslingsplikt innen 24 timer etter at tilbyder fikk kjennskap til hendelsen. Forslaget oppstiller krav til varselets innhold og at informasjonen skal oppdateres innen 72 timer. Tilbyder av samfunnsviktig tjeneste skal innen en måned følge opp med en hendelsesrapport. Se nærmere om varsling om hendelser i punkt 7.

For å sikre rettslig grunnlag for deling av taushetsbelagt informasjon og personopplysninger foreslås det inntatt en bestemmelse i forskrift som regulerer deling av taushetsbelagt informasjon og personopplysninger mottatt ved hendelsesvarsling, se punkt 9.3.2.

Det foreslås også regler om behandling av personopplysninger hos tilbyderne, varslingsmottakere, utpekte sektormyndigheter, tilsynsmyndigheter og nasjonalt kontaktpunkt for sikkerhet i nettverk og informasjonssystemer. Dette omtales nærmere i punkt 11.

Myndigheter med sektoransvar fører tilsyn etter digitalsikkerhetsloven i den enkelte sektor. Nasjonal sikkerhetsmyndighet vil ha en koordinerende rolle og yte bistand til tilsynsmyndighetene gjennom veiledning. Det foreslås at det kan føres tilsyn med tilbydere av digitale tjenester etter at tilsynsmyndigheten har mottatt opplysninger om overtredelser av bestemmelser gitt i eller i medhold av loven og når tilsynsmyndigheten ellers finner det nødvendig. Tilsynsmyndigheten har rett til å kreve opplysninger og få tilgang til lokaler. Tilsyn er omtalt i punkt 9.

Tilsynsmyndigheten kan etter digitalsikkerhetsloven fatte enkeltvedtak om overtredelsesgebyr, tvangsmulkt og gi pålegg om opphør av ulovlige forhold. Som forutsatt i lovproposisjonen, gjelder forvaltningsloven for tilsynsmyndighetenes saksbehandling, jf. forvaltningsloven § 1 første punktum og Prop. 109 LS (2022–2023) kapittel 9. Dette innebærer at forvaltningslovens regler om klageadgang ved enkeltvedtak, hvem som er klageinstans, klagefrister og forvaltningens plikt til samordning i sanksjonssaker vil gjelde. Det foreslås at tilsynsmyndigheten skal kunne ilegge overtredelsesgebyr på opptil 25 ganger grunnløpet eller, dersom det dreier seg om et foretak, på opptil 4 prosent av den samlede årsomsetningen i det forutgående regnskapsår, der det høyeste beløpet anvendes. Overtredelsesgebyr er nærmere omtalt i punkt 12.

Departementet foreslår å utpeke Nasjonal sikkerhetsmyndighet som nasjonalt kontaktpunkt for sikkerhet i nettverk og informasjonssystemer og som nasjonalt responsmiljø for håndtering av hendelser, se punkt 10.

2 NIS1-direktivet

Europaparlamentets- og rådsdirektiv (EU) 2016/1148 ble vedtatt i EU 6. juli 2016 og har som formål å styrke den digitale sikkerheten i EU. Bakgrunnen for forslaget var at det, innen EU, ikke har vært implementert tilstrekkelige og helhetlige beskyttelsestiltak for å oppnå god nok sikkerhet i nettverk og informasjonssystemer som er særlig viktige for det indre markeds funksjon. Medlemslandene har ulik kvalitet på de beskyttelsestiltak som er implementert, hvilket medfører en fragmentert tilnærming på EU-nivå.

NIS1-direktivet omfatter utvalgte virksomheter som leverer tjenester som er viktige for å opprettholde funksjonen i det indre marked. Virksomhetene som omfattes av direktivet får i hovedsak to forpliktelser. De skal gjennomføre sikkerhetstiltak som står i et rimelig forhold til den risikoen virksomheten står overfor, og det innføres en plikt til å varsle om alvorlige digitale hendelser.

Direktivet gjelder for tilbydere av samfunnsviktige tjenester innenfor samfunnssektorene energi, transport, helse, vannforsyning, bank, finansmarkedsinfrastruktur og digital infrastruktur. Også tilbydere av digitale tjenester, nærmere bestemt nettbaserte markedsplasser, nettbaserte søkemotorer og skytjenester, omfattes av direktivet.

NIS1-direktivet gir medlemsstatene rom for nasjonal tilpasning, og setter minimumskrav til medlemsstatene når det gjelder både virkeområde og sikkerhetskrav. For eksempel er det opp til den enkelte medlemsstat å inkludere flere samfunnssektorer, samt å stille strengere sikkerhetskrav enn det som følger av direktivet. Direktivet stiller strengere krav til sikkerhet for tilbydere av samfunnsviktige tjenester enn for tilbydere av digitale tjenester. En konkretisering av kravene for sistnevnte kategori følger av gjennomføringsforordning 2018/151. Dette omtales nærmere i punkt 6 om krav til sikkerhet.

3 NIS2-direktivet

Europaparlaments- og rådsdirektiv (EU) 2022/2555 av 14. desember 2022 om tiltak for å sikre et høyt felles nivå for sikkerhet i nett- og informasjonssystemer i hele Unionen (NIS 2-direktivet) erstatter NIS1-direktivet.

Formålet med NIS2-direktivet er å øke motstandsdyktigheten i nettverk og informasjonssystemer til både private og offentlige aktører som opererer i relevante sektorer i EU, redusere fragmenteringen av det indre markedet i sektorer som allerede er omfattet av NIS1-direktivet, og forbedre den felles bevisstheten og kapasiteten knyttet til motstandsdyktighet. Direktivets virkeområde er utvidet i forhold til NIS1-direktivet ved at det omfatter flere sektorer som anses som kritiske for både økonomien og samfunnet. Utvidelsen innebærer at virkeområdet omfatter tilbydere av samfunnsviktige tjenester innen 18 definerte sektorer. Direktivet gjelder for offentlige og private enheter i sektorer som er angitt i vedlegg I eller II til direktivet. Det skilles mellom sektorer av høy kritisk betydning («high criticality») (vedlegg I) og andre kritiske sektorer (vedlegg II). For de enkelte enhetene som blir omfattet av NIS2-direktivet, skilles det mellom vesentlige («essential») og viktige («important») enheter, hvor vurderingen av hvilken kategori enheten tilhører blant annet beror på hvilken sektor enheten opererer i, størrelsen på enheten og om enheten er den eneste leverandøren av en samfunnsviktig tjeneste i en medlemsstat. Skillet mellom tilbydere av samfunnsviktige tjenester og tilbydere av digitale tjenester videreføres ikke, men tilbydere av digitale tjenester er kategorisert i NIS2-direktivet vedlegg II, såkalte andre kritiske sektorer.

NIS2-direktivet innfører mer presise bestemmelser om varsling av hendelser, herunder hva det skal varsles om og når det skal varsles. Direktivet er også nært knyttet til direktiv (EU) 2022/5557 om kritiste enheters motstandsdyktighet (CER-direktivet). Det pågår for tiden et arbeid med å utarbeide et utkast til høringsnotat med nødvendige regelverksendringer for gjennomføring av NIS2-direktivet og CER-direktivet i norsk rett.

Dersom NIS2-direktivet tas inn i EØS-avtalen blir det behov for revisjon av digitalsikkerhetsloven, eller regulering i en annen lov, og endringer eller opphevelse av en eventuell forskrift om digital sikkerhet basert på forslaget i dette høringsnotatet. Der det er hensiktsmessig har imidlertid departementet allerede forsøkt å tilnærme seg kravene i NIS2-direktivet, se blant annet forslag til § 15 om varslingsplikt og omtalen i punkt 7.

4 Lovens virkeområde

4.1 Gjeldende rett

Digitalsikkerhetsloven § 2 angir lovens saklige virkeområde. Virkeområdet til loven tilsvarer NIS1-direktivet artikkel 1 nr. 2 bokstav d. I § 2 første ledd bokstav a fremgår det at loven gjelder for tilbydere av samfunnsviktige tjenester innenfor samfunnssektorene energi, transport, helse, vannforsyning, bank, finansmarkedsinfrastruktur og digital infrastruktur. Loven gjelder ikke for virksomheter som er omfattet av lov om elektroniske tillitstjenester, jf. § 2 andre ledd.

Tilbydere av samfunnsviktige tjenester er definert i digitalsikkerhetsloven § 6 og må etter første ledd bokstav a til e oppfylle tre kumulative vilkår: virksomheten må levere en tjeneste som er viktig for å opprettholde kritiske samfunnsmessige eller økonomiske aktiviteter, den må være avhengig av nettverk og informasjonssystemer for å levere tjenesten, og kan få tjenesteleveransen betydelig forstyrret av en hendelse.

Det er kun den delen av virksomheten som leverer den aktuelle tjenesten som omfattes, se Prop. 109 LS (2022–2023) side 19.

Dersom det stilles krav om sikkerhet og varsling i annen lov eller forskrift som minst tilsvarer kravene etter digitalsikkerhetsloven, skal kravene etter denne andre loven eller forskriften benyttes, se § 5. Anvendelse av § 5 vil ikke direkte unnta de aktuelle virksomhetene fra lovens virkeområde. Identifiseringsprosessen skal fortsatt gjennomføres, og virksomhetene vil underlegges direktivet og loven. Konsekvensene av å bli underlagt vil imidlertid i praksis være begrenset, gitt at regelverket virksomheten er underlagt har tilsvarende eller strengere sikkerhets- og varslingskrav.

I loven § 2 tredje ledd er det fastsatt en hjemmel for Kongen til å gi forskrift med nærmere bestemmelser om og unntak fra lovens virkeområde. Bestemmelsen innebærer at Kongen i forskrift kan gi myndighet til å utpeke enkeltvirksomheter som ikke tilfredsstiller terskelverdiene eller andre kriterier som defineres i forskrift, men som det av andre årsaker er viktig å underlegge regelverket.

Lovens geografiske virkeområde er angitt i lovens § 3 andre ledd hvor Kongen gis forskriftskompetanse til å fastsette lovens anvendelse for Svalbard, Jan Mayen og bilandene og fastsette særlige regler som er nødvendige av hensyn til de stedlige forhold.

4.2 Departementets vurderinger og forslag

4.2.1 Lovens geografiske virkeområde

Svalbard er underlagt norsk suverenitet, men er unntatt fra virkeområdet til EØS-avtalen. Departementet uttalte i Prop. 109 LS (2022–2023) at også Svalbard bør omfattes av digitalsikkerhetslovens geografiske virkeområde, og foreslo i § 3 andre ledd at Kongen i forskrift kan bestemme om loven helt eller delvis skal gjelde for Svalbard. Etter departementets vurdering er flere av tjenestene nevnt i forslaget til § 1 i forskriften relevante på Svalbard, og departementet foreslår at forskriften § 3 angir at loven skal gjelde for Svalbard.

De særlige forholdene på Svalbard kan imidlertid tilsi at enkelte virksomheter på Svalbard bør underlegges loven ved enkeltvedtak, jf. forskriftsforslaget § 4 og punkt 4.2.3. Det gjelder for eksempel Svalbard Energi AS, som drifter energiforsyningen på Svalbard. Det samme kan gjelde for Longyearbyen sykehus og Apotek 1 Spitsbergen. Vannforsyningssystemet i Longyearbyen når ikke opp til terskelen som er angitt i forskriften § 1 nr. 23, men det kan likevel være aktuelt å fatte vedtak om at loven skal gjelde likevel for virksomheten. Det kan også bli aktuelt å fatte vedtak om at Longyearbyen havn og rederier med fast anløp til Longyearbyen havn underlegges digitalsikkerhetsloven selv om det per i dag ikke er slik at godsomlaget oppfyller terskelverdien i forskriftsforslagets.

Når det gjelder digitalsikkerhetslovens anvendelse for utenlandsk virksomhet på Svalbard, er det for tiden ingen utenlandske virksomheter som har noen av tjenestene som listes opp i forskriftsforslaget § 1. Det fremstår heller ikke som særlig nærliggende at utenlandske virksomheter vil kunne bli omfattet av opplistingen i § 1 i overskuelig fremtid.

4.2.2 Virkeområde for tilbydere av samfunnsviktige tjenester

4.2.2.1 *Identifiseringsprosess og terskelverdier*

Nasjonal sikkerhetsmyndighet gjennomførte i 2020 et kartleggingsarbeid i samarbeid med Direktoratet for samfunnssikkerhet og beredskap og berørte sektormyndigheter for å identifisere kriterier og terskelverdier som kan benyttes for å angi hvilke virksomheter som skal anses som tilbydere av samfunnsviktige tjenester. Forskriftsforslaget er basert på dette kartleggingsarbeidet. Terskelverdiene identifiserer hvilke tjenester som er viktige for å opprettholde kritiske samfunnsmessige eller økonomiske aktiviteter, jf. digitalsikkerhetsloven § 6 første ledd bokstav a og direktivet artikkel 5 nr. 2, jf. artikkel 4 nr. 4. Virksomheter som yter disse tjenestene vil være omfattet av lovens virkeområde.

Tilnærmingen med terskelverdier fungerer slik at det innenfor hver sektor angis kategorier av tjenester eller størrelser på produksjon, drift eller brukere. Ved utarbeidelsen av terskelverdier er det sett hen til andre europeiske land, særlig Storbritannia og Sverige. Terskelverdiene er søkt harmonisert på tvers av sektorer slik at innslagspunktet for loven vil være likest mulig uavhengig av sektor. Videre er det lagt vekt på å benytte allerede eksisterende sektorregelverk, herunder terskelverdier der det foreligger. I tillegg er terskelverdiene forsøkt utformet så konkret at det skal være mulig for tilbyder selv å avgjøre hvorvidt de leverer en samfunnsviktig tjeneste.

For tilbydere av samfunnsviktige tjenester vil terskelverdiene etter forslaget her avgrense virkeområdet til tilbyderne som opererer innenfor en av sektorene angitt i loven § 2 første ledd bokstav a, og som i tillegg anses som en «tilbyder av en samfunnsviktig tjeneste» i lovens og direktivets forstand. Dette innebærer at det i utgangspunktet kun er virksomhetene innenfor de nevnte sektorene som vil være underlagt loven.

4.2.2.2 *Kraft*

Digital sikkerhet i kraftsektoren er i dag regulert i forskrift 7. desember 2012 nr. 1157 om sikkerhet og beredskap i kraftforsyningen (kraftberedskapsforskriften). Kraftberedskapsforskriften gjelder for virksomheter som inngår i kraftforsyningens beredskapsorganisasjon (KBO-enheter). KBO-enheter er virksomheter som eier eller driver anlegg, system eller annet som er klassifisert etter kapittel 5 i kraftberedskapsforskriften, samt andre virksomheter Norges vassdrags- og energidirektorat har utpekt ved enkeltvedtak.

Anlegg, system eller annet som har vesentlig betydning for drift eller gjenoppretting av eller sikkerhet i produksjon, omforming, overføring eller fordeling av elektrisk energi eller fjernvarme, skal klassifiseres. Klasse 1 til 3 blir benyttet. Klasse 3 er de anlegg/system/annet hvor betydningen for kraftforsyningen er størst. Bestemmelsen oppstiller videre kriterier for hvilken klasse et anlegg eller system tilhører.

Markedsplasser og omsettere av kraft faller utenfor kriteriene i forskriften § 5-2. Norges vassdrags- og energidirektorat vurderte i mars 2020 at markedsplassene EMCO og Nordpool var av så stor betydning for kraftforsyningen at de ble utpekt som KBO-enheter. Det er per i dag ingen omsettere som er utpekt som KBO-enheter.

Dersom en virksomhet eier eller driver et klassifisert anlegg eller system, er dette anlegget/systemet definert å være av vesentlig betydning for kraftforsyningen. Alle enheter i kraftforsyningen er avhengige av nettverk og informasjonssystemer, og hendelser vil derfor ha betydelig innvirkning på tjenesteleveransen. På bakgrunn av dette bør digitalsikkerhetsloven etter departementets syn gjøres gjeldende for alle virksomheter som er KBO-enheter eller helt eller delvis er underlagt.

Departementet foreslår at KBO-enheter, jf. kraftberedskapsforskriften § 2-1 andre ledd og virksomheter som helt eller delvis er underlagt kraftberedskapsforskriften etter samme forskrift § 1-3 andre ledd, blir underlagt digitalsikkerhetsloven gjennom forslag til forskriften § 1 første ledd nr. 1 og nr. 2.

4.2.2.3 *Olje- og gassforsyning*

Som nevnt er forskriftsforslaget ment å bidra til å gjennomføre NIS1-direktivet i norsk rett, jf. Prop. 109 LS (2022–2023) side 13. I tråd med EØS-avtalen artikkel 126 gjelder ikke NIS1-direktivet for virksomhet på kontinentalsokkelen. Departementet viser i den forbindelse til Prop. 109 LS (2022–2023) side 28 hvor det fremgår at direktivets geografiske virkeområde som utgangspunkt vil tilsvare EØS-avtalens virkeområde. Det vil si at direktivet vil gjelde på norsk territorium, jf. EØS-avtalen artikkel 126. Kontinentalsokkelen, den økonomiske sonen og den tilstøtende sonen omfattes ikke. Direktivet gjelder dermed ikke for norsk oppstrøms petroleumsvirksomhet, som i all hovedsak foregår på kontinentalsokkelen. Av den grunn vil ikke oppstrøms olje- og gassanlegg

omfattes i listen over tilbydere av samfunnsviktige tjenester etter forskriftsforslaget § 1. Departementet legger til at også landanleggene dermed vil falle utenfor lovens virkeområde. Etter departementets vurdering er likevel norsk oppstrøms olje- og gassproduksjon av sentral betydning for Norge. Gode grunner taler for at denne typen virksomhet bør omfattes av et nasjonalt regelverk om sikkerhet i nettverk og informasjonssystemer på sikt.

Når det gjelder drivstofflager innbefatter dette all infrastruktur og utstyr som er nødvendig for å kunne motta petroleumsprodukter for lagring, lagre disse på tank og få disse ut av tank og over på tankbil og tog. Det legges til grunn at drivstofflagrene benytter IKT-systemer til inn- og utpumping av drivstoff og derfor er avhengig av nettverk og informasjonssystemer, jf. NIS1-direktivet artikkel 5 nr. 2 bokstav b.

