FOLKETINGET

Folketingstidende
Tillæg A

Lovforslag nr. **L 142** Folketinget 2024-25

Fremsat den 6. februar 2025 af ministeren for samfundssikkerhed og beredskab (Torsten Schack Pedersen)

Forslag

til

Lov om sikkerhed og beredskab i telesektoren[1)]

Kapitel 1

Anvendelsesområde og definitioner

§ 1. Denne lov finder anvendelse for teleudbydere, der med et kommercielt formål stiller offentlige elektroniske kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester til rådighed i Danmark, jf. dog stk. 2.

Stk. 2. Loven finder ikke anvendelse for kommuner og regioner, der stiller offentlige elektroniske kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester til rådighed.

§ 2. I denne lov forstås ved følgende:

1) Beredskabssituationer og andre ekstraordinære situationer: Situationer, hvor der allerede er, eller hvor der kan opstå større ulykker, katastrofer eller hændelser, herunder krise eller krig, og hvor der er risiko for påvirkning af udbuddet af net og tjenester.
2) Cybertrussel: Enhver potentiel omstændighed, begivenhed eller handling, som kan skade, forstyrre eller på anden måde have en negativ indvirkning på net- og informationssystemer, brugerne af sådanne systemer og andre personer.
3) Elektronisk kommunikationsnet: Transmissionssystem, uanset om det bygger på en permanent infrastruktur eller en centraliseret administrati-onskapacitet, og, hvor det er relevant, koblings- og dirigeringsudstyr og andre ressourcer, herunder netelementer, der ikke er aktive, som gør det muligt at overføre signaler ved hjælp af trådforbindelse, radiobølger, lysleder-teknik eller andre elektromagnetiske midler, herunder satellitnet, jordbaserede fastnet (kredsløbs- og pakkekoblede, herunder i internettet) og mobilnet, elkabelsystemer, i det omfang de anvendes til transmission af signaler, net, som anvendes til radio- og tv-spredning, og kabel-tv-net, uanset hvilken type information der overføres.
4) Elektronisk kommunikationstjeneste: En tjeneste, som normalt ydes mod betaling via elektroniske kommunikationsnet, og som med undtagelse af tjenester, der består i tilrådighedsstillelse af eller udøvelse af redaktionel kontrol over indhold fremført via elektroniske kommunikationsnet og -tjenester, omfatter følgende typer tjenester
   a) internetadgangstjenester,
   b) interpersonelle kommunikationstjenester og
   c) tjenester, der udelukkende eller overvejende består i overføring af signaler, som f.eks. transmissionstjenester, der anvendes til levering af maskine-til-maskine-tjenester og til radio- og tv-spredning.
5) Hændelse: En begivenhed, der bringer tilgængeligheden, autenticiteten, integriteten eller fortroligheden af lagrede, overførte eller behandlede data eller af de tjenester, der tilbydes af eller er tilgængelige via net- og informationssystemer, i fare.
6) Håndtering af hændelser: Enhver handling og procedure, der tager sigte på at forebygge, opdage, analysere og inddæmme eller at reagere på og reetablere sig efter en hændelse.
7) Interpersonel kommunikationstjeneste: En tjeneste, som normalt ydes mod betaling, og som muliggør direkte interpersonel og interaktiv informationsudveksling via elektroniske kommunikationsnet mellem et afgrænset antal personer, hvor de personer, der indleder eller deltager i kommunikationen, bestemmer

[1)] Loven gennemfører dele af Europa-Parlamentets og Rådets direktiv 2018/1972/EU af 11. december 2018 om oprettelse af en europæisk kodeks for elektronisk kommunikation (omarbejdning), EU-Tidende 2018, nr. L 321, side 36. Loven gennemfører desuden dele af Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen, om ændring af forordning (EU) nr. 910/2014 og direktiv (EU) 2018/1972 og om ophævelse af direktiv (EU) 2016/1148 (NIS 2-direktivet), EU-Tidende 2022, nr. L 333, side 80.

Min. for Samfundssikkerhed og Beredskab, j.nr. 2025-75

hvem modtageren eller modtagerne skal være, undtaget tjenester, der blot muliggør interpersonel og interaktiv kommunikation som en mindre støttefunktion, der er tæt knyttet til en anden tjeneste.