Departementet foreslår på denne bakgrunn at forskriften § 1 første ledd nr. 3 angir at hovedtankanlegg for petroleumsbasert drivstoff anses som en samfunnsviktig tilbyder innenfor olje- og gassforsyningen.

4.2.2.4 *Luftfart*

Avinor driver den nasjonale flysikringstjenesten i Norge. Norsk kommersiell lufttransport består av kommersielle lufthavner, leverandører av ulike tjenester på sikkerhetsbegrenset område på lufthavnene, og fly- og helikopterselskaper med godkjenning fra Luftfartstilsynet (AOC/Air Operator's Certificate).

Driftsforstyrrelser på lufthavnene vil ha en betydelig forstyrrende effekt på den nasjonale lufttransporten. Det er også nødvendig med et felles sikkerhetsnivå på samtlige lufthavner. Det foreslås derfor at samtlige kommersielle lufthavner underlegges loven.

Forstyrrelser på informasjons- og nettverksinfrastruktur hos de som leverer tjenester på sikkerhetsbegrenset område på lufthavnen kan ha betydning for driften av selve lufthavnen, og disse bør også omfattes av loven. I tillegg vil driftsforstyrrelser hos kommersielle fly- og helikopterselskaper kunne få konsekvenser for persontrafikk, godstrafikk og trafikk til og fra offshoreinstallasjoner i olje- og gassektoren.

Departementet foreslår på denne bakgrunn at det i forskriften § 1 første ledd nr. 4, nr. 5 og nr. 6 angis at innenfor lufttransport skal følgende tilbydere regnes som samfunnsviktige:

- flysikringstjenesten
- kommersielle lufthavner og tjenesteleverandører innenfor sikkerhetsbegrenset område på en kommersiell lufthavn
- flyselskaper som driver kommersiell transport med AOC i Norge.

4.2.2.5 *Jernbanetransport*

Bane NOR forvalter jernbaneinfrastrukturen i Norge og har ansvar for trafikkstyringen. Infrastrukturen består av spor, strømforsyning, signalsystemer, radiokommunikasjon, stasjoner, godsterminaler og tekniske anlegg.

De foreslåtte terskelverdiene vil omfatte persontransport på flytogene, lokaltog i Oslo, Stavanger, Bergen og Trondheim, InterCity-togene på Østlandet, samt nattog og fjerntrafikk. Terskelverdien for godstransport vil omfatte de største

transportørene. Den foreslåtte terskelverdien vil også inkludere T-bane og trikk i Oslo, samt Bybanen i Bergen.

Departementet foreslår at det innenfor jernbanetransport i forskriften § 1 første ledd nr. 7, nr. 8, nr. 9 og nr. 10 angis at følgende tilbydere av tjenester skal anses som samfunnsviktige:

- infrastrukturforvaltning og trafikkstyring av det nasjonale jernbanenettet
- persontransport som overstiger 375 000 togkilometer pr. år, inkludert grenseoverskridende transport
- godstransport som overstiger 500 000 togkilometer pr. år, inkludert grenseoverskridende transport
- infrastrukturforvaltning, trafikkstyring og togfremføring av T-bane og trikk som overstiger 12,5 millioner årlige passasjerreiser.

4.2.2.6 *Vegtransport*

Terskelverdien vil omfatte trafikkstyring og overvåking på deler av europavegnettet (E6, E16, E18, E39) og de mest sentrale vegnettene rundt de store byområdene. Dette innebærer at både vegtrafikksentralene og utstyr som er nødvendig for vegtrafikksentralenes evne til å overvåke disse vegnettene, omfattes. Videre vil eventuelle nasjonale eCall alarmsentraler omfattes. Det samme gjelder nasjonale databanker med veg- og trafikkinformasjon. I dag gjelder dette Nasjonal vegdatabank drevet av Statens vegvesen.

Departementet foreslår at det innenfor vegtransport i forskriften § 1 første ledd nr. 11, nr. 12, nr. 13 og nr. 14 angis at følgende tilbydere av tjenester skal anses som samfunnsviktige:

- trafikkstyring og -overvåking av TEN-T-vegnett
- det viktigste vegnettet i områder med årsdøgntrafikk over 20 000
- alarmsentraler for eCall
- nasjonale databanker som inneholder veg- eller trafikkinformasjon.

4.2.2.7 *Sjøtransport*

De foreslåtte terskelverdiene vil omfatte de største havnene for gods- og persontrafikk. I tillegg vil terskelverdiene også omfatte de rederiene som har en betydelig del av trafikken på disse havnene.

Departementet foreslår at det innenfor sjøtransport i forskriften § 1 første ledd nr. 15, nr. 16, nr. 17 og nr. 18 angis at følgende tilbydere av tjenester regnes som samfunnsviktige:

- trafikkstyring og -overvåking av kysttrafikken
- havner eller havneanlegg som har et godsomlag på mer enn 100 000 tonn pr. år sett over en femårsperiode
- havner eller havneanlegg som håndterer mer enn 100 000 passasjerer pr. år sett over en femårsperiode
- rederier som har skip med fast anløp eller som transporterer minst fem prosent av passasjerantallet eller godsomlaget i en havn som nevnt over

4.2.2.8 *Helse*

Departementet viser til at helsesektoren i Danmark og Norge er organisert relativt likt, og forslaget til terskelverdier er derfor basert på den danske modellen. Departementet foreslår at det innen helsesektoren i forskriften § 1 første ledd nr.

19, nr. 20, nr. 21 og nr. 22 angis at følgende tilbydere av tjenester anses som samfunnsviktige:

- Helse- og omsorgsdepartementet med underliggende etater og foretak, som utgjør den nasjonale helseberedskapen
- tjenester som tilbys av de regionale helseforetakene
- sentrale systemer for rekvirering og utlevering av legemidler og andre medisinske produkter
- helse- og omsorgstjenester som tilbys av en kommune med
    - a. flere enn 50 000 innbyggere, eller
    - b. flere enn 20 000 brukere som er avhengige av tjenesten, og
    - c. tjenesten ikke kan overføres eller avlastes av andre tjenester.

Med «omfattet av» menes antall innbyggere som ligger innenfor helsetjenestens ansvarsområde. Men «avhengig av» menes antall brukere, altså pasienter og helsepersonell, som ikke kan benytte andre tjenester i tilfelle bortfall.

4.2.2.9 *Drikkevann*

Den foreslåtte terskelverdien bygger på samme systematikk som forskrift om vannforsyning og drikkevann, og innebærer at vannforsyningsanlegg som forsyner ca. 10 000 innbyggere vil omfattes av digitalsikkerhetsloven. Departementet foreslår derfor at det innen drikkevannsforsyning og -distribusjon angis i forskriften § 1 første ledd nr. 23 at tilbydere av følgende tjeneste skal regnes som samfunnsviktig: vannforsyningsanlegg, jf. drikkevannsforskriften § 3 bokstav k, som behandler minst 2000 m3 pr. døgn.

4.2.2.10 *Digital infrastruktur*

Norid AS er registerenheten for toppdomener i Norge og driver registeret for norske domenenavn. Alle domenenavn direkte under .no er registrert hos Norid. Tjenesten er regulert av forskrift om domenenavn under norske landkodetoppdomener (domeneforskriften) med Nasjonal kommunikasjonsmyndighet som tilsynsmyndighet. Denne tjenesten er en sentral del av den grunnleggende nettinfrastrukturen i Norge, og har høye krav til tilgjengelighet. Norid har også ansvaret for toppdomenene .bv (Bouvetøya) og .sj (Svalbard og Jan Mayen), men disse er ikke åpnet for registrering av domenenavn.

Rekursiv navneservertjeneste er en tjeneste innenfor domenenavnsystemet (DNS). Fordi datamaskiner kun forstår tall, oversetter DNS en URL til et nettsted om til tall, en såkalt IP-adresse. Domenenavnsystemet er et hierarkisk oppbygget navnesystem som brukes til å knytte domenenavn til IP-adresser og til å formidle teknisk informasjon som trengs for å adressere nettsider, e-post og andre tjenester over internett. DNS er dermed en sentral enhet i internetts funksjonalitet.

En viktig kjernefunksjon for internett er samtrafikkpunkter (Internet Exchange Point-IXP). I Norge utveksler internettaktørene trafikk mellom sine nett på samtrafikkpunkter. Samtrafikkpunkter kobler sammen lokale, regionale og nasjonale internettaktører og bidrar dermed til en robust og motstandsdyktig internettinfrastruktur i Norge. Samtrafikkpunktene har sikkerhets- og beredskapsmessig betydning uavhengig av det daglige trafikkvolumet i en normalsituasjon.

Departementet foreslår derfor at det innenfor digital infrastruktur i forskriften § 1 første ledd nr. 24, nr. 25 og nr. 26 angis at tilbydere av følgende tjenester skal anses som samfunnsviktige:

- sentralt register over norske toppnivådomener (.no, .bv og .sj)
- rekursiv navneservertjeneste med flere enn 50 000 aktive brukere
- samtrafikkpunkter for Internett

4.2.2.11 *Bank og finansmarkedsinfrastruktur*

Departementet har mottatt forslag fra Finansdepartementet basert på innspill fra Finanstilsynet om hvilke terskelverdier som bør foreslås for sektorene bank og finansmarkedsinfrastruktur. I sitt innspill har Finanstilsynet sett hen til både reguleringene som følger av NIS1-direktivet og NIS2-direktivet, og foreslår to alternative muligheter for innretning av terskelverdier. Departementet foreslår i dette høringsnotatet kun at terskelverdiene etter NIS1-direktivet reguleres i forskriftsforslaget. Det har sammenheng med at det pågår et større utredningsarbeid knyttet til innlemmelse av NIS2-direktivet i norsk rett. Finanstilsynet har vurdert at langt flere foretak vil bli omfattet av NIS2-direktivet sammenlignet med NIS1-direktivet. Etter departementets syn vil det derfor være naturlig at terskelverdiene i forskriftsforslaget samsvarer med NIS1-direktivets bestemmelser.

Departementet foreslår at terskelverdiene for banker skal være de tilsvarende kriterier som ligger til grunn for utpeking av foretak som er systemviktige foretak etter forskrift 22. august 2014 nr. 1097 om kapitalkrav og nasjonal tilpasning av CRR/CRD IV (CRR/CRD IV-forskriften) § 30. Bestemmelsen gjelder identifisering av foretak som er systemviktige i Norge. Etter første ledd skal Finansdepartementet hvert år treffe beslutning om hvilke foretak som skal anses som systemviktige i Norge. Etter andre og tredje ledd er det oppgitt hvilke foretak som skal anses som systemviktige etter nærmere kriterier. Finansdepartementet har i medhold av bestemmelsen identifisert DNB ASA, Kommunalbanken AS, Nordea Eiendomskreditt AS og Sparebank 1 SR-Bank ASA som systemviktige finansforetak i Norge. Av disse er DNB ASA og Sparebank 1 SR-Bank ASA banker, mens Kommunalbanken og Nordea Eiendomskreditt er kredittforetak. Departementet legger opp til at kredittforetakene ikke omfattes av digitalsikkerhetslovens virkeområde fordi kredittforetak ikke er banker, og dermed faller utenfor NIS1-direktivet, jf. NIS1-direktivet vedlegg II nr. 3.

Når det gjelder terskelverdier for finansmarkedsinfrastruktur, har Finanstilsynet på oppdrag fra Finansdepartementet foreslått at det skal foretas en vurdering av foretakets betydning for det norske kapitalmarkedet. For at kriteriet skal være oppfylt, må virksomheten ha vesentlig betydning for det norske kapitalmarkedet. Finanstilsynet har identifisert at Oslo Børs ASA vil være det eneste foretaket som faller innunder denne terskelverdien.

Sektorene bank og finansmarkedsinfrastruktur foreslås derfor omfattet av lovens virkeområde forutsatt at de faller innenfor digitalsikkerhetsforskriftens terskelverdier. Disse foretakene er i dag underlagt krav etter finansregelverket, herunder IKT-forskriften, som tilsvarer kravene i digitalsikkerhetsloven. Foretak i finanssektoren er dermed allerede omfattet av krav som tilsvarer kravene i digitalsikkerhetsloven. Dette innebærer at foretak i disse sektorene som omfattes av virkeområdet i forskriftsforslaget, ikke vil pålegges særskilte krav etter

digitalsikkerhetsloven, jf. Prop. 109 LS (2022–2023) punkt 3.5.1. Finansdepartementet arbeider for øvrig med gjennomføring av et EU-regelverk om digital operasjonell motstandsdyktighet i finanssektoren (DORA), som vil gi mer omfattende krav enn dagens IKT-forskrift.

Terskelverdier for bank og finansmarkedsinfrastruktur foreslås inntatt i forskriftsforslaget § 1 første ledd nr. 27 og nr. 28.

4.2.3 Utpeking av virksomheter som tilbyr samfunnsviktige tjenester

For å sikre at loven gjelder for virksomheter som ikke tilfredsstiller terskelverdiene, men som likevel er i en særstilling eller har en rolle som gjør at de bør omfattes av loven, bør det etter departementets syn gis anledning til å utpeke enkeltvirksomheter loven skal gjelde helt eller delvis for. Denne adgangen vil gi nødvendig fleksibilitet og sikre oppfyllelse av lovens formål. På denne bakgrunn foreslår departementet at det i forslag til forskrift § 4 angis at det i særlig tilfeller kan fattes enkeltvedtak om at loven skal gjelde helt eller delvis for andre tilbydere av samfunnsviktige tjenester enn de som er nevnt i forskriften § 1. Bestemmelsen gjelder virksomheter som faller innunder samfunnssektorene nevnt i digitalsikkerhetsloven § 2.

Kompetansen til å utpeke virksomheter foreslås lagt til ansvarlig departement, og Nasjonal sikkerhetsmyndighet for virksomheter som ikke omfattes av et departements ansvarsområde. I vurderingen av om en enkeltvirksomhet skal omfattes av loven, skal direktivets og lovens rammer for tilbydere av samfunnsviktige tjenester benyttes. I tillegg skal det tas hensyn til kriteriene for fastsetting av terskelverdier som beskrevet over.

Kompetansen til ansvarlig departement om å utpeke enkeltvirksomheter etter bestemmelsen kan delegeres i tråd med gjeldende prinsipper for delegasjon.

På vanlig måte vil vedtak fattet av ansvarlig departement, kunne påklages til Kongen i statsråd, jf. forvaltningsloven § 28 første ledd. Vedtak truffet av Nasjonal sikkerhetsmyndighet vil kunne påklages til Justis- og beredskapsdepartementet.

4.2.4 Innmelding av samfunnsviktige tjenester

Etter direktivet artikkel 5 skal det føres en liste over virksomheter som tilbyr samfunnsviktige tjenester, se også fortalen punkt 22 og 23. Listen skal oppdateres jevnlig og minst hvert andre år. I tilfelle tjenesten tilbys i flere land, forutsettes det i direktivet at myndighetene i de aktuelle landene konfererer før det tas en beslutning om identifikasjon, jf. artikkel 5 nr. 4.

Listen over virksomheter som tilbyr samfunnsviktige tjenester utgjør et av flere forhold Norge skal rapportere om til EFTAs overvåkingsorgan (ESA). I tillegg vil det være nødvendig for tilsynsmyndigheten å få oversikt over hvilke virksomheter det skal føres tilsyn med. For Nasjonal sikkerhetsmyndighet er det viktig å ha den totale oversikten over alle innmeldte virksomheter for å ivareta sin rolle som nasjonalt kontaktpunkt. Departementet viser også til at Nasjonal sikkerhetsmyndighet skal ha en koordinerende rolle for alle tilsynsmyndigheter.

På denne bakgrunn foreslår departementet i § 5 en plikt for virksomheter om å melde inn både til tilsynsmyndigheten og Nasjonal sikkerhetsmyndighet at

virksomheten tilbyr tjenester som regnes som samfunnsviktig og dermed omfattes av digitalsikkerhetsloven. Etter departementets syn vil det være begrensede administrative byrder ved at tilbyder skal melde inn samme informasjonen til både tilsynsmyndigheten og Nasjonal sikkerhetsmyndighet. Et alternativ er at tilbyderen kun melder inn til Nasjonal sikkerhetsmyndighet, og at Nasjonal sikkerhetsmyndighet deretter melder videre til tilsynsmyndighetene. Et annet alternativ er at offentlige myndigheter utpeker tilbyderne på tilsvarende måte som etter sikkerhetsloven § 7-1 andre ledd. Departementet ber om høringsinstansenes syn på dette.

I tillegg til tilbyders navn, organisasjonsnummer og kontaktinformasjon, foreslås det at innmeldingen nevner hvilken tjeneste som er aktuell og om tjenesten tilbys i andre land. Listen bør holdes oppdatert ved at tilbyder melder inn endringer i informasjonen, og om tjenesten ikke lenger kan anses å være samfunnsviktig i lovens forstand, slik at virksomheten kan fjernes fra listen. Plikten vil også gjelde ved endringer i virksomheter som tidligere ikke har oppfylt terskelverdiene og for nye virksomheter som oppfyller terskelverdiene.

Virksomheter som opererer innen flere sektorer, må melde inn til samtlige tilsynsvirksomheter i sektorene de opererer i, samt Nasjonal sikkerhetsmyndighet.

4.2.5 Unntak for små virksomheter

Det følger av direktivet artikkel 16 nr. 11 at kapittel 5 ikke får anvendelse på mikrovirksomheter og små virksomheter som er definert i Kommisjonsrekommandasjon 2003/361/EF av 16. mai 2003. Kapittel 5 i direktivet regulerer sikkerhets- og varslingskrav, håndheving og jurisdiksjon for tilbydere av digitale tjenester. I digitalsikkerhetsloven er det bestemt at det i forskrift kan gis nærmere regler om lovens anvendelsesområde, se § 2 tredje ledd. Videre fremgår det i Prop. 109 LS (2022–2023) punkt 3.5.3 at anvendelse for små og mikrovirksomheter skal reguleres nærmere i forskrift.

Kommisjonsrekommandasjonens definisjon av små virksomheter er virksomheter som har færre enn 50 ansatte og som har en årlig omsetning eller årlig samlet balanse som ikke overstiger 10 millioner euro, jf. Kommisjonsrekommandasjonen artikkel 2. Definisjonen av mikrovirksomheter i artikkel 3 konsumeres av artikkel 2.

Kommisjonsrekommandasjonen er ikke tatt inn i EØS-avtalen, men tilsvarende terskel er tatt inn i annet norsk regelverk. For eksempel er det i forskrift 27. mars 2020 nr. 490 til lov om statlig garantiordning for lån til små og mellomstore bedrifter § 3 andre ledd angitt at med små bedrifter menes blant annet virksomheter som sysselsetter færre enn 50 personer og som har en årlig omsetning eller årsbalanse som ikke overstiger 10 millioner euro.

På denne bakgrunn foreslår departementet at det i forskriften § 2 angis at tilbydere av digitale tjenester som har færre enn 50 ansatte og som har en årlig omsetning eller årlig samlet balanse som ikke overstiger 100 millioner kroner ikke omfattes av § 13 om sikkerhetskrav for tilbydere av digitale tjenester og § 15 om varslingsplikt. Dette innebærer at denne typen virksomheter fortsatt vil være å anse som «tilbydere av digitale tjenester» i lovens forstand, men at de er unntatt krav til sikkerhet og varsling. Til forskjell fra for eksempel forskrift til lov om statlig garantiordning for lån til små og mellomstore bedrifter, foreslår

departementet at terskelverdien oppgis i norske kroner og ikke euro. For enkelhets skyld foreslår departementet at beløpet settes til 100 millioner kroner.

5 Krav til sikkerhet for samfunnsviktige tjenester

5.1 Gjeldende rett

I digitalsikkerhetsloven § 7 oppstilles krav til sikkerhet for tilbydere av samfunnsviktige tjenester. Etter første ledd skal en tilbyder av en samfunnsviktig tjeneste gjennomføre en risikovurdering av nettverk og informasjonssystemer som benyttes for å levere tjenesten.

Etter andre ledd skal tilbyderen iverksette hensiktsmessige og proporsjonale tekniske og organisatoriske tiltak som samlet skal sørge for et sikkerhetsnivå som er tilpasset risikoen. Ved vurderingen skal det blant annet ses hen til den teknologiske utviklingen.

Etter tredje ledd skal tilbyderen iverksette proporsjonale tiltak for å forebygge, avdekke og redusere konsekvensene av hendelser med det formål å opprettholde tjenesteleveransen. Ved vurderingen av hva som er et forsvarlig sikkerhetsnivå, skal det blant annet ses hen til den teknologiske utviklingen. Departementet viser til at dette kan ha betydning for både nye trusler og sårbarheter og oppdatering eller iverksetting av nye tiltak. I den grad tilstrekkelig sikkerhet oppnås gjennom annet regelverk, viser departementet til at det ikke er nødvendig å følge sikkerhetskravene som følger av digitalsikkerhetsloven.

5.2 NIS1-direktivet

Sikkerhetskravene som stilles til tilbydere av samfunnsviktige tjenester følger av artikkel 14 nr. 1 og 2. Tilbyderne skal sikre nettverk og informasjonssystemer som anvendes for å levere den samfunnsviktige tjenesten. Tilbyderen skal treffe tekniske og organisatoriske tiltak som er hensiktsmessige og står i et rimelig forhold til risikoen som knytter seg til nettverkene og informasjonssystemene. Ved vurderingen av hvilke tiltak som er proporsjonale skal det tas hensyn til den teknologiske utviklingen. For å sikre opprettholdelse av tjenesteleveransen, skal tilbyderen treffe tiltak som er egnet til å forebygge, avdekke og redusere virkningen av hendelser som truer sikkerheten i tilbyderens IKT-systemer.

Nærmere om hva som ligger i sikkerhetskravene er bare til en viss grad omhandlet i fortalen. Det gis 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 har utarbeidet retningslinjer for hva som ligger i sikkerhetskravet i Reference document on security measures for Operators of Essential Services CG Publication 01/2018. Retningslinjene oppsummerer landenes tilnærming til sikkerhetskrav.

Etter NIS1-direktivet artikkel 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. artikkel 16 nr. 10.

Det fremgår av fortalepunkt 52 at tilbydere av samfunnsviktige tjenester og tilbydere av digitale tjenester bør sikre sikkerheten i nettverk og informasjonssystemene som de bruker. Dette er først og fremst private nettverk og informasjonssystemer som ivaretas av internt IT-personell eller der sikkerhetsoppgavene er satt ut. Sikkerhets- og meldingskravene bør få anvendelse på berørte ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester, uansett om de utfører vedlikehold av nettverk og informasjonssystemene sine internt eller setter det ut.

5.3 Departementets vurderinger og forslag

5.3.1 Innledning

I Prop. 109 LS (2022–2023) punkt 6.5 forutsetter departementet at det nærmere innholdet i sikkerhetskravene som følger av digitalsikkerhetsloven vil bli spesifisert i forskrift. Bestemmelsene i loven er funksjonsbaserte og tar utgangspunkt i forsvarlighetsstandarden «forsvarlig sikkerhet». Forsvarlighetsstandarder benyttes også i andre lover, blant annet sikkerhetsloven og ekomloven. Sikkerhetskravene i digitalsikkerhetsloven kan være tilfredsstilt ved å følge anerkjente standarder, generelle eller sektorspesifikke retningslinjer eller prinsipper for digital sikkerhet. Virksomhetene må vurdere om de gjennom allerede gjeldende tiltak tilfredsstiller lovens krav til sikkerhet, eller om det må iverksettes andre tiltak for å oppfylle kravene basert på gjennomført risikovurdering.

I departementets forslag til forskriftsbestemmelser om digital sikkerhet er det foreslått flere konkrete krav til digital sikkerhet. Det foreslås ni bestemmelser som samlet skal bidra til et minimumsnivå av sikkerhet i nettverk og informasjonssystemer. Omtalen følger nedenfor i punktene 5.3.2 til 5.3.7. Forslaget bygger på anerkjente standarder og prinsipper for digital sikkerhet.

Departementet finner grunn til å presisere at sikkerhetstiltakene som foreslås i forskriftsforslaget skal være hensiktsmessige, proporsjonale og samlet sørge for et sikkerhetsnivå som er tilpasset risikoen. I dette ligger at omfanget av sikkerhetstiltakene må tilpasses størrelsen og kompleksiteten på virksomheten.

5.3.2 Krav til styringssystem for sikkerhet

Departementet foreslår en bestemmelse i § 6 som stiller krav til at tilbydere av samfunnsviktige tjenester skal etablere og vedlikeholde et styringssystem for sikkerhet som omfatter digital sikkerhet. Dette skal være dokumentert og inngå som en del av den overordnede styringen av virksomheten.

Etter departementets vurdering er det sentralt at virksomheten har en systematisk og dokumentert tilnærming til digital sikkerhet, og det er viktig at arbeidet med digital sikkerhet inngår som en del av den ordinære styringen av virksomheten. Styringssystemet vil blant annet kunne sikre at virksomheten implementerer nødvendige sikkerhetstiltak og har en plan for håndtering av hendelser.

I forslag til andre ledd foreslås det en bestemmelse om at styringssystemet skal baseres på anerkjente standarder og bidra til å forebygge, avdekke og håndtere hendelser, korrigere og gjenopprette sikkerheten i nettverk og informasjonssystemer ved hendelser og kontinuerlig styre og følge opp at nevnte formål oppnås.

Departementet foreslår at det i tredje ledd fastsettes at sikkerhetsstyringssystemet skal inneholde alle aktiviteter som er nødvendige for å etablere og opprettholde et forsvarlig sikkerhetsnivå, at disse skal dokumenteres og gjøres kjent for personell med tjenstlig behov. Dette inkluderer fordeling av roller og ansvar for sikkerhetsarbeidet, men departementet finner ikke grunn til å gjengi dette i forskriften.

I fjerde ledd foreslås det et krav om at virksomhetens leder har ansvar for at virksomheten har et forsvarlig sikkerhetsnivå innen virkeområdet til digitalsikkerhetsloven. Det foreslås videre et krav om at sikkerhetsstyringssystemet skal godkjennes av virksomhetens leder og årlig gjennomgås med sikte på forbedring av virksomhetens sikkerhetsarbeid, herunder arbeid med digital sikkerhet. Departementet har sett hen til sikkerhetslovens systematikk og krav om at det det overordnede ansvaret for det forebyggende sikkerhetsarbeidet ligger hos virksomhetens leder.

Virksomhetens øverste ledelse er ansvarlig for å sette mål og føringer for sikkerhet, etablere et styringsdokument for det forebyggende sikkerhetsarbeidet, sikre hensiktsmessig sikkerhetsorganisering og følge opp sikkerhetsarbeidet jevnlig, blant annet ved å sørge for at iverksatte sikkerhetstiltak kontrolleres. Etter departementets vurdering er det viktig at virksomhetens øverste ledelse har et bevisst forhold til digital sikkerhet, og dette sikres blant annet ved krav om ledelsesforankring av sikkerhetsstyringssystemet.

Formålet med sikkerhetsstyring er å etablere en kontinuerlig forbedringsprosess for forebyggende sikkerhetsarbeid i virksomheten slik at sikkerheten i nettverk og informasjonssystemer i virksomheten er tilstrekkelig ut fra en risikobasert tilnærming. Sikkerhetsstyring omfatter alle aktiviteter som er nødvendige for å ivareta og forbedre sikkerheten i virksomhetens nettverk og informasjonssystemer som ligger til grunn for tjenesteleveransen. Departementet vil bemerke at dersom tjenesten ikke er avhengig av nettverk og informasjonssystemer, gjelder ikke loven, jf. digitalsikkerhetsloven § 6 første ledd bokstav b.

Sikkerhetsstyring er avgjørende for at virksomheten kan identifisere og iverksette riktige tiltak og forbedre det forebyggende sikkerhetsarbeidet over tid. Et styringssystem for digital sikkerhet skal sørge for at virksomheten identifiserer og lukker sårbarheter.

5.3.3 Risikovurdering

Risikovurderinger er en helt nødvendig del av arbeidet med digital sikkerhet fordi denne blant annet vil være styrende for hvilke sikkerhetstiltak som er relevante og proporsjonale i virksomheten. Dette må dokumenteres både for virksomhetens egenvurdering av tiltak, og for tilsynsmyndighetenes kontroll med overholdelse av loven. Departementet foreslår derfor en egen bestemmelse i § 7 om risikovurdering. I første ledd første punktum foreslås det fastsatt en plikt til å utarbeide, vedlikeholde og dokumentere risikovurderinger. Departementet har

vurdert om bestemmelsen skal si noe mer om metode for risikovurdering, men kommet til at dette ikke anses hensiktsmessig. Det er nærliggende å anta at virksomhetene vil følge anerkjente og relevante standarder for risikovurdering eller veileder fra sektormyndigheter eller Nasjonal sikkerhetsmyndighet. Departementet vurderer at forskriften bør gi rom for at virksomhetene tilpasser metodikken for risikovurderingen til egen sektor og egenart.

I andre ledd første punktum foreslår departementet et funksjonskrav til risikovurderingen, nemlig at den skal ha et slikt omfang at tilbyderen kan identifisere organisatoriske, teknologiske, fysiske og personellmessige sikkerhetstiltak som ivaretar formålene i § 8. Departementet anser dette som et grunnleggende krav til enhver risikovurdering. Det er helt sentralt at en risikovurdering kan benyttes til å tilpasse sikkerhetstiltakene til den identifiserte risikoen. Det foreslås også angitt eksplisitt i forslag til andre ledd andre punktum at risikoen ved endringer i virksomheten som kan påvirke sikkerheten særskilt skal vurderes.

I forslag til tredje ledd foreslås det enkelte konkrete krav til hva risikovurderingen minst skal inneholde:

a. en kartlegging av virksomhetens nettverk og informasjonssystemer og hvilken betydning disse har for leveransen av den samfunnsviktige tjenesten
b. hvilke hendelser disse kan bli utsatt for,
c. hvilke sårbarheter som er knyttet til virksomhetens nettverk og informasjonssystemer,
d. sannsynligheten for at en hendelse kan inntreffe,
e. konsekvensen av hendelser
f. i hvilken grad virksomheten er avhengig av andre virksomheter for å fungere som den skal

I forslag til punkt a pålegges tilbyderen å kartlegge virksomhetens nettverk og informasjonssystemer og hvilken betydning disse har for leveransen av den samfunnsviktige tjenesten. For å kunne utarbeide en god risikovurdering er det viktig å ha oversikt over virksomhetens nettverk og informasjonssystemer og å kunne beskrive betydningen disse har for leveransen av tjenester. I beskrivelsen av hvilken betydning nettverk og informasjonssystemer har for leveransen av den samfunnsviktige tjenesten inngår en vurdering av hvor avhengig virksomheten er av at disse fungerer for at den samfunnsviktige tjenesten fungerer.

Etter forslag til punkt b skal tilbyderen ha et bevisst forhold til hvilke hendelser virksomheten kan bli utsatt for. Hendelsesbegrepet her må ses i sammenheng med definisjonen av «hendelse» i digitalsikkerhetsloven § 4 nr. 3. Det er her snakk om både digitale og fysiske hendelser som kan virke inn på virksomhetens nettverk og informasjonssystemer og som kan virke inn på virksomhetens evne til å levere den samfunnsviktige tjenesten.

I forslag til punkt c pålegges tilbyder å beskrive hvilke sårbarheter som er tilknyttet virksomhetens nettverk og informasjonssystemer. En sårbarhet er alt som kan misbrukes av en som har til hensikt å angripe nettverk og informasjonssystemer, men det kan også være sårbarheter mot utilsiktede hendelser. Det kan være manglende sikkerhetsoppdateringer av nettverk og informasjonssystemer, eller det kan være svake krav til passord for innlogging.

Det kan også være en sårbarhet at nettverk og informasjonssystemer ikke er satt opp med alternative strømkilder i tilfelle strømbrudd.

I forslag til punkt d pålegges tilbyder å vurdere sannsynligheten for at en hendelse kan inntreffe. En sannsynlighetsvurdering kan være krevende å utarbeide, men det bør blant annet ses hen til virksomhetens betydning for leveransen av den samfunnsviktige tjenesten i Norge, erfaring og åpne trussel- og risikovurderinger utgitt av myndighetene. Dersom tilbyderen er en av få tilbydere av den samfunnsviktige tjenesten i landet, er dette relevant for vurderingen av om tilbyderen er et aktuelt mål for tilsiktede hendelser. Det kan også være relevant å se hen til hvor i landet virksomhetens nettverk og informasjonssystemer er lokalisert med tanke på de er lokalisert i område som er særlig utsatt for flom eller lignende.

Etter forslag til punkt e skal tilbyderen beskrive konsekvensen av hendelsen. Det er her snakk om å vurdere hvorvidt hendelsen vil skade, ødelegge, begrense eller på annen måte påvirke virksomhetens nettverk og informasjonssystemer og derigjennom leveransen av den samfunnsviktige tjenesten. Også her er det relevant å få med om tilbyderen er en sentral leverandør av den samfunnsviktige tjenesten slik at hendelsen får betydning for befolkningens generelle tilgang til tjenesten.

I forslag til punkt f pålegges tilbyderen å beskrive i hvilken grad virksomheten er avhengig av andre virksomheter for å fungere som den skal. Dette punktet har også betydning for sårbarhetsvurderingen. Dersom virksomheten er sterkt avhengig av en annen virksomhet for å fungere, kan dette representere en sårbarhet for virksomheten.

Departementet har vurdert om det bør tilføyes en bokstav g om at tilbyderen i risikovurderingen skal gi en oversikt over kriterier for risikoaksept og hvilke kompenserende tiltak som iverksettes for å redusere risikoen til et akseptabelt nivå. Det er i utgangspunktet fornuftige krav til en tilbydere at de har et bevisst forhold til hva som er akseptabel risiko og på hvilken måte en risiko kan reduseres til akseptabelt nivå. Samtidig erkjenner departementet at dette kan være unødvendig byrdefullt for virksomhetene. Forskriften skal angi et minimumsnivå for digital sikkerhet og skal kunne benyttes av flere virksomheter av ulike størrelse og karakter.

Det er virksomheten selv som, basert på risikovurderingen, skal vurdere hvilke sikkerhetstiltak som er tilstrekkelige for å ivareta digital sikkerhet. Departementet viser likevel til forslag til § 8 og § 9 og omtalen i punkt 0 som angir noen minstekrav og krav om begrunnelse dersom virksomheten ikke iverksetter disse minstekravene.

5.3.4 Risikohåndtering

Departementet foreslår at det i forskriften § 8 reguleres krav til risikohåndtering. Bestemmelsen er generelt utformet og viser til at sikkerhetstiltak for å håndtere den identifiserte risikoen minst skal bidra til sikker plattform, sikker drift og vedlikehold og sikker hendelseshåndtering og gjenoppretting. Etter departementets vurdering er sikkerhetstiltakene i forslag til §§ 9-14 dekkende for minimumsnivået av digital sikkerhet som forskriften skal ivareta. Samtidig er risikohåndtering en vesentlig del av et godt sikkerhetsarbeid. Innen denne tematikken finnes det en

rekke grunnprinsipper og anerkjente råd for forsvarlig sikkerhet, og departementet har vurdert om forskriften skal skrive disse ut noe nærmere.

Gitt at dette regelverket skal omfatte en rekke ulike virksomheter med ulike grad av behov for tiltak, har departementet etter en samlet vurdering kommet til at det er mer hensiktsmessig at sikkerhetstiltakene som foreslås i §§ 9-14 bør suppleres med veiledningsmateriale fra Nasjonal sikkerhetsmyndighet, som i kombinasjon med anerkjente standarder støtter virksomhetene i arbeidet. Departementet ber om høringsinstansenes syn på dette punktet.

5.3.5 Sikkerhetstiltak

5.3.5.1 *Organisatoriske sikkerhetstiltak*

Departementet foreslår i § 9 en bestemmelse om krav til organisatoriske sikkerhetstiltak og viser til at det i §§ 7 og 8 nevnes som en egen kategori sikkerhetstiltak. Bestemmelsen har som formål å sikre at tiltakene forankres i dokumentasjon ut over selve sikkerhetsstyringssystemet og gjøres tilgjengelig for relevant personell. Det er de personell med tilgang til virksomhetens nettverk og informasjonssystemer, eller personell som på annen måte kan påvirke sikkerheten i disse systemene, som utgjør førstelinja i virksomhetens sikkerhetsarbeid. Departementet ser det derfor som viktig å sikre at virksomheten utarbeider relevant materiale for dette personalet, men at omfanget må tilpasses størrelsen og kompleksiteten på virksomheten.