8) Net- og informationssystem:
   a) Et elektronisk kommunikationsnet, jf. nr. 3.
   b) Enhver anordning eller gruppe af forbundne eller beslægtede anordninger, hvoraf en eller flere ved hjælp af et program udfører automatisk behandling af digitale data.
   c) Digitale data, som lagres, behandles, fremfindes eller overføres af elementer i litra a og b med henblik på deres drift, brug, beskyttelse og vedligeholdelse.
9) Nærvedhændelse: En begivenhed, der kunne have bragt tilgængeligheden, autenticiteten, integriteten eller fortroligheden af lagrede, overførte eller behandlede data eller af de tjenester, der tilbydes af eller er tilgængelige via net- og informationssystemer, i fare, men som det lykkedes at forhindre, eller som ikke indtraf.
10) Offentligt elektronisk kommunikationsnet: Et elektronisk kommunikationsnet, som udelukkende eller overvejende bruges til udbud af elektroniske kommunikationstjenester, der er tilgængelige for offentligheden, og som danner grundlag for overførsel af information mellem nettermineringspunkter.
11) Offentligt tilgængelige elektroniske kommunikationstjenester: En elektronisk kommunikationstjeneste, jf. nr. 4, der stilles til rådighed for en ikke på forhånd afgrænset kreds af slutbrugere eller teleudbydere.
12) Radiobaseret lokalnet: Et trådløst adgangssystem med lav effekt og lille rækkevidde, der har en lav risiko for at skabe interferens med andre sådanne systemer etableret i nærheden af andre brugere, og som på et ikkeeksklusivt grundlag anvender harmoniserede radiofrekvenser.
13) Sikkerhed i net- og informationssystemer: Net- og informationssystemers, jf. nr. 8, evne til, på et givet sikkerhedsniveau, at modstå enhver begivenhed, der kan være til skade for tilgængeligheden, autenticiteten, integriteten eller fortroligheden af lagrede, overførte eller behandlede data eller af de tjenester, der tilbydes af eller er tilgængelige via disse net- og informationssystemer.
14) Teleudbyder: Den, der med et kommercielt formål stiller produkter af offentlige elektroniske kommunikationsnet og offentligt tilgængelige elektroniske kommunikationstjenester til rådighed for andre.
15) Væsentlig cybertrussel: En cybertrussel, som på grundlag af sine tekniske karakteristika kan antages at have potentiale til at få alvorlig indvirkning på en udbyders net- og informationssystemer eller på brugerne af udbyderens tjenester ved at forårsage betydelig fysisk eller ikke fysisk skade

Væsentlige udbydere

§ 3. Teleudbydere, der med et kommercielt formål udbyder offentlige elektroniske kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester som deres hovedydelse, eller som en ikke-accessorisk del af virksomheden, anses for at være væsentlige, hvis de opfylder én af følgende betingelser, jf. dog stk. 2:

1) Udbyderen beskæftiger mere end 50 ansatte.
2) Udbyderen har en årlig omsætning på over 10 mio. EUR og en årlig balance på over 10 mio. EUR.

Stk. 2. Uanset teleudbyderens størrelse anses følgende teleudbydere for at være væsentlige teleudbydere:

1) Teleudbyderen er den eneste udbyder i Danmark af et net eller en tjeneste, der er væsentlig for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter.
2) En forstyrrelse af det net eller den tjeneste, som teleudbyderen leverer, vil kunne have væsentlig indvirkning på den offentlige sikkerhed eller folkesundheden. ¬3) En forstyrrelse af det net eller den tjeneste, teleudbyderen leverer, vil kunne medføre en væsentlig systemisk risiko, herunder hvor en sådan forstyrrelse kan have en grænseoverskridende virkning.
4) Teleudbyderen er kritisk på grund af udbyderens specifikke betydning på nationalt eller regionalt plan for sektoren eller typen af net eller tjeneste eller for andre indbyrdes afhængige sektorer i Danmark.
5) Teleudbyderen er identificeret som en kritisk enhed i henhold til lov om kritiske enheders modstandsdygtighed.

Stk. 3. Ministeren for samfundssikkerhed og beredskab kan fastsætte nærmere regler om kriterier for, hvornår enheder er omfattet af stk. 2.

Vigtige udbydere

§ 4. Teleudbydere, der ikke opfylder kriterierne for at være væsentlige udbydere efter lovens § 3, anses som vigtige teleudbydere, såfremt de med et kommercielt formål udbyder offentlige elektroniske kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester som deres hovedydelse, eller som en ikke-accessorisk del af virksomheden.