Etter forslag til første ledd skal tilbyder av samfunnsviktig tjeneste utarbeide skriftlige instrukser for rutiner og prosedyrer innenfor sikkerhet, herunder digital sikkerhet. Instruksene skal tilpasses størrelsen og kompleksiteten på virksomheten.

Etter forslag til andre ledd skal tilbyder ha oppdaterte lister over sikkerhetstiltak som kan iverksettes dersom risikoen endrer seg eller det oppstår en hendelse, jf. § 13.

Etter forslag til tredje ledd skal relevante instrukser, rutiner, prosedyrer og lister etter første og andre ledd skal gjøres kjent for personell som utfører oppgaver for eller på vegne av virksomheten og som kan få tilgang til virksomhetens nettverk og informasjonssystemer.

5.3.5.2 *Teknologiske sikkerhetstiltak*

Departementet foreslår at det i forskriften § 10 angis teknologiske sikkerhetstiltak. I forslag til § 11 foreslås det fysiske sikkerhetstiltak, se omtalen i punkt 5.3.5.3.

I forslag til § 10 første ledd foreslås det en bestemmelse om at tilbyder av samfunnsviktige tjenester skal, basert på risikovurderingen etter § 7, iverksette teknologiske sikkerhetstiltak som er tilpasset omfang, kompleksitet, driftsmiljø, brukermiljø, funksjon og risiko ved virksomhetens nettverk og informasjonssystemer. Tiltakene skal dokumenteres i sikkerhetsstyringssystemet, jf. forslag til § 6.

Det foreslås i andre ledd noen konkrete kategorier av sikkerhetstiltak som minst skal implementeres. Det foreslås krav om to- eller flerfaktorautentisering for adgang til nettverk og informasjonssystemer, tilgangskontroll til innholdet i nettverk og informasjonssystemer basert på tjenstlig behov, tiltak for segmentering av tjenester basert på et prinsipp om minste minimum av rettigheter, tiltak som

skal sikre håndtering av avbrudd og gjenoppretting, tiltak som skal sikre videreutvikling av nettverk og informasjonssystemer, oppdateringer samt overvåkning for avdekking av hendelser.

To- eller flerfaktorautentisering er et viktig tiltak for å redusere sårbarhet for at uvedkommende får tilgang til virksomhetens nettverk og informasjonssystemer, gjennom at det blir vanskeligere å få tilgang til alle passord som trengs for å komme inn i systemet. Tilgangskontroll basert på tjenstlig behov sørger for at personell kun får tilgang til de delene i virksomhetens nettverk og informasjonssystemer som de har behov for. Dette vil bidra til å redusere eventuelle risikoer knyttet til eget personell og/eller dersom innloggingsdetaljer fra en brukerkonto kommer på avveie.

Ved segmentering eller bruk av soner hvor det etableres tilgangsstyring inn og ut av segmenter plasseres de ulike tjenestene i egne segmenter. Tiltaket kan bidra til å hindre spredning av for eksempel virus internt på nettverket og redusere skadeomfanget. Det er også et tiltak som kan begrense bevegelsesmulighetene til en eventuell ekstern trussel hvor angriperne forsøker å bevege seg rundt i nettverket.

Tiltak for å håndtere avbrudd og gjenoppretting anses nødvendig for å sikre at virksomheten er forberedt på å håndtere eventuelle avbrudd som følge av en hendelse og er relevant for å sikre fortsatt leveranse av den samfunnsviktige tjenesten.

Tiltak for å sikre videreutvikling av nettverk og informasjonssystemer, herunder oppdateringer, er et viktig tiltak for å sørge for at nettverk og informasjonssystemer har implementert siste sikkerhetsoppdateringer.

Overvåkning av nettverk og informasjonssystem for å avdekke hendelser er viktig for å ha et godt kunnskapsgrunnlag for å avdekke og håndtere hendelser rettidig, men også til å analysere hendelser i etterkant.

Departementet understreker at det er her er snakk om *kategorier* av sikkerhetstiltak uten krav om metoden for implementering av tiltakskategorien. Det er for eksempel opp til virksomheten å vurdere på hvilken måte tilgangskontroll skal implementeres, så lenge det oppfyller forskriftens krav om at tilgang til nettverk og informasjonssystemer skal differensieres ut fra tjenstlig behov.

Departementet har vurdert om det i forskriften bør tas inn en bestemmelse som åpner for at dersom tilbyderen ikke kan gjennomføre et eller flere av kategoriene av tiltak, vil de kunne gjøre unntak dersom det begrunnes og dokumenteres. Bakgrunnen for unntaket er at virksomhetene og de digitale systemene som blir omfattet av regelverket er svært ulike og det er ikke gitt at det er mulig å implementere i alle system uten at de blir uforholdsmessig kostbare og dermed ikke proporsjonale opp mot risiko. Samtidig vil det være vanskelig å oppnå hensikten med regelverket dersom tiltakene etter forskriften ikke gjennomføres. Dessuten kan en slik bestemmelse bidra til at vi får et lavere sikkerhetsnivå enn det regelverket har som formål å oppnå.

På denne bakgrunnen foreslår ikke departementet en slik unntaksbestemmelse. Departementet vurderer likevel om det bør tas inn en bestemmelse som gir myndighetene kompetanse til å gi unntak fra enkelte krav og ber om høringsinstansenes syn på dette.

5.3.5.3 *Fysiske sikkerhetstiltak*

Departementet foreslår en egen bestemmelse i § 11 om fysiske sikkerhetstiltak. Hensikten med en slik bestemmelse er å sikre nettverk og informasjonssystemer mot fysiske hendelser. Hendelsesbegrepet etter loven og forskriften er kildenøytralt og skiller verken mellom tilsiktede og utilsiktete hendelser eller mellom fysiske eller digitale hendelser. Det er derfor viktig at tilbyderne har iverksatt tiltak for å sikre nettverk og informasjonssystemer fysisk.

I første ledd fastsettes plikten til å iverksette tiltak for fysisk sikkerhet for å opprettholde forsvarlig sikkerhet. Tiltakene skal dokumenteres i sikkerhetsstyringssystemet, jf. § 6.

I andre ledd foreslås det noen konkrete kategorier av sikkerhetstiltak som minst skal implementeres. I likhet med kategoriene etter § 9 inneholder ikke bestemmelsen krav til metode for implementering av tiltakene.

Det foreslås i andre ledd bokstav a tiltak for å forhindre at uvedkommende får tilgang til lokasjoner og fysisk og teknisk infrastruktur som nettverk og informasjonssystemer benytter eller er avhengige av. Det kan her være tale om adgangsbegrensninger i serverrom eller lignende.

I andre ledd bokstav b foreslås det at tilbyderen skal iverksette tiltak for å identifisere og beskytte bygninger, rom og tilstøtende områder som har betydning for sikkerhetsnivået til nettverk og informasjonssystemer som understøtter den samfunnsviktige tjenesten. Når det gjelder fysisk sikkerhet i datasentre, viser departementet til forslaget til ny ekomlov § 3-7, jf. Prop. 93 LS (2023–2024). Helhetlig sikring av datasentre vil ivaretas av forslagene i ny ekomlov og i enkelte tilfeller også gjennom sikkerhetslovens bestemmelser. Departementet understreker likevel at den enkelte virksomhet som omfattes av digitalsikkerhetsloven, må sørge for tilstrekkelig sikkerhet i egne verdikjeder, herunder datasentre som benyttes.

Det er viktig at tilbyderen har en oversikt over fysisk infrastruktur som nettverk og informasjonssystemer er avhengige av og lokalisert i. Dernest må sårbarhetene disse kan utgjøre identifiseres. Det kan være sårbarheter i form av nærhet til områder som er flomutsatt, nærhet til andre som lett kan få tilgang til områdene med videre. Disse sårbarhetene må håndteres, for eksempel i form av forsterkede dører, vegger eller lignende.

Etter andre ledd bokstav c foreslås det tiltak for å ivareta eksterne avhengigheter i nettverk og informasjonssystemer, herunder datakommunikasjon og strømtilførsel. Slike tiltak skal ha som formål at tilbyderen sikrer fortsatt leveranse av den samfunnviktige tjenesten selv om det oppstår svikt eller brudd i eksterne innsatsfaktorer Det kan her være snakk om at tilbyderen iverksetter tilstrekkelige tiltak for å opprettholde tjenesten i form av tilstrekkelig strømtilførsel, eventuelt nødtilførsel av strøm, samt robuste nettverkstilganger.

5.3.5.4 *Sikkerhetstiltak for personell*

Departementet foreslår en egen bestemmelse om sikkerhetstiltak for personell i § 12. Departementet bemerker at det her ikke er snakk om tiltak for personellsikkerhet etter sikkerhetsloven kapittel 8. For tilbydere som er omfattet av sikkerhetsloven er det sikkerhetslovens bestemmelser som vil gjelde.

Departementet foreslår i første ledd at tilbyderen skal iverksette nødvendige sikkerhetstiltak for ansatte, leverandører og oppdragstakere som kan få tilgang til virksomhetens nettverk og informasjonssystemer. Bestemmelsen er ment å omfatte bruk av underleverandører. Departementet understreker at pliktene etter loven og forskriften påhviler tilbyderen av en samfunnsviktig tjeneste. Ved bruk av underleverandører er det tilbyderen som har plikt til å påse at leverandøren overholder de nødvendige krav til digital sikkerhet, se nærmere om dette i punkt 5.3.7.

På samme måte som etter §§ 10 og 11, foreslås det kategorier av tiltak som tilbyderen minst skal implementere: adgangskontroll, brukerautentisering og tilgangskontroll. Adgangskontroll handler om adgang til både den fysiske og digitale infrastrukturen til nettverk og informasjonssystem. Med brukerautentisering menes at de enkelte brukerne skal bekrefte sin identitet når de går fysisk eller digitalt inn i nettverk og informasjonssystemer. Tilgangskontroll handler om å differensiere tilgangen til nettverk og informasjonssystemer basert på tjenstlig behov.

I forslag til tredje ledd foreslår det en bestemmelse som handler om kunnskaps- og kompetansebygging og opplæring. Det foreslås en plikt for tilbyder til å sikre at personell som kan få tilgang til virksomhetens nettverk og informasjonssystemer kjenner til sikkerhetstiltak som er relevante for oppgavene deres. Departementet mener at det er viktig at sikkerhetstiltak er kjent for hele organisasjonen, og spesielt de delene som har betydning for oppgavene til enkeltpersoner og at de er kjent med egen rolle i sikkerhetsarbeidet. Det foreslås også at tilbyderen sørger for at nevnte personell har tilstrekkelig kompetanse om digital sikkerhet og gis nødvendig opplæring ved behov. Plikten er løpende og betyr at oppfriskningskurs og vedlikehold av kompetanse kan være nødvendig.

Det foreslås i fjerde ledd en bestemmelse som skal sikre at tilbyderen sørger for å fjerne tilgangen til virksomhetens nettverk og informasjonssystemer når arbeids- eller tjenesteforholdet er avsluttet. Departementet har vurdert om det er i tillegg bør være krav om at personell som ikke lenger er tilknyttet virksomheten skal ha en form for taushetsplikt, men har gått bort fra et konkret krav om dette. Departementet antar at en del virksomheter opererer med en form for taushetsplikt eller konfidensialitetserklæringer og anser at det ikke er behov for et eksplisitt krav om dette.

5.3.6 Hendelseshåndtering og beredskap

Departementet foreslår en egen bestemmelse om hendelseshåndtering og beredskap i § 13. Etter første ledd første punktum foreslås det fastsatt en plikt til å ha en beredskapsplan for håndtering av hendelser og varsling etter § 17. Bestemmelsen utfyller kravene i § 14 om varsling. Formålet med bestemmelsen er å sikre at tilbyderen på forhånd har etablert interne rutiner for håndtering av hendelser og varsling ut over loven og forskriftens krav. I en beredskapsplan vil det for eksempel kunne være aktuelt å beskrive hvilke beredskapstiltak som skal iverksettes ved en hendelse.

I første ledd andre punktum foreslås det at tilbyder plikter å vurdere relevante beredskapstiltak eller påbygningstiltak som kan iverksettes ved behov. Formålet med bestemmelsen er å sørge for at tilbydere har et forhåndsvurdert sett med tiltak som kan iverksettes når det oppstår en hendelse. Med påbygningstiltak menes at

det som følge av en hendelse kan være aktuelt å forsterke tiltak. For eksempel kan det være aktuelt å ytterligere begrense kretsen av personer som skal ha tilgang til nettverk og informasjonssystemer under håndteringen.

I andre ledd er det beskrevet hva tilbyderen skal gjøre dersom virksomheten blir utsatt for en hendelse. Hendelsens karakter og omfang skal identifiseres, og tilbyderen skal iverksette nødvendige mottiltak og tiltak for å gjenopprette den sikre tilstanden i nettverk og informasjonssystemer. Med mottiltak menes tiltak for å forsvare seg mot hendelsen gjennom avverging eller redusering av skade, og med tiltak for å gjenopprette den sikre tilstanden menes tiltak som skal reparere skaden som eventuelt har skjedd.

I tredje ledd foreslås det at tilbyderen skal utarbeide, vedlikeholde og dokumentere beredskapsplaner og gjennomføre øvelser for å teste planverket og utvikle virksomhetens kompetanse til å håndtere hendelser. Det foreslås også at øvelser gjennomføres i samarbeid med underleverandører eller andre som utfører arbeid på vegne av virksomheten dersom det er relevant. Etter departementets vurdering er øvelser et sentralt tiltak for kompetanse- og erfaringsbygging og til å avdekke behov for endringer i implementerte tiltak. Øvelser vil kunne bidra til å styrke virksomhetens evne til å motstå og håndtere hendelser. Dessuten er øvelser en påminnelse om viktigheten av digital sikkerhet.

5.3.7 Oppfølgingsplikt

Departementet foreslår i § 14 en bestemmelse som regulerer tilbyderens bruk av leverandører og oppdragstaker. Etter forslag til første ledd foreslås det at tilbyder av samfunnsviktig tjeneste skal påse at leverandører og andre som utfører arbeid som kan påvirke sikkerheten i nettverk og informasjonssystemer og som utfører arbeid for eller på vegne av virksomheten, utfører arbeidet på en måte som gjør at virksomhetens krav til forsvarlig sikkerhet overholdes. Formålet med bestemmelsen er å tydeliggjøre at kravene til forsvarlig sikkerhetsnivå også gjelder ved bruk av leverandører, innleid personell, konsulenter med videre.

I forslag til andre ledd foreslås det presisert at tilbyder av samfunnsviktig tjeneste skal gjøre sikkerhetstiltakene gjeldende overfor leverandører som kan påvirke nettverk og informasjonssystemer, i den grad det er nødvendig for å opprettholde et forsvarlig sikkerhetsnivå. Formålet med bestemmelsen er å konkret angi at tilbyderen gjennom avtalevilkår og lignende fastsetter konkrete krav til sikkerhet som er nødvendig for at tilbyderens bruk av leverandører er i tråd med tilbyderens egne krav til sikkerhet. Departementet legger til grunn at flere virksomheter som blir omfattet av regelverket vil benytte underleverandører som ikke selv er underlagt digitalsikkerhetsloven, men som leverer tjenester som har betydning for sikkerheten i nettverk og informasjonssystemer og leveransen av den samfunnviktige tjenesten. Dette innebærer en sårbarhet som må håndteres og bestemmelsen er ment å ivareta det.

Det fremgår av NIS1-direktivets fortalepunkt 52 at varslingskravene skal gjelde uavhengig av om tilbyder har satt bort oppgavene med vedlikehold av nettverk og informasjonssystem til andre eller utfører det selv. De hemmelige tjenestene har i sine nasjonale risikovurderinger pekt på at lange og uoversiktlige leverandørkjeder fortsatt utgjør en sårbarhet som trusselaktører vet å utnytte. De siste årene har vi sett mange eksempler på at leverandørkjedeangrep mot leverandører av IKT-tjenester med svært store kundebaser får omfattende konsekvenser. Krav til

varsling og sikkerhet gjelder for tilbyder av samfunnsviktig tjeneste og tilbyder av digital tjeneste uavhengig av om drift og vedlikehold av tjenesten er satt bort til andre, for eksempel en underleverandør. I disse tilfellene påhviler det tilbyder et særskilt ansvar for å følge opp underleverandør.

Departementet mener på denne bakgrunn at det er behov for regelverk som stiller krav om å følge opp egne underleverandører og ha oversikt over kjeden av leverandører og andre kontraktører. Ved gjennomføring av tilsyn vil myndigheten kunne ha behov for å gjøre undersøkelser opp mot underleverandører. Departementet foreslår derfor i § 22 at tilsynsmyndigheten skal kunne kreve opplysninger fra tilbyder, leverandør og andre som utfører arbeid for eller på vegne av tilbyder, se mer om dette i punkt 9.3.

6 Krav til sikkerhet for tilbydere av digitale tjenester

6.1 Gjeldende rett

Digitalsikkerhetsloven § 10 setter krav til sikkerhet for tilbydere av digitale tjenester. Som tilbyder av en digital tjeneste regnes virksomheter som tilbyr tjenester som definert i ehandelsloven § 1 andre ledd bokstav a og b i form av nettbaserte markedsplasser, nettbaserte søkemotorer eller skytjenester, jf. digitalsikkerhetsloven § 9 første ledd. Etter første ledd skal tilbyder av en digital tjeneste gjennomføre en risikovurdering av nettverk og informasjonssystemer som benyttes for å levere tjenesten. Etter andre ledd skal tilbyderen iverksette hensiktsmessige og proporsjonale tekniske og organisatoriske sikkerhetstiltak som samlet skal sørge for et sikkerhetsnivå som er tilpasset risikoen. For tilbydere av digitale tjenester er, i tråd med direktivet, momenter som skal hensyntas konkretisert i digitalsikkerhetsloven § 10 andre ledd bokstav a til e. Ved vurderingen av hva som er et forsvarlig sikkerhetsnivå, skal det blant annet ses hen til den teknologiske utviklingen og tas hensyn til sikkerheten i systemer, utstyr og anlegg, hendelseshåndtering, styring av opprettholdelse av tjenesteleveransen, overvåking, revisjon og testing, og anerkjente internasjonale standarder. Etter tredje ledd skal tilbyderen iverksette proporsjonale tiltak for å forebygge, avdekke og redusere konsekvensene av hendelser, slik at tjenesteleveransen kan opprettholdes.

Kravene som stilles til tilbydere av digitale tjenester er ytterligere konkretisert i gjennomføringsforordningen.

6.2 Gjennomføringsforordningen

EU-kommisjonens gjennomføringsforordning (EU) 2018/151 viser til NIS1-direktivet artikkel 16 nr. 8 om at Kommisjonen skal vedta gjennomføringsrettsakter for å angi nærmere elementene som er nevnt i nr. 1 (sikkerhetskrav) og parametrene som er oppført i nr. 4 (melding om hendelser) i denne artikkel. Gjennomføringsforordningen ble vedtatt 30. januar 2018 og trådte i kraft 10. mai 2018. Denne gjelder kun for tilbydere av digitale tjenester. Artikkel 2 i forordningen spesifiserer hvilke momenter som skal tas i betraktning når det fastsettes og iverksettes tiltak for å garantere et nivå av sikkerhet i nettverk og informasjonssystemer som benyttes i leveransen av tjenester som nevnt i NIS1-direktivet vedlegg III.

Der NIS1-direktivet omtaler sikkerheten i systemer og utstyr i artikkel 16 nr. 1 bokstav a, presiserer forordningen at dette innebærer systematisk forvaltning av nettverk og informasjonssystemer, fysisk og miljømessig sikkerhet, forsyningssikkerhet og adgangskontroll, jf. artikkel 2 nr. 1.

Der NIS1-direktivet omtaler hendelseshåndtering i artikkel 16 nr. 1 bokstav b, presiserer forordningen at det omfatter tiltak som innebærer opprettholdelse og overvåkning av deteksjonsprosesser, prosesser og retningslinjer for rapportering om hendelser, plan for reaksjon på hendelser og vurdering av hendelsenes alvorlighetsgrad, jf. artikkel 2 nr. 2.

I NIS1-direktivet artikkel 16 nr. 1 bokstav c omtales håndtering av kontinuitet for tilbydere av digitale tjenester. Ifølge gjennomføringsforordningen artikkel 2 nr. 3 innebærer dette utarbeidelse av beredskapsplanverk og å opprettholde en katastrofeberedskapskapasitet som vurderes og testes jevnlig.

I NIS1-direktivet artikkel 16 nr. 1 bokstav d omtales overvåkning, revisjon og testing. Det presiseres i gjennomføringsforordningen artikkel 2 nr. 4 at dette innebærer å gjennomføre planlagte sekvenser for observasjon og målinger, inspeksjoner for å sjekke om retningslinjer etterleves og en prosess for å avdekke mangler i systemers sikkerhetsmekanismer.

I NIS1-direktivet artikkel 16 nr. 1 bokstav e vises det til at det skal tas hensyn til overholdelse av anerkjente internasjonale standarder. Ifølge gjennomføringsforordningen artikkel 2 nr. 5 innebærer dette standarder vedtatt av et internasjonalt standardiseringsorgan etter Europaparlamentets og Rådets forordning (EU) 1025/2012. Etter NIS1-direktivets artikkel 19 kan det også benyttes andre standarder som er relevante for sikkerheten, herunder også nasjonale.

Gjennomføringsforordningen artikkel 2 nr. 6 stiller krav om at tilbyderne skal kunne fremlegge dokumentasjon om overnevnte som den kompetente myndighet etter NIS1-direktivet trenger for å utøve sin kontroll.

Det følger av direktivets fortalepunkt 49 at det skal stilles mindre strenge sikkerhetskrav til tilbydere av digitale tjenester enn til tilbydere av samfunnsviktige tjenester. Videre fremgår det at tilbydere av digitale tjenester, på grunn av sin tverrnasjonale karakter, bør være underlagt en mer harmonisert tilnærming i EU.

6.3 Departementets vurderinger og forslag

Siden gjennomføringsforordningen er en forordning, må den som helhet tas inn i nasjonal rett. Departementet foreslår derfor en bestemmelse i § 15 «Tiltak for sikkerhetsstyring for tilbydere av digitale tjenester og kriterier for å avgjøre om en hendelse skal anses for å ha betydelig innvirkning» som angir at forordningen gjelder som forskrift. En nærmere presisering av sikkerhetskravene for tilbydere av digitale tjenester fremgår av forordningen, og følger som vedlegg til denne høringen.

7 Responsmiljøer

7.1 Gjeldende rett

Etter NIS1-direktivet artikkel 9 skal hver stat utpeke en eller flere nasjonale responsmiljøer som skal oppfylle kravene som følger av direktivet vedlegg I. Responsmiljøet skal blant annet overvåke hendelser på nasjonalt nivå, respondere på hendelser, bidra med analyser og situasjonsforståelse og delta i nettverket av responsmiljøer som er etablert av direktivet.

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

Nasjonal sikkerhetsmyndighet har etter sikkerhetsloven § 2-4, jf. virksomhetsikkerhetsforskriften § 63, ansvar for å drive en nasjonal responsfunksjon for alvorlige digitale angrep og et nasjonalt varslingssystem for digital infrastruktur. Nasjonal sikkerhetsmyndighet er også nasjonalt fagmiljø for digital sikkerhet og understøtter Justis- og beredskapsdepartementet og Forsvarsdepartementet på det digitale sikkerhetsområdet, herunder har de ansvaret for nasjonal håndtering av digitale hendelser.

I tillegg er det etablert et system med sektorvise responsmiljøer nasjonalt, se blant annet Meld. St. 38 (2016–2017), jf. Innst. 187 S (2017–2018) og *Rammeverk for håndtering av IKT-sikkerhet* utgitt av Nasjonal sikkerhetsmyndighet.

7.2 Departementets vurderinger og forslag

Departementer foreslår at forskriften § 16 regulerer responsmiljøer. I forslag til første ledd fastsettes det at Nasjonal sikkerhetsmyndighet er nasjonalt responsmiljø for håndtering av hendelser etter digitalsikkerhetsloven. Det nasjonale responsmiljøet skal ha en overordnet nasjonal oversikt over håndtering av hendelser, koordinere håndtering på nasjonalt nivå og der det er nødvendig for å ivareta nasjonale interesser, bistå eventuelle sektorvise responsmiljøer eller i håndtering av alvorlige hendelser av nasjonal betydning.

Etter forslag til andre ledd kan ansvarlig departement utpeke sektorvise responsmiljøer som kan bistå tilbyder med å håndtere hendelser innenfor energi, transport, helse, vannforsyning, bank, finansmarkedsinfrastruktur og digital infrastruktur. Nasjonal sikkerhetsmyndighet skal orienteres om utpekingen.

Forslaget er i tråd med gjeldende prinsipper innen digital sikkerhet, der Nasjonal sikkerhetsmyndighet er nasjonalt hendelseshåndteringsmiljø og fagmyndighet for digital sikkerhet, samtidig som flere sektorer har etablert egne responsmiljøer.

Etter forslag til tredje ledd skal et responsmiljø for håndtering av hendelser etter digitalsikkerhetsloven som et minimum oppfylle krav som følger av vedlegg I til NIS1-direktivet og overholde relevante krav som følger i eller i medhold av digitalsikkerhetsloven. Etter departementets vurdering vil det kunne være behov for at de sektorvise responsmiljøene overholder en del av de samme kravene som stilles til tilbydere av samfunnsviktige tjenester, herunder sikkerhetstiltak. Forslag til bestemmelse er ment å oppstille et krav om at også responsmiljøene har et minimumsnivå av sikkerhet i sine nettverk og informasjonssystemer. Departementet vurderer at det vil være opp til tilbyderne og responsmiljøene å implementere dette gjennom avtale eller egenoppfylling av relevante krav.

8 Varsling om hendelser

8.1 Gjeldende rett

I digitalsikkerhetsloven §§ 8 og 11 oppstilles krav om varsling for tilbydere av samfunnsviktige tjenester og tilbydere av digitale tjenester. Tilbyderen skal, uten unødig opphold og uten hinder av taushetsplikt, varsle om hendelser som virker betydelig inn på tjenesteleveransen.

Hva som utgjør en «hendelse» i lovens forstand er definert i § 4 nr. 3. Varslingsplikten etter loven gjelder ikke for enhver hendelse som virker betydelig inn på opprettholdelsen av tjenesteleveransen, men avgrenses til hendelser med negativ virkning på sikkerheten i nettverk og informasjonssystemer. Årsaken til hendelsen er uten betydning.

I §§ 8 og 11 andre punktum angis momenter som skal vektlegges ved vurderingen av om innvirkningen er betydelig. Det skal legges vekt på antall brukere som påvirkes, hendelsens varighet og størrelsen på det geografiske området som berøres av hendelsen. For tilbydere av digitale tjenester skal det i tillegg legges vekt på omfanget av funksjonalitetssvikten i tjenesten og omfanget av innvirkningen på økonomisk og samfunnsmessig aktivitet.

8.2 Direktivet og gjennomføringsforordningen

Etter artikkel 14 nr. 3 og 16 nr. 3 skal varselet inneholde nok opplysninger til at det kan fastslås om hendelsen har virkninger utover landets grenser. Varsling av hendelser skal ikke medføre utvidet ansvar for tilbyder av tjenesten.

For samfunnsviktige tjenester følger det av fortalepunkt 47 at kompetente myndigheter skal kunne utstede nasjonale retningslinjer om når og på hvilken måte hendelser skal varsles. Det fremgår av fortalepunkt 58 at direktivet ikke utelukker statene fra å stille krav om sikkerhet og varsling til virksomheter som ikke faller inn under direktivets definisjon av tilbydere av digitale tjenester.

Direktivet slår fast i artikkel 16 nr. 1 at det ikke skal innføres ytterligere varslingskrav for digitale tjenester enn det som følger av direktivet. Det er derfor ikke noe nasjonalt handlingsrom hva gjelder varslingskrav, med unntak av de føringer som er gitt i artikkel 1 nr. 6, jf. artikkel 16 nr. 10. Dette har blant annet sammenheng med at aktiviteten er grenseoverskridende av natur, se fortalepunkt 57.

I gjennomføringsforordningen artikkel 3 og 4 er kriteriene for å avgjøre om en hendelse har betydelig innvirkning nærmere spesifisert, jf. direktivet artikkel 16 nr. 4, og som er reflektert i digitalsikkerhetsloven § 11.

Etter NIS1-direktivet artikkel 16 nr. 4 bokstav a skal det tas hensyn til antall berørte brukere som påvirkes av hendelsen, særlig brukere som er avhengige av tjenesten for å kunne yte egne tjenester. Etter gjennomføringsforordningen artikkel 3 nr. 1 bokstav a og b skal tilbydere av digitale tjenester kunne fastslå enten antallet av berørte fysiske og juridiske personer som det er inngått avtale om levering av tjeneste med, eller antallet berørte brukere som har benyttet tjenesten basert på tidligere trafikkdata.

Gjennomføringsforordningen presiserer i artikkel 3 nr. 2 hva som mener med en hendelses «varighet» i NIS1-direktivet artikkel 16 nr. 4 bokstav b. Med hendelsens

varighet skal det legges til grunn tiden fra avbrytelse av tjenesteleveranse når det gjelder tilgjengelighet, autentisitet eller fortrolighet, til det tidspunkt hvor tjenesten er gjenopprettet.

Artikkel 3 nr. 3 presiserer at ved avgjørelse av hendelsens geografiske omfang, jf. NIS1-direktivet artikkel 16 nr. 4 bokstav c, må tilbyderne være i stand til å fastslå om hendelsen påvirker leveransen av tjenester i bestemte EU-land.

Når det gjelder omfanget av driftsforstyrrelser etter NIS1-direktivet artikkel 16 nr. 4 bokstav d, presiserer gjennomføringsforordningen artikkel 3 nr. 4 at dette skal måles basert på om en eller flere av følgende egenskaper svekkes som følge av en hendelse: dataenes eller dermed tilknyttede tjenesters tilgjengelighet, autentisitet, integritet eller konfidensialitet.

Gjennomføringsforordningen artikkel 3 nr. 5 gjelder omfanget av innvirkningen på økonomisk og samfunnsmessig aktivitet, jf. direktivet artikkel 16 nr. 4 bokstav e. Tilbydere av digitale tjenester skal kunne avgjøre om hendelsen har medført betydelige materielle eller ikke-materielle tap for brukerne, for eksempel med hensyn til helse, sikkerhet eller skade på eiendom.

Artikkel 3 nr. 6 slår fast at tilbydere av digitale tjenester ikke er forpliktet til å innsamle informasjon om overstående som de ikke har tilgang til.

Gjennomføringsforordningen artikkel 4 nr. 1 inneholder kriterier for å fastslå når en hendelse har betydelig innvirkning, jf. direktivet artikkel 16 nr. 4. En hendelse anses for at ha betydelige betydelig innvirkning hvis den har medført minst en av følgene situasjoner:

- tjenesten er utilgjengelig i over 5 000 000 brukertimer. Med brukertimer menes antallet berørte brukere i EU i en periode på 60 minutter
- hendelsen har ført til tap av integritet, autentisitet eller konfidensialitet i forbindelse med lagrede, overførte eller behandlede data og som er tilknyttet tjenester som tilbys av tilbyderen eller er tilgjengelige via tilbyderens nettverk og informasjonssystem, og tapet berører mere enn 100 000 brukere i EU
- hendelsen har medført risiko for offentlig sikkerhet eller tap av menneskeliv
- hendelsen har forårsaket materielle skader på over 1 000 000 euro for minst én bruker i EU

8.3 Varslingskrav i Sverige

I Sverige er det i lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster §§ 18 og 19 «utan onödigt dröjsmål». Tidspunktet for varsling er videre spesifisert i föreskrifter och allmänna råd om rapportering av incidenter för leverantörer av samhällsviktiga tjänster (MSBFS 2018:9) kapittel 2 og i föreskrifter och allmänna råd om rapportering av incidenter för leverantörer av digitala tjänster (MSBFS 2018:10) § 7. Første varslingstid er angitt til senest seks timer fra tilbyder har identifisert en rapporteringspliktig hendelse, neste er innen 24 timer og siste er senest fire uker fra hendelsestidspunktet. Tiden for varsling er differensiert utfra hvilke opplysninger som samtidig skal inngis. Ved første rapportering (innen 6 timer) skal tilbyder opplyse om tilbyders navn og kontaktperson, berørt tjeneste, informasjon om ekstern aktør dersom tjenesten er

satt ut, beskrivelse av hendelsen og beskrivelse av konsekvenser, også i andre EU-land.

Tilbyder av samfunnsviktige tjenester skal i tillegg rapportere om konsekvenser for andre enn brukere av tjenesten. Innen 24 timer skal det rapporteres om tiltak for å minimere konsekvensene av hendelsen. Innen 4 uker skal varselet oppdateres og kompletteres med opplysninger om tidligere iverksatte og nye tiltak for å forebygge og motvirke lignende hendelser.

For samfunnsviktige tjenester er det spesifisert hvilke hendelser som skal anses som rapporteringspliktige innen hver sektor. For eksempel omfattes hendelser innen sektoren transport som har pågått i minst en time og kan antas å påvirke minst 1000 brukere i et sammenhengende geografisk område på minst 10 000 km2, eller har pågått i minst 2 timer.

8.4 Varslingsreglene i NIS2-direktivet

Sammenlignet med NIS1-direktivet innfører NIS2 -direktivet mer presise bestemmelser om varsling av hendelser, herunder hva det skal varsles om og når. Etter NIS 2-direktivet artikkel 23 skal først et tidlig varsel inngis uten unødig opphold, men ikke senere enn 24 timer. Dersom informasjonen er tilgjengelig, skal varselet indikere hvorvidt hendelsen mistenkes å være forårsaket av ulovlige eller villede handlinger eller kan ha grenseoverskridende virkninger. Innen 72 timer skal varselet oppdateres og gi en innledende vurdering av hendelsen, herunder alvorlighetsgrad og virkninger, samt indikatorene for kompromittering. I begge tilfeller forutsettes det at informasjonen er tilgjengelig for avsender. Det forutsettes at informasjonen er tilgjengelig for avsender. Etter påkrav skal det kunne gis en foreløpig rapport om relevante statusoppdateringer. Etter fortalepunkt 102 skal forpliktelsen til å varsle ikke gå på bekostning av hendelseshåndtering.

Senest en måned etter første varsel skal det leveres en endelig rapport som skal inneholde en detaljert beskrivelse av hendelsen, inkludert alvorlighet og virkning, type trussel eller rotårsak som sannsynlig har forårsaket hendelsen, innførte og pågående avhjelpende tiltak og, dersom det er aktuelt, grenseoverskridende virkninger av hendelsen.

Blant annet skal varselet inneholde tilstrekkelig informasjon til at mottaker kan fastslå om hendelsen har konsekvenser i andre land. Tilsvarende som i NIS1-direktivet, skal varsling av hendelser ikke medføre utvidet ansvar for enheten som skal varsle.

8.5 Departementets vurderinger og forslag

Departementet foreslår at forskriften § 17 regulerer varslingsplikt. Etter forslag til første ledd første punktum skal varselet gå til tilsynsmyndigheten med kopi til Nasjonal sikkerhetsmyndighet. Varsel skal etter andre punktum gis senest innen 24 timer etter at tilbyder fikk kjennskap til hendelsen. Det er viktig for dem som omfattes av regelverket at det fremgår tydelig hvem det skal varsles til og hvilke tidsfrister som gjelder. Lovens utgangspunkt er at det skal varsles uten unødig opphold, jf. §§ 8 og 11. Absolutte tidsfrister kan bidra til forutberegnelighet både for varsler og mottaker. Konsekvensene av en hendelse kan være like uavhengig av hvilken sektor det er snakk om, og fristene bør derfor ikke være sektorspesifikke. Som redegjort for over, innføres det i NIS 2-direktivet flere

absolutte frister for varsling. I den utstrekning det bør fastsettes absolutte frister, er det departementets vurdering at det bør ses hen til hva som trolig blir den fremtidige ordningen. Også i Sverige er det fastsatt flere absolutte frister, se omtalen over. Tidsfristen bidrar til at relevante myndigheter blir raskt kjent med hendelser, både for å vurdere om det er behov for tiltak og for å identifisere om hendelsen har betydning i et nasjonalt perspektiv.