Stk. 2. Styrelsen for Samfundssikkerhed kan træffe afgørelse om, at en teleudbyder, der er omfattet af § 3, stk. 2, nr. 1-4, skal anses som en vigtig teleudbyder.

Kapitel 2

Foranstaltninger til styring af sikkerhedsrisici m.v.

§ 5. Væsentlige og vigtige teleudbydere skal træffe passende og forholdsmæssige tekniske, operationelle og organisatoriske foranstaltninger for at styre risiciene for sikkerheden i net- og informationssystemer, som disse udbydere anvender til deres operationer eller til at levere deres tjenester, og for at forhindre hændelser eller minimere hændelsers indvirkning på modtagere af deres tjenester og på andre tjenester. Foranstaltningerne skal som minimum omfatte følgende:

1) Politikker for risikoanalyse og informationssystemsikkerhed.
2) Håndtering af hændelser.
3) Driftskontinuitet, herunder backup-styring og reetablering efter en katastrofe, og krisestyring.
4) Forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem den enkelte teleudbyder og udbyderens direkte leverandører eller tjenesteudbydere.
5) Sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer, herunder håndtering og offentliggørelse af sårbarheder.
6) Politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af sikkerhedsrisici.
7) Grundlæggende cyberhygiejnepraksisser og cybersikkerhedsuddannelse.
8) Politikker og procedurer vedrørende brug af kryptografi og, hvor det er relevant, kryptering.
9) Personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver.
10) Brug af løsninger med multifaktorautentificering eller kontinuerlig autentificering, sikret tale-, video- og tekstkommunikation og sikrede nødkommunikationssystemer internt hos udbyderen, hvor det er relevant.

Stk. 2. Væsentlige og vigtige teleudbyder, der ikke overholder ét eller flere af de krav, der er nævnt i stk. 1, til foranstaltningerne eller regler om krav til foranstaltninger fastsat i medfør af stk. 3, skal uden unødigt ophold træffe alle nødvendige, passende og forholdsmæssige korrigerende foranstaltninger.

Stk. 3. Ministeren for samfundssikkerhed og beredskab fastsætter regler om krav til foranstaltninger efter stk. 1, og om yderligere foranstaltninger og krav hertil for teleudbydere omfattet af denne lov. Ministeren kan i den forbindelse fastsætte regler om, at væsentlige og vigtige teleudbydere skal anvende særlige IKT-produkter, -tjenester og -processer, som er certificeret i henhold til en europæisk cybersikkerhedscertificeringsordning for at påvise overensstemmelse med bestemte krav efter stk. 1, eller regler om krav til foranstaltninger fastsat i medfør af 1. pkt.

§ 6. De foranstaltninger, som væsentlige og vigtige teleudbydere træffer på baggrund § 5, stk. 1 og 2, samt regler fastsat i medfør af § 5, stk. 3, skal være godkendt af teleudbyderens ledelsesorgan. Ledelsesorganet fører tilsyn med foranstaltningernes gennemførelse.

Stk. 2. Medlemmerne af ledelsesorganet i væsentlige og vigtige teleudbydere skal deltage i relevante kurser om styring af informationssikkerhedsrisici og tilskynde til, at tilsvarende kurser tilbydes til udbyderens øvrige ansatte.

Kapitel 3

Oplysnings- og underretningspligter mv.

§ 7. Væsentlige og vigtige teleudbydere skal registrere sig hos Styrelsen for Samfundssikkerhed og i den forbindelse oplyse følgende:
1) Teleudbyderens navn.
2) Teleudbyderens adresse og ajourførte kontaktoplysninger, herunder e-mailadresser, IP-intervaller og telefonnumre.
3) En liste over de øvrige medlemsstater i Den Europæiske Union, hvor teleudbyderen leverer tjenester, der er omfattet af anvendelsesområdet i artikel 2 i NIS 2-direktivet.

Stk. 2. Væsentlige og vigtige teleudbydere skal indgive oplysningerne efter stk. 1, senest to uger efter, at teleudbyderen omfattes af loven.

Stk. 3. I tilfælde af ændring i de oplysninger, der er afgivet i medfør af stk. 1, skal den væsentlige eller vigtige teleudbyder give Styrelsen for Samfundssikkerhed underretning herom senest to uger efter datoen for ændringen.