Når det gjelder innholdet i varselet foreslås det at varselet skal inneholde informasjon om tilbyders navn og kontaktinformasjon, berørt tjeneste, hendelsen, herunder mulige årsaker og konsekvenser, antall berørte brukere og virkninger i andre land.

I andre ledd foreslås det at tilbyderen skal oppdatere varselet innen 72 timer. Hensikten med denne bestemmelsen er at det erfaringsmessig skjer mye i løpet av den første tiden etter en hendelse og det vil være behov for at relevante myndigheter får ny relevant informasjon, eventuelt at informasjonen i første tidlige varsel stadfestes, noe som har betydning for videre håndtering.

I tredje ledd foreslås det at tilbyder skal utarbeide en fullstendig hendelsesrapport innen en måned fra første varsel. Hendelsesrapporten skal inneholde oppdatert informasjon om punktene som skal gis i det første tidlige varselet og suppleres med opplysninger om iverksatte og planlagte avhjelpende tiltak. Hendelsesrapporten skal inneholde en detaljert beskrivelse av hendelsen, inkludert alvorlighet og virkning, type trussel eller rotårsak som sannsynlig har forårsaket hendelsen, avhjelpende tiltak og grenseoverskridende virkninger av hendelsen. En slik fullstendig hendelsesrapport er nyttig både for generell læring og for videreutvikling av det nasjonale arbeidet med digital sikkerhet.

I Prop. 109 LS (2022–2023) side 39 forutsettes det at tidspunkt for varsling, kravene til det nærmere innholdet i varselet og begrensningene i varslingsplikten for tilbydere av digitale tjenester vil bli angitt i forskrift, jf. § 18 bokstav a. Som det fremgår av NIS1-direktivet artikkel 14 nr. 3 og 16 nr. 3 skal varselet inneholde nok opplysninger til at det kan fastslås om hendelsen har virkninger utover landets grenser. Varsling av hendelser skal ikke medføre utvidet ansvar for den som tilbyr tjenesten.

For tilbydere av digitale tjenester skal det ikke innføres ytterligere varslingskrav enn det som følger av direktivet. I tillegg er det for tilbydere av digitale tjenester i gjennomføringsforordningen fastlagt kriterier for å avgjøre om en hendelse har betydelig innvirkning. Tilsvarende begrensninger gjelder ikke for samfunnsviktige tjenester.

Kriteriene som gjelder for både for tilbydere av digitale tjenester og samfunnsviktige tjenester for å avgjøre om innvirkningen av en hendelse er betydelig (digitalsikkerhetsloven §§ 6 og 11) forutsetter at tilbyder har kjennskap til antall berørte brukere, hendelsens varighet og berørt geografisk område. For tilbydere av digitale tjenester forutsettes det i tillegg at funksjonalitetssvikten og konsekvensene for økonomisk og samfunnsmessig aktivitet er kjent. Varselet kan derfor inneholde informasjon om disse punktene, jf. forslaget i tredje ledd andre setning.

Det foreslås i fjerde ledd at varslingsorganet kan, uavhengig av fristene, kreve statusoppdateringer fra tilbyder og ellers de opplysningene som er nødvendig for å fastslå virkningen av hendelsen i andre land.

9 Tilsyn

9.1 Gjeldende rett

Digitalsikkerhetsloven gir i §§ 13 til 15 bestemmelser om tilsyn. Den nærmere gjennomføringen av tilsynet, og eventuelle begrensninger av tilsynet med tilbydere av digitale tjenester, jf. § 18 bokstav b, er forutsatt regulert i forskriften.

I loven § 14 stilles det krav til tilbyderne om opplysningsplikt og å gi tilgang til lokaler og utstyr i forbindelse med tilsyn. Bestemmelsen gjennomfører NIS1-direktivet artikkel 15 nr. 1 og 2 og artikkel 17 nr. 1 og 2. Tilbyderne skal gi tilsynsmyndigheten de opplysninger den krever for å utføre sine oppgaver og gi tilgang til virksomhetens lokaler og utstyr og yte nødvendig bistand ved tilsynsmyndighetens undersøkelser. Opplysningsplikten og medvirkningsplikten gjelder uten hinder av lovbestemt taushetsplikt.

I loven § 15 gis tilsynsmyndigheten hjemmel til å gi pålegg om retting. Bestemmelsen gjennomfører NIS1-direktivet artikkel 15 nr. 3. Ved overtredelse av bestemmelser gitt i eller i medhold av loven kan tilsynsmyndigheten gi tilbydere pålegg om at forholdet skal bringes i orden. Tilsynsmyndigheten skal sette en frist for oppfyllelse av pålegget.

9.2 NIS1-direktivet

I henhold til direktivet artikkel 8 skal hvert medlemsland utpeke en eller flere myndigheter som skal føre tilsyn med anvendelsen av direktivet på nasjonalt nivå. Direktivet åpner for at eksisterende myndighetsstruktur kan benyttes, jf. fortalepunkt 37.

Videre oppstiller NIS1-direktivet ulike regler for tilsyn med tilbydere av samfunnsviktige tjenester og tilbydere av digitale tjenester. Direktivets fortalepunkt 60 legger til grunn at tilsynsmyndigheter kun skal føre reaktive, hendelsesbaserte tilsyn med tilbydere av digitale tjenester, eller når tilsynsmyndigheten blir kjent med at tilbyderen av digitale tjenester ikke etterlever kravene som følger av direktivet. For tilbydere av samfunnsviktige tjenester skal tilsynsmyndigheten føre både forebyggende og reaktive tilsyn. Direktivets fortalepunkt 49 utdyper at tilbydere av samfunnsviktige tjenester gjerne er utsatt for større risiko enn tilbydere av digitale tjenester, gitt deres betydning for andre viktige funksjoner i samfunnet. Dette er noe av bakgrunnen for ulike tilsynsregimer.

Artikkel 15 regulerer tilsyn med tilbydere av samfunnsviktige tjenester. Tilsynsmyndigheten skal gis hjemmel til å innhente nødvendige opplysninger for å kunne utføre tilsynet.

Tilsyn med tilbydere av digitale tjenester reguleres av artikkel 17. Tilsyn kan kun utføres dersom det foreligger dokumentasjon på at en tilbyder av digitale tjenester ikke oppfyller direktivets krav. Det er med andre ord kun adgang til å gjennomføre etterfølgende tilsyn. Etter artikkel 17 skal statene sørge for at den kompetente myndigheten kan agere dersom det er bevist at en tilbyder av digitale tjenester ikke har overholdt kravene til varsling i artikkel 16. Dette innebærer blant annet at myndigheten skal kunne få tilgang til all den informasjonen som er nødvendig for å vurdere sikkerhetsnivået hos tilbyderen og kunne kreve retting av ethvert brudd på artikkel 16.

Medlemsstatene skal sørge for at tilsynsmyndigheten kan kreve at tilbyderen gir nødvendige opplysninger for å kunne vurdere sikkerheten i nettverkene og informasjonssystemene. I følge fortalepunkt 60 kan relevant informasjon om overtredelse 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.

Artikkel 2 nr. 6 bestemmer at tilbydere av digitale tjenester skal dokumentere oppfyllelse av sikkerhetskravene i art. 2 og fremvise dette til tilsynsmyndigheten.

9.3 Departementets vurderinger og forslag

9.3.1 Tilsyn, opplysningsplikt og tilgang til lokaler

Departementet foreslår at forskriften § 20 regulerer tilsyn med tilbydere omfattet av digitalsikkerhetsloven. Det foreslås i første ledd at ansvarlig departement utpeker tilsynsmyndighet innenfor egen sektor og at Nasjonal sikkerhetsmyndighet er tilsynsmyndighet for virksomhet uten sektortilsyn. Bakgrunnen for bestemmelsen er at for de fleste virksomheter som blir omfattet av regelverket, eksisterer det sektortilsyn som er egnet til å føre tilsyn med kravene etter digitalsikkerhetsloven. Samtidig er det viktig at det ikke er uklart hvorvidt virksomheten er underlagt tilsyn, derfor foreslår departementet at Nasjonal sikkerhetsmyndighet er tilsynsmyndighet der det ikke er utpekt sektortilsyn.

I andre ledd foreslås det at tilsynsmyndigheten kan benytte bistand fra andre ved tilsyn. Dette kan være praktisk der tilsynsmyndigheten ikke har den nødvendige spisskompetanse innenfor et fagområde eller det av andre grunner kan være behov for å benytte bistand.

I tredje ledd foreslås det en bestemmelse som gir grunnlag for behandling av personopplysninger i forbindelse med tilsyn.

Departementet foreslår videre i § 21 en bestemmelse som angir begrensninger i adgangen til å føre tilsyn med tilbydere av digitale tjenester.

I forslag til § 22 første ledd foreslås det at tilsynsmyndigheten kan fastsette frister og i hvilken form opplysningene etter digitalsikkerhetsloven § 14 skal gis. Det foreslås i andre ledd at nødvendig dokumentasjon og informasjon skal gjøres tilgjengelig for tilsynsmyndigheten. Den det føres tilsyn med eller dennes representant kan pålegges å være tilstede under tilsynet, jf. forslaget i andre ledd andre punktum. Det er uten betydning for tilsynsadgangen om driften av tjenesten er satt bort til andre, for eksempel en underleverandør. Opplysningene skal gis uten hinder av lovbestemt taushetsplikt, jf. digitalsikkerhetsloven § 14 andre ledd.

I tråd med direktivet er det i forskriften foreslått forskjellige tilsynsregimer for henholdsvis tilbydere av samfunnsviktige tjenester og tilbydere av digitale tjenester. Adgangen til å føre tilsyn med tilbydere av digitale tjenester foreslår begrenset ved at det kun åpnes for tilsyn etter mottak av opplysninger om overtredelse av bestemmelser i loven eller forskriften og tilsynsmyndigheten finner det nødvendig. Tilbydere av samfunnsviktige tjenester kan imidlertid være gjenstand for tilsyn uavhengig av overtredelser.

9.3.2 Særlig om deling av taushetsbelagt informasjon

Departementet foreslår i § 18 første ledd at varslingsmottaker kan dele taushetsbelagt informasjon som er mottatt i forbindelse med varsling med andre når det er innenfor digitalsikkerhetslovens formål og i den utstrekning det er nødvendig. Ordlyden «i den utstrekning det er nødvendig» innebærer at organet som mottar opplysningene, må sikre at færrest mulig får tilgang til opplysningene. Taushetsbelagt informasjon vil blant annet omfatte tekniske innretninger og fremgangsmåter samt drifts- eller forretningsforhold som det vil være av konkurransemessig betydning å hemmeligholde av hensyn til den som opplysningen angår, jf. forvaltningsloven § 13 første ledd nr. 2. I andre ledd foreslås det at ved fare for alvorlige hendelser skal varslingsmottaker informere berørte nasjonale og internasjonale aktører om trusler, sårbarheter og mulige tiltak.

10 Nasjonalt kontaktpunkt for sikkerhet i nettverk og informasjonssystemer

10.1 Gjeldende rett og direktivet

I digitalsikkerhetsloven § 18 bokstav h gis det adgang til å gi forskrift om nasjonalt kontaktpunkt for sikkerhet i nettverk og informasjonssystemer. I dette ligger også hvilke oppgaver kontaktpunktet skal ha. Med kontaktpunkt for sikkerhet i nettverk og informasjonssystemer menes nasjonalt felles kontaktpunkt som omtalt i direktivet artikkel 8 nr. 3.

Etter direktivet artikkel 8 nr. 3 skal kontaktpunktet utpekes. Kontaktpunktet kan legges til en eksisterende myndighet. Dersom det det kun utpekes én kompetent myndighet, skal denne myndigheten også være kontaktpunktet.

Kontaktpunktet skal etter artikkel 8 nr. 4 utøve en liaison-funksjon for å sikre grensekryssende samarbeid mellom myndighetene i landene og samarbeidsfora i EU som opprettes under direktivet, jf. artikkel 11 og 12.

Kontaktpunktet har flere forpliktelser etter direktivet, og skal blant annet utarbeide og oversende til Cooperation Group en rapport om mottatte varsler mv. etter direktivet artikkel 14 og 16.

10.2 Departementets vurderinger og forslag

Departementet foreslår i forskriften § 19 at rollen som nasjonalt kontaktpunkt utøves av Nasjonal sikkerhetsmyndighet. Som kontaktpunkt vil Nasjonal sikkerhetsmyndighet foruten å ivareta forpliktelser ovenfor EU ha en koordinerende rolle nasjonalt innen lovens virkeområde, bistå tilsynsmyndighetene gjennom veiledning, utarbeide og utvikle grunnleggende kriterier for tilsyn, legge til rette for felles opplæring av tilsynspersonell og bidra til samordning av tilsyn i den grad det er relevant. Som nasjonalt kontaktpunkt og nasjonal kompetent sikkerhetsmyndighet etter digitalsikkerhetsloven vil også Nasjonal sikkerhetsmyndighet ha et generelt veiledningsansvar innen lovens virkeområde, jf. forvaltningsloven § 11.

11 Behandling av personopplysninger

11.1 Gjeldende rett og NIS1-direktivet

Behandling av personopplysninger i henhold til NIS1-direktivet skal skje i overenstemmelse med reglene i personvernforordningen, se Prop. 109 LS (2022–2023) punkt 5.2. I digitalsikkerhetsloven § 18 bokstav g gis det adgang til å gi nærmere regler om behandling av personopplysninger i forskrift.

I Prop. 109 LS (2022–2023) punkt 5.5 la departementet til grunn at digitalsikkerhetsloven med tilhørende forskrifter langt på vei vil gi rettsgrunnlag for behandling av personopplysninger etter personvernforordningen artikkel 6 nr. 1, jf. nr. 3 og nr. 4 og artikkel 9 og 10.

Pliktene fastsatt i loven og forskriften kan utgjøre forholdsmessige tiltak og den registrertes rettigheter ivaretas blant annet ved at pliktene er avgrenset og ikke primært rettet mot rapportering om enkeltpersoner, jf. artikkel 9 nr. 2 bokstav g. Likevel må det vurderes konkret om det er nødvendig og forholdsmessig å behandle personopplysningene i hvert enkelt tilfelle.

11.2 Departementets vurderinger og forslag

Departementet foreslår i forskriften å tydeliggjøre det supplerende rettsgrunnlaget til å behandle personopplysninger og at det kan behandles opplysninger etter artikkel 9 og 10 ved varsling, tilsyn og utføring av oppgaver som nasjonalt kontaktpunkt, jf. forslag til § 17 femte ledd, § 19 andre ledd og § 20 tredje ledd. Se også punkt 9.3.2 om deling av taushetsbelagte opplysninger.

Etter forslag til § 17 femte ledd kan varslingsmottaker behandle personopplysninger når det er nødvendig for å utøve varslingsplikten. Det presiseres videre i forslag til § 17 at dette omfatter særlige kategorier personopplysninger etter personvernforordningen artikkel 9, personopplysninger om straffedommer og lovovertredelser etter personvernforordningen artikkel 10. Som redegjort for ved innføringen av digitalsikkerhetsloven kan pliktene etter loven nødvendiggjøre behandling av opplysninger om lovovertredelser for tilbyderne og myndighetene underlagt loven med henvisning til personvernforordningen artikkel 6 nr. 1 bokstav c og e. Forslaget i forskriften § 17 femte ledd gir det nødvendige rettslige supplerende behandlingsgrunnlag for private rettssubjekter til å behandle personopplysninger om straffedommer og lovovertredelser, jf. personvernforordningen artikkel 10, samt supplerende rettslig behandlingsgrunnlag for offentlige myndigheter og private rettssubjekter til å behandle særlige kategorier av personopplysninger etter personvernforordningen artikkel 9.

Behandlingsgrunnlaget i personvernforordningen artikkel 6 nr. 1 vil for varslingsmottaker kunne være bokstav e som gjelder behandling som er nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt. Det vil også her måtte gjøres en konkret nødvendighets- og forholdsmessighetsvurdering av varslingsmottaker. De ulike typer behandlinger som vil kunne være aktuelle knytter seg til mottak av varsel og eventuell bistand til tilbyderen i håndtering av hendelsen.

Videre er det i forskriften § 19 andre ledd foreslått supplerende rettsgrunnlag for behandling av personopplysninger for nasjonalt kontaktpunkt og for

tilsynsmyndigheten i § 20 tredje ledd. Hvilke personopplysninger som kan behandles fremgår av bestemmelsene og er tilsvarende som etter varslingsplikten i § 17. Departementet viser til omtalen over. Når det er nødvendig for å utføre oppgaver som nasjonalt kontaktpunkt kan Nasjonal sikkerhetsmyndighet behandle personopplysninger, jf. § 19 andre ledd. Når det er nødvendig for å utføre sine oppgaver, kan tilsynsmyndigheten behandle personopplysninger, jf. § 20 tredje ledd. Behandlingsgrunnlag i personvernforordningen vil være artikkel 6 nr. 1 bokstav e, jf. omtalen over. Nasjonal sikkerhetsmyndighet og tilsynsmyndigheten vil måtte gjøre konkrete nødvendighets- og forholdsmessighetsvurderinger dersom personopplysninger skal behandles.

Når det gjelder tiltak og garantier for å beskytte de registrerte vil personvernforordningens prinsipper gjelde, særlig prinsippene om formålsbegrensning, dataminimering og sletting, jf. personvernforordningen artikkel 5. Reglene i forskriften gir også nærmere rammer for behandling av opplysningene, herunder hvilke aktører som er omfattet, hvilke oppgaver disse har og hvilke opplysninger det er særlig aktuelt å behandle. Dersom det er aktuelt er det lagt opp til at forslaget skal kunne gi grunnlag for behandling til nye og uforenelige formål, jf. artikkel 6 nr. 4.