Stk. 4. Ministeren for samfundssikkerhed og beredskab kan fastsætte regler om, at væsentlige og vigtige teleudbydere skal afgive yderligere oplysninger ved registrering.

Stk. 5. Ministeren for samfundssikkerhed og beredskab kan fastsætte regler om oplysnings- og underretningspligter for væsentlige og vigtige teleudbydere, herunder regler om følgende:
1) Afgivelse af oplysninger om væsentlige dele af teleudbyderens net eller tjenester eller driften heraf.
2) Krav om underretning af Styrelsen for Samfundssikkerhed ved påtænkt indgåelse af aftaler om leverancer, der vedrører væsentlige dele af udbyderens net eller tjenester eller driften heraf.
3) Krav om, at teleudbyderen skal indsende et endeligt aftaleudkast til Styrelsen for Samfundssikkerhed umiddelbart forud for indgåelse af aftalen, og at aftalen først kan indgås op til 25 arbejdsdage efter styrelsens modtagelse af pågældende udkast.

§ 8. Bestemmelsen i § 17 i lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS 2-loven) om Computer Security Incident Response Teams (CSIRT) opgaver finder tilsvarende anvendelse for teleudbydere omfattet denne lov.

Stk. 2. Teleudbydere skal underrette Styrelsen for Samfundssikkerhed og CSIRT'en om enhver væsentlig hændelse efter proceduren i § 9.

Stk. 3. En hændelse anses for at være væsentlig, hvis den
1) har forårsaget eller er i stand til at forårsage alvorlige driftsforstyrrelser af net eller tjenester eller økonomiske tab for den berørte udbyder, eller
2) har påvirket eller er i stand til at påvirke andre fysiske eller juridiske personer ved at forårsage betydelig fysisk eller ikke-fysisk skade.

Stk. 4. Ministeren for samfundssikkerhed og beredskab kan fastsætte nærmere regler om, hvornår en hændelse kan anses for at være væsentlig og hvilke oplysninger, der skal gives i forbindelse med underretningen.

§ 9. Underretningen efter § 8, stk. 2, skal bestå af følgende og ske på følgende måde:
1) En tidlig varsling, som skal angive, om den væsentlige hændelse mistænkes at være forårsaget af ulovlige eller ondsindede handlinger eller kunne have en grænseoverskridende virkning, sendes uden unødigt ophold og se-

nest inden for 24 timer efter, at teleudbyderen har fået kendskab til den væsentlige hændelse.

2) En hændelsesunderretning, som skal ajourføre oplysningerne fra den tidlige varsling, jf. nr. 1, og give en indledende vurdering af den væsentlige hændelse, herunder dens alvor og indvirkning samt kompromitteringsindikatorerne, hvor sådanne foreligger, sendes uden unødigt ophold og senest inden for 72 timer efter, at teleudbyderen har fået kendskab til den væsentlige hændelse, jf. dog stk. 2.
3) En foreløbig rapport med relevante statusopdateringer sendes til enten Styrelsen for Samfundssikkerhed eller CSIRT'en efter myndighedens anmodning herom.
4) En endelig rapport sendes til Styrelsen for Samfundssikkerhed og CSIRT'en senest en måned efter fremsendelsen af den hændelsesunderretning, der er omhandlet i nr. 2. Den endelige rapport skal indeholde følgende:
   a) En detaljeret beskrivelse af hændelsen, herunder dens alvor og indvirkning.
   b) Den type trussel eller grundlæggende årsag, der sandsynligvis har udløst hændelsen.
   c) Anvendte og igangværende afbødende foranstaltninger.
   d) De eventuelle grænseoverskridende virkninger af hændelsen.
5) Pågår hændelsen fortsat på tidspunktet for fremsendelsen af den endelige rapport, jf. nr. 4, skal den berørte teleudbyder indsende en statusrapport på det pågældende tidspunkt og en endelig rapport senest en måned efter, at hændelsen er håndteret.

Stk. 2. Styrelsen for Samfundssikkerhed og CSIRT'en sikrer, at den berørte teleudbyder uden unødigt ophold og senest inden for 24 timer efter modtagelsen af den tidlige varsling, jf. stk. 1, nr. 1, gives et svar, herunder indledende tilbagemeldinger om den væsentlige hændelse. Efter anmodning fra teleudbyderen skal CSIRT'en desuden yde vejledning, operativ rådgivning om gennemførelsen af mulige afbødende foranstaltninger og supplerende teknisk bistand.