For å gi virksomheter det rettslige supplerende rettsgrunnlaget og handlingsrommet til å kunne behandle personopplysninger etter en konkret vurdering, foreslås dette inntatt særskilt i forskriften. For tilbydere av samfunnsviktige tjenester og tilbydere av digitale tjenester som står i hendelseshåndtering vil også personvernforordningen art. 6 nr. 1 bokstav f kunne gi relevant behandlingsgrunnlag for behandling av personopplysninger dersom behandlingen er nødvendig for formål knyttet til de berettigede interessene som forfølges av den behandlingsansvarlige eller en tredjepart, med mindre den registrertes interesser eller grunnleggende rettigheter og friheter går foran. De ulike typer behandlinger som vil kunne være aktuelle knytter seg til håndtering av en hendelse og varsling til myndigheten. Virksomheten vil måtte gjøre en konkret nødvendighets- og forholdsmessighetsvurdering. Etter fortalepunkt 49 i personvernforordningen vil behandling av personvernopplysninger i det omfang som er strengt nødvendig og forholdsmessig for å sikre nettverk og informasjonssikkerheten utgjøre en berettiget interesse for den berørte behandlingsansvarlige.

12 Overtredelsesgebyr

12.1 Gjeldende rett

Digitalsikkerhetsloven § 17 regulerer overtredelsesgebyr. I første ledd fremgår det at tilsynsmyndigheten kan ilegge en tilbyder overtredelsesgebyr dersom tilbyderen eller noen som handler på dennes vegne forsettlig eller uaktsomt har overtrådt bestemmelsene om krav til sikkerhet i §§ 7 og 10, krav til varsling etter §§ 8 og 11 og der det er gitt uriktige eller ufullstendige opplysninger til tilsynsmyndigheten i § 14. Det fremgår i andre ledd at dersom den ansvarlige for overtredelsesgebyret er et foretak som inngår i et konsern, hefter foretakets morselskap og morselskapet i det konsern selskapet er en del av, subsidiært for beløpet.

I tredje ledd første punktum er det fastsatt at adgangen til å pålegge overtredelsesgebyr foreldes etter fem år etter at overtredelsen er opphørt. I tredje

ledd andre punktum fremgår det at fristen avbrytes når tilsynsmyndigheten gir forhåndsvarsel om eller fatter vedtak om overtredelsesgebyr.

Etter digitalsikkerhetsloven § 18 første ledd bokstav d kan det i forskrift gis utfyllende bestemmelser om ileggelse og utmåling av overtredelsesgebyr. Etter bokstav e kan det fastsettes i forskrift at overtredelse av forskriftskrav om sikkerhet og varsling kan utløse overtredelsesgebyr.

Overtredelsesgebyr retter seg mot den enkelte tilbyderen som er pliktsubjekt etter loven. Under lovarbeidet foreslo departementet i høringsrunden at fysiske personer skal kunne ilegges overtredelsesgebyr dersom vedkommende har handlet uaktsomt eller forsettlig. I lovproposisjonen kapittel 9.5 andre spalte omtalte departementet at adgangen til å ilegge fysiske personer overtredelsesgebyr skulle gjelde dersom det var nødvendig i det enkelte tilfellet. Dette kommer imidlertid ikke klart frem i digitalsikkerhetsloven § 17, men følger forutsetningsvis av ordlyden «noen som handler på dennes vegne». Ved ileggelse av overtredelsesgebyr overfor fysiske personer vil det gjelde et krav til skyld.

Som departementet omtalte i lovproposisjonen, jf. kapittel 9.5 andre spalte, gjelder det etter forvaltningsloven § 47 en samordningsplikt av sanksjonssaker, der det er grunn til å anta at andre forvaltningsorgan vurderer spørsmålet om å ilegge sanksjoner.

12.2 NIS1-direktivet

I henhold til artikkel 21 skal EØS-statene fastsette regler om sanksjoner ved brudd på forpliktelser som følger av nasjonal lovgivning, og som er implementert som følge av direktivet. Sanksjonene skal være virkningsfulle, stå i et rimelig forhold til overtredelsen og virke avskrekkende. Direktivet skiller her ikke mellom tilbydere av samfunnsviktige tjenester og tilbydere av digitale tjenester. Statene står fritt til å fastsette maksimalbeløp ved overtredelser, og det angis at det bør være rom for en konkret vurdering for å ilegge passende gebyr. Blant annet bør det legges vekt på forholdets alvorlighetsgrad og om det er tale om gjentakende overtredelser.

12.3 Departementets vurderinger og forslag

Departementet foreslår en bestemmelse i forskriften § 23 som regulerer overtredelsesgebyr. I første og andre ledd foreslås det at tilsynsmyndigheten skal ta hensyn til en rekke forhold ved ileggelse av gebyr, både ved vurderingen av overtredelsens grovhet og overtredelsesgebyrets størrelse.

I tredje ledd foreslår departementet en øvre ramme for overtredelsesgebyr. Om den nærmere begrunnelsen for å kunne ilegge overtredelsesgebyr ved brudd på enkelte bestemmelser i digitalsikkerhetsloven, vises det til Prop. 109 LS (2022–2023) kapittel 9, og viktigheten av at sikkerhetskrav og krav til varsling samt opplysningsplikten etterleves for å oppnå lovens formål.

Overtredelsesgebyr etter digitalsikkerhetslovens bestemmelser kan både rette seg mot offentlige og private virksomheter.

For overtredelsesgebyr ilagt en privat virksomhet foreslås det at øvre ramme for overtredelsesgebyr er fire prosent av virksomhetens samlede omsetning for siste regnskapsår. Departementet viser til at det er en rekke eksempler på lover hvor den

øvre rammen for overtredelsesgebyrets størrelse er knyttet til en prosentandel av omsetningen til et foretak, se for eksempel konkurranseloven, verdipapirhandelloven, revisorloven og markedsføringsloven.

For offentlige organer passer ikke beregning av overtredelsesgebyret ut fra årsomsetning like godt. Etter personopplysningsloven kan både offentlige og private virksomheter ilegges overtredelsesgebyr, og den maksimale rammen er satt til 20 millioner euro eller fire prosent av årsomsetningen forutgående regnskapsår, der det høyeste beløpet anvendes. I forarbeidene er det imidlertid klart forutsatt at det ligger et betydelig skjønn med hensyn til størrelsen på gebyret som faktisk ilegges.

Etter departementets vurdering er den øvre rammen på 20 millioner euro angitt i personopplysningsloven, for våre forhold, kunstig høy. En ramme for overtredelsesgebyr bør ha en reell funksjon, nemlig skape forutsigbarhet for hvor stor gebyrene potensielt kan bli. En prosentsats av samlet omsetning forutgående regnskapsår vil gi slik forutsigbarhet for private virksomheter.

For offentlige virksomheter vurderer departementet at rammen kan ta utgangspunkt i folketrygdens grunnbeløp, for tiden 124 028 kroner, ved at overtredelsesgebyr maksimalt utgjøre et visst antall ganger folketrygdens grunnbeløp. Departementet er i tvil om hva som vil være en passende øvre ramme for offentlige virksomheter, men foreslår at den øvre rammen for overtredelsesgebyr ilagt overfor en offentlig virksomhet skal være 25 ganger grunnbeløpet. Beløpet tilsvarer for tiden i overkant av 3 millioner kroner. Departementet ber om høringsinstansenes syn på om det foreslåtte beløpet vil være treffende.

Det relativt høye beløpet som er satt som øvre ramme for gebyrene skal reflektere det alvorlige i overtredelser av regler som er gitt for å ivareta grunnleggende krav til digital sikkerhet i nettverk og informasjonssystemer som brukes for å levere samfunnsviktige tjenester og digitale tjenester. Departementet understreker at rammen er nettopp en øvre grense for gebyr, og ikke er ment som en antatt vanlig størrelse på ilagt gebyr. Overtredelsesgebyr er et pålegg gitt av forvaltningen til et rettssubjekt om å betale et pengebeløp til det offentlige som følge av overtredelse av fastsatte krav i lov eller forskrift. Overtredelsesgebyr har i likhet med straff et pønalt og preventivt formål, og retter seg mot handlinger eller unnlatelser i fortid. Sanksjonen kan derfor ilegges for forhold som er skjedd, selv om pliktbruddet har opphørt.

Etter forskriftsforslaget § 23 tredje ledd kan tilsynsmyndigheten ved forsettlig eller uaktsom overtredelse av digitalsikkerhetsloven § 14 eller bestemmelser i eller i medhold av digitalsikkerhetsloven §§ 7, 8, 10 eller 11, ilegge et overtredelsesgebyr.

I forvaltningsloven § 44 andre ledd første punktum fremgår det at overtredelsesgebyr kan ilegges etter faste satser eller utmåles i det enkelte tilfelle (individuell utmåling) innenfor en øvre ramme som må fastsettes i eller i medhold av lov. Bakgrunnen for bestemmelsen er blant annet at handlingsrommet for skjønnsutøvelse ikke skal være videre enn nødvendig, se Prop. 62 L (2015–2016) side 86-87.

Som beskrevet i Prop. 109 LS (2022–2023) side 46 vil utmålingen av overtredelsesgebyr for øvrig bero på en konkret helhetsvurdering i hver enkelt sak

hva som er et passende gebyr der også den aktuelle tilbyderens omsetning kan vektlegges. Det vil dessuten kunne variere over tid hva som er passende beløpsmessige rammer, og blant annet kan dette påvirkes av rettsutviklingen i EU. På denne bakgrunn foreslås det i at det skal legges særlig vekt på overtredelsens grovhet, overtredelsens varighet, utvist skyld og tilbyderens omsetning ved ileggelse av overtredelsesgebyr. Betydningen av overtredelsens varighet vil kunne variere med type virksomhet og type pliktbrudd, der en tidsperiode vil kunne være kritisk i en sektor og for en virksomhet, men ikke for en annen sektor eller virksomhet. Vurderingene som gjøres av om det foreligger skyld som grunnlag for å i det hele tatt å ilegge overtredelsesgebyr, vil kunne legges til grunn også i utmålingen. Når det gjelder virksomhetens omsetning vil myndigheten kunne innhente opplysninger om dette fra Brønnøysundregistrene og legge til grunn den netto salgsinntekten. Virksomhetens størrelse sammenlignet med tilsvarende aktører i markedet vil være relevant å se hen til.

Etter forslaget er det opplistet flere momenter som det i vurdering av overtredelsens grovhet særlig skal tas hensyn til. Det første momentet er overtredelsens art. Med dette forstås hvilken av virksomhetens verdier som er berørt, eksempelvis kan verdien i et gitt tilfelle være infrastruktur, og da må man blant annet se på om dette er en svært viktig eller kritisk infrastruktur for virksomheten selv eller andre virksomheter eller sektorer. I denne vurderingen inngår om det er gjennomført risiko- og sårbarhetsanalyser knyttet til verdien, om det er foretatt tiltak for å redusere restrisiko med videre. Det andre momentet i forslaget til andre ledd gjelder tilbyderens gevinst. Dette vil for eksempel kunne omfatte manglende avsatte ressurser til planmessig sikkerhetsarbeid, manglende system og håndtering for varsling ved hendelser. Manglende avsatte ressurser som nevnt, vil kunne innebære sparte kostnader, men som kan være vanskelig å tallfeste. Det tredje momentet som gjelder overtredelsens faktiske innvirkning på markedet vil kunne innebære forskjellige forhold ut i fra den konkrete saken. Departementet fremhever imidlertid eventuell sannsynlig betydning som overtredelsen kan ha hatt på andre virksomheter i egen eller andre sektorer som en viktig faktor. Avhengigheter på tvers av sektorer og leverandører blir en stadig større risiko som det derfor må tas hensyn til. Det fjerde momentet gjelder størrelsen på det berørte markedet, og det vil her være relevant å se hen til virksomhetens betydning og størrelse i markedet og eventuelle viktige eller kritiske kunder denne har. Det femte momentet gjelder om overtrederen har hatt en ledende eller passiv rolle i overtredelsen.

Etter forslaget i andre ledd er andre momenter som kan påvirke utmålingen av overtredelsesgebyret blant annet om tiltak er gjennomført, om tilbyderen ved retningslinjer, instruksjon, opplæring, kontroll eller andre tiltak kunne ha forebygget overtredelsen og om tilbyderen har bistått myndigheten i forbindelse med utredning av overtredelsen.

Opplistingen er ikke uttømmende, og det kan for eksempel være aktuelt å se hen til allmennpreventive hensyn i form av å sende et signal til bransjen om betydningen av for eksempel bestemte sikkerhetskrav. Departementet viser også til at relevante momenter kan fremgå av annet regelverk, for eksempel kommuneloven § 30-4 andre ledd som bestemmer at tilsynsmyndigheten skal vurdere virkningene for kommunens eller fylkeskommunens øvrige virksomhet før tilsynsmyndigheten vedtar en reaksjon hjemlet i lov mot en kommune eller en fylkeskommune. Videre

vil man kunne se hen til eventuelle formildende omstendigheter på rettssubjektets side.

I forslaget til fjerde ledd fremgår det at vedtak om overtredelsesgebyr er tvangsgrunnlag for utlegg. Dersom det anlegges sak mot staten for å prøve vedtaket, foreslår departementet i andre punktum å regulere at tvangskraften suspenderes. Oppfyllelsesfristen er fire uker fra vedtaket ble truffet, jf. forvaltningsloven § 44 femte ledd. Lengre frist kan fastsettes i vedtaket eller senere, jf. andre punktum.

13 Økonomiske og administrative konsekvenser

For virksomheter som allerede er underlagt sikkerhets- og varslingskrav i eksisterende sektorregelverk, antar departementet at forskriftsforslaget ikke medfører vesentlige økonomiske eller administrative konsekvenser. Virksomheter som ikke allerede er underlagt sikkerhets- og varslingskrav vil derimot måtte påregne kostnader knyttet til etablering av styringssystem for sikkerhet, gjennomføring av risikovurderinger og implementering av tiltak, samt opplæringsaktiviteter med videre. Særlig er det knyttet økonomiske og administrative konsekvenser til implementering av et sikkerhetssystem i den enkelte virksomhet. Det er imidlertid vanskelig å anslå merkostnadene knyttet til dette, da rekkevidden trolig vil variere betydelig mellom virksomhetene. Departementet viser i den forbindelse til at tilbyderne etter digitalsikkerhetsloven § 7 andre ledd skal iverksette hensiktsmessige og proporsjonale tekniske og organisatoriske sikkerhetstiltak som samlet skal sørge for et sikkerhetsnivå som er tilpasset risikoen.

Den enkelte virksomhet vil trolig også måtte bruke mer ressurser på oppfølging av leverandører av digital infrastruktur og digitale tjenester, jf. forskriftsforslaget § 14. Samtidig er det å forvente at en rekke av virksomhetene som blir omfattet av regelverket allerede har betydelige sikkerhetstiltak på plass og jobber systematisk med sikkerhet, og at regelverket i seg selv ikke medfører vesentlige merkostnader.

For berørte tilsynsmyndigheter vil forlagene innebære kostnader knyttet til gjennomføring av tilsyn og håndtering av varsler. Særlig vil nye tilsynsoppgaver kreve ressurser og i mange tilfeller kompetansehevingstiltak. Også mer omfattende veiledningsplikt og krav til økt samhandling med andre myndigheter vil kunne kreve økt ressursbruk.

Varslingsordningen vil kunne medføre økt ressursbruk hos varslingsmottakerne og kontaktpunkt for sikkerhet i nettverk og informasjonssystemer for etablering og drift av varslingsordningen, samt kostnader forbundet med etablering av varslingskanal. Det foreslås ingen endringer i den eksisterende organiseringen av nasjonalt og sektorvise responsmiljøer, men det antas likevel at det kan være behov for enkelte justeringer av rammeverket for hendelseshåndtering som følge av ordningen nå foreslås regulert, som igjen kan kreve ressursbruk ved responsmiljøene. Det vises for øvrig til redegjørelsen i Prop. 109 LS (2022–2023) punkt 11.1.

Departementet ber i lys av dette om høringsinstansenes innspill på konsekvensene forslagene i høringsnotatet vil få for dem.

Avslutningsvis legger departementet til at EU-kommisjonen i 2013 foretok beregninger knyttet til innføringen av NIS1-direktivet i EU. Etter departementets

syn vil EU-kommisjonens beregninger trolig være utdatert både som følge av at en rekke virksomheter har styrket sikkerheten i deres nettverk og informasjonssystemer siden 2013, og som følge av lønns- og prisstigning fra 2013 til i dag. Departementet gjengir imidlertid en av beregningene, som var at sikkerhetskostnadene knyttet til innføring av direktivet ville utgjøre 6,61 pst. av en virksomhets totale IKT-budsjett. Det vises til høring om digitalsikkerhetsloven fra 2018 for gjengivelse EU-kommisjonens kostnadsberegninger knyttet til innføring av direktivet.

Forslag til forskrift til digitalsikkerhetsloven (digitalsikkerhetsforskriften)

Hjemmel: Fastsatt av Justis- og beredskapsdepartementet [dato] med hjemmel i lov 20. desember 2023 nr. 108 om digital sikkerhet (digitalsikkerhetsloven) § 2, § 3, § 9, § 17 og § 18.