§ 10. Teleudbydere kan underrette Styrelsen for Samfundssikkerhed og CSIRT'en om hændelser, nærvedhændelser og cybertrusler.

Stk. 2. Styrelsen for Samfundssikkerhed og CSIRT'en behandler underretninger efter stk. 1 på samme måde som underretninger modtaget i medfør af § 8. CSIRT'en og Styrelsen for Samfundssikkerhed kan prioritere håndteringen af underretninger, der er modtaget i medfør af § 8 frem for underretninger efter stk. 1.

Stk. 3. Teleudbydere kan, uanset om de er omfattet af lovens anvendelsesområde, give frivillig underretning til CSIRT'en efter stk. 1.

§ 11. Er det sandsynligt, at en væsentlig hændelse, jf. § 8, stk. 3, vil påvirke teleudbyderens levering af deres tjenester til modtagerne heraf negativt, underretter teleudbyderen i relevant omfang modtagerne herom uden unødigt ophold.

Stk. 2. Teleudbydere oplyser uden unødigt ophold modtagerne af deres tjenester, som potentielt er berørt af en væsentlig cybertrussel, om eventuelle foranstaltninger eller modforholdsregler, som modtagerne kan træffe som reaktion på den pågældende trussel. Hvor det er relevant, skal udbyderne også informere de pågældende modtagere om selve den væsentlige trussel.

§ 12. Styrelsen for Samfundssikkerhed kan efter høring af en teleudbyder, der er ramt af en væsentlig hændelse, jf. § 8, stk. 3 informere offentligheden om den væsentlige hændelse, hvis offentliggørelsen er nødvendig for at forebygge eller håndtere hændelsen, eller hvis offentliggørelse af hændelsen på anden vis er i offentlighedens interesse.

Stk. 2. Styrelsen for Samfundssikkerhed kan i de situationer, der er nævnt i stk. 1, træffe afgørelse om, at den relevante teleudbyder informerer offentligheden om den væsentlige hændelse og bestemme, hvordan denne information skal gives.

Stk. 3. CSIRT'en kan efter samme kriterier som i stk. 1 informere offentligheden om væsentlige hændelser, der kan påvirke mere end én sektor.

Stk. 4. CSIRT'en kan efter samme kriterier som i stk. 1 informere offentligheden om væsentlige hændelser i andre medlemsstater.

Kapitel 4

Beredskabssituationer og andre ekstraordinære situationer

§ 13. Styrelsen for Samfundssikkerhed koordinerer og prioriterer beredskabsaktørernes behov for samfundsvigtig elektronisk kommunikation i beredskabssituationer og i andre ekstraordinære situationer.

Stk. 2. Væsentlige og vigtige teleudbydere skal sikre, at de foretagne prioriteringer gennemføres i net og tjenester.

Stk. 3. Væsentlige og vigtige teleudbydere skal underrette Styrelsen for Samfundssikkerhed i tilfælde, hvor udbyderen aktiverer sit beredskab, eller hvor udbyderen bliver bekendt med en hændelse, som vurderes at kunne føre til en beredskabssituation eller en anden ekstraordinær situation for teleudbyderen selv eller for en anden udbyder. Ministeren for samfundssikkerhed og beredskab kan fastsætte nærmere regler om underretningspligten efter 1. pkt.

Stk. 4. Teleudbydere, som i medfør af lov om elektroniske kommunikationsnet og -tjenester skal udsende offentlige advarsler om overhængende eller truende alvorlige nødsituationer og katastrofer, skal træffe alle nødvendige foranstaltninger til at sikre uafbrudt transmission af advarslerne. Ministeren for samfundssikkerhed og beredskab kan fastsætte nærmere regler om foranstaltninger efter 1. pkt.

Stk. 5. I beredskabssituationer og i andre ekstraordinære situationer kan Styrelsen for Samfundssikkerhed påbyde væsentlige og vigtige teleudbydere uden unødigt ophold at iværksætte nærmere angivne sikkerhedsforanstaltninger. Ministeren for samfundssikkerhed og beredskab, kan fastsætte regler om de sikkerhedsforanstaltninger, der er nævnt i 1. pkt.

Stk. 6. I beredskabssituationer og i andre ekstraordinære situationer skal væsentlige teleudbydere efter påbud fra Styrelsen for Samfundssikkerhed prioritere retablering af nærmere angivne dele af udbyderens beskadigede infrastruktur.

Stk. 7. I beredskabssituationer og i andre ekstraordinære situationer, hvor der opstår kapacitetsproblemer, skal væsentlige teleudbydere efter påbud fra Styrelsen for Samfundssikkerhed prioritere fremførsel i net af nærmere angivne forbindelser og tjenester, herunder om nødvendigt afbryde andre forbindelser eller tjenester helt eller delvist.

Kapitel 5

Aktindsigt i oplysninger og underretninger

§ 14. Underretninger modtaget i medfør af § 8, stk. 2, og § 10 er undtaget fra aktindsigt efter lov om offentlighed i forvaltningen og partsaktindsigt efter forvaltningsloven.

§ 15. Det kan i regler udstedt i medfør af § 7, stk. 5, fastsættes, at underretninger og afgivelse af oplysninger efter denne bestemmelser er undtaget fra aktindsigt efter lov om offentlighed i forvaltningen og partsaktindsigt efter forvaltningsloven.

Kapitel 6

Sikkerhedsgodkendelser

§ 16. Medarbejdere hos væsentlige og vigtige teleudbydere og repræsentanter for disse udbydere skal sikkerhedsgodkendes af Styrelsen for Samfundssikkerhed, når én af følgende betingelser er opfyldt:

1) Det er nødvendigt i forhold til den pågældendes adgang til klassificeret information eller til de funktioner, som den pågældende skal varetage.
2) Den pågældende varetager kontakten til Styrelsen for Samfundssikkerhed i relation til beredskabet i henhold til regler, der er udstedt i medfør af § 13, stk. 3.

Stk. 2. Ministeren for samfundssikkerhed og beredskab kan efter forhandling med justitsministeren fastsætte regler om ansøgninger vedrørende sikkerhedsgodkendelser, herunder betingelser for indgivelse af sådanne ansøgninger samt meddelelse og tilbagekaldelse af sikkerhedsgodkendelser.

Kapitel 7

Tilsyn og håndhævelse

§ 17. Styrelsen for Samfundssikkerhed fører tilsyn med overholdelse af denne lov og regler, der er udstedt i medfør af loven.

§ 18. Styrelsen for Samfundssikkerhed kan påbyde væsentlige og vigtige teleudbydere at inddrage nærmere angivne områder af deres virksomhed og nærmere angivne trusler mod sikkerheden i net- og informationssystemer i deres foranstaltninger efter § 5, stk. 1.

Stk. 2. Er det af væsentlig samfundsmæssig betydning, kan Styrelsen for Samfundssikkerhed påbyde væsentlige og vigtige teleudbydere at træffe konkrete foranstaltninger med henblik på at sikre sikkerheden i net- og informationssystemer, herunder påbud om, at udstyr, der skal anvendes i forbindelse med indgreb i meddelelseshemmeligheden, skal opsættes i og drives fra Danmark. Ministeren for samfundssikkerhed og beredskab kan fastsætte nærmere regler om påbud om foranstaltninger efter 1. pkt.

Tilsyns- og kontrolforanstaltninger for væsentlige teleudbydere

§ 19. Styrelsen for Samfundssikkerhed kan anvende følgende tilsynsforanstaltninger over for en væsentlig teleudbyder:

1) Uden retskendelse og mod behørig legitimation foretage kontrol hos teleudbydere samt deres samarbejdspartnere, leverandører eller underleverandører i relation til outsourcet aktivitet og eksternt tilsyn, herunder foretage stikprøvekontroller.
2) Foretage regelmæssige og målrettede sikkerhedsaudits eller stille krav om, at teleudbyderen får et kvalificeret uafhængigt organ til at foretage disse audits, og at resultaterne heraf stilles til rådighed for Styrelsen for Samfundssikkerhed.
3) Foretage sikkerhedsaudits ad hoc.
4) Foretage sikkerhedsscanninger.
5) Kræve at få udleveret oplysninger, der er nødvendige for at vurdere de foranstaltninger til styring af sikkerhedsrisici, som den berørte udbyder har indført.
6) Kræve at få adgang til data, dokumenter og oplysninger, der er nødvendige for udførelsen af tilsynsopgaven, herunder til afgørelse af om et forhold er omfattet af denne lov eller regler udstedt i medfør af loven.
7) Kræve at få udleveret dokumentation for gennemførelsen af sikkerhedspolitikker.
8) Kræve at få skriftlige udtalelser og redegørelser om faktiske forhold af betydning for Styrelsen for Samfundssikkerheds tilsynsvirksomhed.