Kapittel 1. Lovens virkeområde

§ 1. Tilbydere av samfunnsviktige tjenester

Tilbydere av samfunnsviktige tjenester etter digitalsikkerhetsloven § 2 første ledd bokstav a og § 6 er

1. KBO-enheter, jf. kraftberedskapsforskriften § 2-1 andre ledd
2. virksomheter som ved enkeltvedtak helt eller delvis er underlagt kraftberedskapsforskriften § 1-3 andre ledd
3. hovedtankanlegg for petroleumsbasert drivstoff
4. flysikringstjenesten
5. kommersielle lufthavner og tjenesteleverandører innenfor sikkerhetsbegrenset område på en kommersiell lufthavn
6. flyselskaper som driver kommersiell transport med AOC i Norge
7. infrastrukturforvaltning og trafikkstyring av det nasjonale jernbanenettet
8. persontransport som overstiger 375 000 togkilometer pr. år, inkludert grenseoverskridende transport
9. godstransport som overstiger 500 000 togkilometer pr. år, inkludert grenseoverskridende transport
10. infrastrukturforvaltning, trafikkstyring og togfremføring av T-bane og trikk som overstiger 12,5 millioner årlige passasjerreiser
11. trafikkstyring og -overvåking av TEN-T-vegnett
12. det viktigste vegnettet i områder med årsdøgntrafikk over 20 000
13. alarmsentraler for eCall
14. nasjonale databanker som inneholder veg- eller trafikkinformasjon
15. trafikkstyring og -overvåking av kysttrafikken
16. havner eller havneanlegg som har et godsomlag på mer enn 100 000 tonn pr. år sett over en femårsperiode
17. havner eller havneanlegg som håndterer mer enn 100 000 passasjer pr. år sett over en femårsperiode
18. rederier som har skip med fast anløp eller som transporterer minst fem prosent av passasjerantallet eller godsomslaget i en havn som nevnt i nr. 18
19. Helse- og omsorgsdepartementet med underliggende etater og foretak, som utgjør den nasjonale helseberedskapen
20. tjenester som tilbys av de regionale helseforetakene
21. sentrale systemer for rekvirering og utlevering av legemidler og andre medisinske produkter
22. helse- og omsorgstjenester som tilbys av en kommune med
    a. flere enn 50 000 innbyggere, eller
    b. flere enn 20 000 brukere som er avhengige av tjenesten, og
    c. tjenesten ikke kan overføres eller avlastes av andre tjenester
23. vannforsyningssystem etter drikkevannsforskriften § 3 bokstav k, som behandler minst 2000 m3 pr. døgn

24. sentralt register over norske toppnivådomener (.no, .bv og .sj)
25. rekursiv navneservertjeneste med flere enn 50 000 aktive brukere
26. samtrafikkpunkter for Internett
27. banker som Finansdepartementet har truffet beslutning om at skal anses som systemviktige i Norge, jf. CRR/CRD IV-forskriften § 30
28. foretak som Finanstilsynet vurderer at har vesentlig betydning for det norske kapitalmarkedet.

§ 2. Unntak for små virksomheter

Krav til digital sikkerhet for tilbydere av digitale tjenester etter § 13 og varslingsplikten etter § 15 gjelder ikke for tilbydere av digitale tjenester som har færre enn 50 ansatte og som har en årlig omsetning eller årlig samlet balanse som ikke overstiger 100 millioner kroner.

§ 3. Lovens anvendelse for Svalbard

Digitalsikkerhetsloven med forskrifter gjelder for Svalbard.

§ 4. Vedtak om at loven skal gjelde for andre tilbydere av samfunnsviktige tjenester

For andre tilbydere av samfunnsviktige tjenester enn de som er nevnt i § 1, kan ansvarlig departement i særlige tilfeller fatte vedtak om at loven helt eller delvis skal gjelde. Nasjonal sikkerhetsmyndighet kan fatte vedtak etter første punktum overfor virksomheter som ikke omfattes av noe departements ansvarsområde.

§ 5. Innmelding av tilbyder av samfunnsviktig tjeneste

Tilbyder av en samfunnsviktig tjeneste skal snarest melde inn til Nasjonal sikkerhetsmyndighet og tilsynsmyndigheten opplysninger om

a. virksomhetens navn, organisasjonsnummer og kontaktinformasjon
b. tjenesten
c. samfunnssektor
d. eventuelt i hvilke andre land tjenesten tilbys
e. berørt geografisk område
f. endringer i opplysninger nevnt i bokstav a til e.

Kapittel 2. Krav til digital sikkerhet for tilbydere av samfunnsviktige tjenester

§ 6. Styringssystem for sikkerhet

Tilbyder av samfunnsviktig tjeneste skal etablere og vedlikeholde et styringssystem for sikkerhet som omfatter digital sikkerhet. Styringssystemet skal være dokumentert og inngå som del av den overordnede virksomhetsstyringen.

Sikkerhetsstyringssystemet skal baseres på anerkjente standarder og bidra til å

a. forebygge hendelser

b. avdekke hendelser
c. håndtere hendelser
d. korrigere og gjenopprette sikkerheten i nettverk og informasjonssystemer ved hendelser
e. kontinuerlig styre og følge opp at formålene i bokstavene a til e oppnås.

Alle aktiviteter som er nødvendige for å etablere og opprettholde et forsvarlig sikkerhetsnivå skal inngå i sikkerhetsstyringssystemet. Aktivitetene skal dokumenteres og gjøres kjent for personell med tjenstlig behov.

Virksomhetens leder har ansvar for at virksomheten har et forsvarlig sikkerhetsnivå innenfor virkeområde til digitalsikkerhetsloven. Sikkerhetsstyringssystemet skal godkjennes av virksomhetens leder og gjennomgås minst årlig med sikte på å forbedre virksomhetens sikkerhetsarbeid.

§ 7. Risikovurdering

Tilbyder av samfunnsviktig tjeneste skal utarbeide, vedlikeholde og dokumentere risikovurderinger.

Risikovurderinger skal være av et slikt omfang at tilbyderen kan identifisere organisatoriske, teknologiske, fysiske og personellmessige sikkerhetstiltak som ivaretar formålene i § 8. Ved endringer i virksomheten som kan påvirke sikkerheten, skal tilbyder vurdere hvilken risiko endringene medfører.

Risikovurderinger skal minst inneholde

g. en kartlegging av virksomhetens nettverk og informasjonssystemer og hvilken betydning disse har for leveransen av den samfunnsviktige tjenesten
h. hvilke hendelser virksomhetens nettverk og informasjonssystemer kan bli utsatt for
i. hvilke sårbarheter som er knyttet til virksomhetens nettverk og informasjonssystemer
j. sannsynligheten for at en hendelse kan inntreffe
k. konsekvensen av hendelser
l. i hvilken grad virksomheten er avhengig av andre virksomheter for å fungere som den skal.

§ 8. Risikohåndtering

Basert på risikovurderingen i § 7 skal tilbyder av samfunnsviktig tjeneste ha en plan for å håndtere risiko. Som en del av risikohåndteringen skal tilbyder iverksette organisatoriske, teknologiske, fysiske og personellmessige sikkerhetstiltak for å redusere risiko og opprettholde et forsvarlig sikkerhetsnivå.

Sikkerhetstiltakene skal som et minimum ha som formål å bidra til sikker plattform, sikker drift og vedlikehold, samt sikker hendelseshåndtering og gjenoppretting.

Nasjonal sikkerhetsmyndighet skal utarbeide veiledninger om risikovurdering og håndtering av risiko.

§ 9. Organisatoriske sikkerhetstiltak

Tilbyder av samfunnsviktig tjeneste skal utarbeide skriftlige instrukser for rutiner og prosedyrer innenfor sikkerhet. Instruksene skal tilpasses virksomhetens størrelse og kompleksitet.

Tilbyder av samfunnsviktig tjeneste skal ha oppdaterte lister over sikkerhetstiltak som kan iverksettes dersom risikoen endrer seg eller det oppstår en hendelse, jf. § 13.

Relevante instrukser, rutiner, prosedyrer og lister etter første og andre ledd skal gjøres kjent for personell som utfører oppgaver for eller på vegne av virksomheten og som kan få tilgang til virksomhetens nettverk og informasjonssystemer.

§ 10. Teknologiske sikkerhetstiltak

Basert på risikovurderingen etter § 7 skal tilbyder av samfunnsviktig tjeneste iverksette teknologiske sikkerhetstiltak som er tilpasset omfang, kompleksitet, driftsmiljø, brukermiljø, funksjon og risiko ved virksomhetens nettverk og informasjonssystemer.

Teknologiske sikkerhetstiltak skal minst omfatte

a. to- eller flerfaktorautentisering for adgang til nettverk og informasjonssystemer for brukere og administratorer
b. tilgangskontroll til innhold i nettverk og informasjonssystemer basert på tjenstlig behov
c. styring av og kontroll med hvem som bruker virksomhetens nettverk og informasjonssystemet
d. tiltak for segmentering av tjenester basert på et prinsipp om minste minimum av rettigheter
e. tiltak som skal sikre at nettverk og informasjonssystemer kan håndtere forskjellige typer avbrudd og gjenopprettes innen rimelig tid uten vesentlig reduksjon av tjenestens kvalitet
f. tiltak som skal sikre at nettverk og informasjonssystemer har tilstrekkelig kapasitet til å tåle overbelastning og utstyrssvikt
g. tiltak som skal sikre at nettverk og informasjonssystemer videreutvikles kontinuerlig, herunder at oppdateringer kvalitetssikres, installeres og testes fortløpende
h. sikkerhetsovervåkning av nettverk og informasjonssystem for å avdekke hendelser.

§ 11. Fysiske sikkerhetstiltak

Tilbyder av samfunnsviktig tjeneste skal iverksette tiltak for fysisk sikkerhet for å opprettholde forsvarlig sikkerhet i nettverk og informasjonssystemer.

Fysiske sikkerhetstiltak skal minst omfatte

a. tiltak for å forhindre at uvedkommende får tilgang til lokasjoner og fysisk og teknisk infrastruktur som nettverk og informasjonssystemer benytter eller er avhengig av

b. tiltak for å identifisere og beskytte bygninger, rom og tilstøtende områder som har betydning for sikkerhetsnivået til nettverk og informasjonssystemer som understøtter den samfunnsviktige tjenesten
c. tiltak for å ivareta eksterne avhengigheter, herunder datakommunikasjon og strømtilførsel.

§ 12. Sikkerhetstiltak for personell

Tilbyder av samfunnsviktig tjeneste skal iverksette nødvendige sikkerhetstiltak for ansatte, leverandører og oppdragstakere som kan få tilgang til virksomhetens nettverk og informasjonssystemer.

Tilbydere skal iverksette tiltak for adgangskontroll, brukerautentisering og tilgangskontroll, slik at kun personell med tjenstlig behov får tilgang til tilbyders nettverk og informasjonssystemer.

Tilbyder skal sørge for at personell nevnt i første ledd er gjort kjent med relevante sikkerhetstiltak og at de har tilstrekkelig kompetanse innenfor sikkerhet og gis nødvendig opplæring ved behov.

Når et arbeidsforhold eller en tjeneste avsluttes, skal tilbyder av samfunnsviktig tjeneste sikre at den som slutter, ikke lenger har tilgang til virksomhetens nettverk og informasjonssystemer.

§ 13. Hendelseshåndtering og beredskap

Tilbyder av samfunnsviktig tjeneste skal ha en beredskapsplan for håndtering av hendelser og varsling etter § 17. Tilbyder skal ha vurdert relevante beredskapstiltak eller innstramminger i eksisterende sikkerhetstiltak som raskt kan iverksettes ved behov.

Når tilbyderens nettverk eller informasjonssystem er utsatt for en hendelse skal hendelsens karakter og omfang identifiseres. Tilbyderen skal iverksette nødvendige mottiltak og tiltak for å gjenopprette den sikre tilstanden i nettverk og informasjonssystemer.

Tilbyder av samfunnsviktig tjeneste skal utarbeide, vedlikeholde og dokumentere beredskapsplaner og gjennomføre øvelser for å teste planverket og utvikle virksomhetens kompetanse til å håndtere hendelser. Dersom det er relevant, bør øvelser gjennomføres i samarbeid med underleverandører eller andre som utfører arbeid for eller på vegne av virksomheten.

§ 14. Oppfølgingsplikt

Tilbyder av samfunnsviktig tjeneste skal påse at leverandører og andre som utfører arbeid som kan påvirke sikkerheten i nettverk og informasjonssystemer og som utfører arbeid for eller på vegne av virksomheten, utfører arbeidet på en måte som gjør at virksomhetens krav til forsvarlig sikkerhet overholdes.

Tilbyder av samfunnsviktig tjeneste skal gjøre sikkerhetstiltakene gjeldende overfor leverandører som kan påvirke nettverk og informasjonssystemer, i den grad det er nødvendig for å opprettholde et forsvarlig sikkerhetsnivå.

Kapittel 3. Krav til digital sikkerhet for tilbydere av digitale tjenester

§ 15. Tiltak for sikkerhetsstyring for tilbydere av digitale tjenester og kriterier for å avgjøre om en hendelse skal anses for å ha betydelig innvirkning

EØS-avtalen vedlegg XI nr. 5cpaa (forordning 2018/151) gjelder som forskrift med de tilpasninger som følger av vedlegg XI, protokoll 1 til avtalen og avtalen for øvrig.

Kapittel 4. Fellesbestemmelser

§ 16. Nasjonalt responsmiljø og sektorvise responsmiljøer

Nasjonal sikkerhetsmyndighet er nasjonalt responsmiljø for håndtering av hendelser etter digitalsikkerhetsloven.

Ansvarlig departement kan utpeke responsmiljøer som kan bistå tilbyder med å håndtere hendelser innenfor energi, transport, helse, vannforsyning, bank, finansmarkedsinfrastruktur og digital infrastruktur. Nasjonal sikkerhetsmyndighet skal orienteres om utpekingen.

Et responsmiljø for håndtering av hendelser etter digitalsikkerhetsloven skal som minimum oppfylle krav som følger av vedlegg I til NIS1-direktivet og overholde relevante krav som følger i eller i medhold av digitalsikkerhetsloven.

§ 17. Varslingsplikt

Varsel etter digitalsikkerhetsloven § 8 og § 11 skal gis til tilsynsmyndigheten med kopi til Nasjonal sikkerhetsmyndighet. Varsel skal gis senest innen 24 timer etter at tilbyder fikk kjennskap til hendelsen. Varselet skal inneholde informasjon om

a. tilbyders navn og kontaktinformasjon
b. berørt tjeneste
c. hendelsen, herunder mulige årsaker og konsekvenser
d. antall berørte brukere
e. hendelsens virkninger i andre land.

Informasjonen i varselet skal oppdateres innen 72 timer.

Innen en måned fra varsel som nevnt i første ledd er gitt, skal tilbyder av samfunnsviktig tjeneste gi varslingsmottaker en hendelsesrapport. Hendelsesrapporten skal inneholde oppdatert informasjon om forhold som nevnt i første ledd og hvilke avhjelpende tiltak som er iverksatt.

Varslingsmottaker kan kreve statusoppdateringer og de opplysningene som er nødvendige for å utføre pålagte oppgaver.

Når det er nødvendig for å utøve varslingsplikten kan tilbyder av samfunnsviktig tjeneste, tilbyder av digitale tjenester og varslingsmottaker behandle personopplysninger, herunder personopplysninger nevnt i personvernforordningen artikkel 9 og artikkel 10.

§ 18. Deling av taushetsbelagt informasjon

Når det er innenfor digitalsikkerhetslovens formål og i den utstrekning det er nødvendig, kan varslingsmottaker dele med andre aktører taushetsbelagt informasjon mottatt ved varsling.

Ved fare for alvorlige hendelser skal Nasjonal sikkerhetsmyndighet informere berørte nasjonale og internasjonale aktører om risiko og mulige tiltak.

§ 19. Nasjonalt kontaktpunkt for sikkerhet i nettverk og informasjonssystemer

Nasjonal sikkerhetsmyndighet er nasjonalt kontaktpunkt for sikkerhet i nettverk og informasjonssystemer.

Når det er nødvendig for å utføre oppgaver som nasjonalt kontaktpunkt, kan Nasjonal sikkerhetsmyndighet behandle personopplysninger, herunder personopplysninger nevnt i personvernforordningen artikkel 9 og artikkel 10.

§ 20. Tilsyn med tilbydere som omfattes av loven

Ansvarlig departement utpeker myndighet som skal føre tilsyn med virksomheter innenfor egen sektor. For virksomheter uten tilsynsmyndighet er Nasjonal sikkerhetsmyndighet tilsynsmyndighet.

Tilsynsmyndigheten kan benytte bistand fra andre ved utførelsen av tilsynet.

Tilsynsmyndigheten kan behandle personopplysninger dersom det er nødvendig for å utføre sine oppgaver, herunder personopplysninger nevnt i personvernforordningen artikkel 9 og artikkel 10.

§ 21. Begrensning i adgangen til å føre tilsyn med tilbydere av digitale tjenester

Tilsyn med tilbydere av digitale tjenester kan kun gjennomføres dersom tilsynsmyndigheten mottar opplysninger om overtredelser av bestemmelser gitt i eller i medhold av digitalsikkerhetsloven og tilsynsmyndigheten finner det nødvendig.

§ 22. Opplysningsplikt og tilgang til lokaler

Tilsynsmyndigheten kan fastsette frister og i hvilken form opplysningene etter digitalsikkerhetsloven § 14 skal gis.

Nødvendig dokumentasjon og informasjon skal gjøres tilgjengelig for tilsynsmyndigheten. Den det føres tilsyn med eller dennes representant kan pålegges å være tilstede under tilsynet.

§ 23. Overtredelsesgebyr

Ved fastsettelse av størrelsen på overtredelsesgebyr ilagt med hjemmel i digitalsikkerhetsloven § 17 skal det legges særlig vekt på overtredelsens grovhet, overtredelsens varighet, utvist skyld og tilbyderens omsetning. Ved vurdering av overtredelsens grovhet skal det særlig tas hensyn til

a. overtredelsens art
b. tilbyderens gevinst
c. overtredelsens faktiske innvirkning på markedet
d. størrelsen på det berørte markedet
e. om overtrederen har hatt en ledende eller passiv rolle i overtredelsen.

Andre momenter som kan påvirke utmålingen av overtredelsesgebyret er blant annet

a. om tiltak er gjennomført
b. om tilbyderen ved retningslinjer, instruksjon, opplæring, kontroll eller andre tiltak kunne ha forebygget overtredelsen
c. om tilbyderen har bistått myndigheten i forbindelse med utredning av overtredelsen.

Ved forsettlig eller uaktsom overtredelse av digitalsikkerhetsloven § 14 eller bestemmelser i eller i medhold av digitalsikkerhetsloven §§ 7, 8, 10 eller 11, kan tilsynsmyndigheten ilegge overtredelsesgebyr på opptil 25 ganger grunnbeløpet eller, dersom det dreier seg om et foretak, på opptil 4 prosent av den samlede årsomsetningen i det forutgående regnskapsår, der det høyeste beløpet anvendes.

Vedtak om overtredelsesgebyr er tvangsgrunnlag for utlegg. Dersom det anlegges sak mot staten for å prøve vedtaket, suspenderes tvangskraften.

§ 24. Ikrafttredelse

Forskriften trer i kraft straks.