Stk. 2. Ved anvendelsen af tiltagene i stk. 1, nr. 5-8, skal Styrelsen for Samfundssikkerhed angive formålet med tiltaget og præcisere, hvilke oplysninger der kræves udleveret og hvordan og i hvilken form oplysningerne og materialet nævnt i stk. 1, nr. 5-8, skal udleveres.

Håndhævelsesforanstaltninger for væsentlige teleudbydere

§ 20. Styrelsen for Samfundssikkerhed kan anvende følgende håndhævelsesforanstaltninger over for en væsentlig teleudbyder:

1) Udstede advarsler om teleudbyderens overtrædelse af kapitel 2-4, og regler udstedt i medfør af bestemmelser i disse kapitler.
2) Udstede bindende instrukser, herunder vedrørende foranstaltninger, der er nødvendige for at forhindre eller afhjælpe en hændelse, samt frister for gennemførelse af sådanne foranstaltninger og for rapportering om deres gennemførelse eller pålægge de pågældende enheder at afhjælpe de konstaterede mangler eller overtrædelserne af lovens kapitel 2-4, og regler udstedt i medfør af bestemmelser i disse kapitler.
3) Påbyde teleudbyderen at træffe foranstaltninger, der er nødvendige for at forhindre eller afhjælpe en hændelse.
4) Meddele teleudbyderen påbud og forbud for at sikre overholdelsen af de krav, der er fastsat i loven kapitel 2-4, og regler udstedt i medfør af bestemmelserne i disse kapitler.

5) Påbyde teleudbyderen at underrette de fysiske eller juridiske personer, som teleudbyderen leverer tjenester til eller udfører aktiviteter for, og som potentielt kan være berørt af en væsentlig trussel, om denne trussels karakter samt om eventuelle beskyttelsesforanstaltninger eller afhjælpende foranstaltninger, som de fysiske eller juridiske personer kan træffe som reaktion på denne trussel.
6) Påbyde teleudbyderen at gennemføre de anbefalinger, der er fremsat i forbindelse med en gennemført sikkerhedsaudit.
7) Udpege en person med ansvar for i en nærmere fastsat periode at føre tilsyn med teleudbyderens overholdelse af kapitel 2 og 3 samt regler udstedt i medfør heraf.
8) Påbyde udbyderen i ikke-anonymiseret form og på en nærmere angiven måde at offentliggøre afgørelser om håndhævelsesforanstaltninger efter nr. 1-5 samt resumeer af domme eller bødevedtagelser, hvor der idømmes eller vedtages en bøde.

§ 21. Har én eller flere af de håndhævelsesforanstaltninger, der er pålagt i medfør af § 20, nr. 1-8, vist sig at være utilstrækkelige, kan Styrelsen for Samfundssikkerhed fastsætte en frist, inden for hvilken den væsentlige teleudbyder skal foretage de nødvendige tiltag for at afhjælpe manglerne eller opfylde Styrelsen for Samfundssikkerheds krav. Er manglerne ikke afhjulpet eller Styrelsen for Samfundssikkerheds krav ikke opfyldt inden for den fastsatte frist, kan Styrelsen for Samfundssikkerhed træffe afgørelse om følgende:

1) Midlertidigt at suspendere en certificering eller godkendelse vedrørende dele af eller alle de relevante tjenester, som teleudbyderen leverer, eller aktiviteter, der udføres af teleudbyderen.
2) Midlertidigt at forbyde enhver fysisk person med ledelsesansvar på niveau med administrerende direktør eller den juridiske repræsentant hos udbyderen at udøve ledelsesfunktioner hos den pågældende teleudbyder.

Stk. 2. Suspensioner eller forbud, som er pålagt i medfør af stk. 1, kan kun anvendes, indtil den væsentlige teleudbyder træffer de nødvendige tiltag for at afhjælpe de mangler eller opfylde de krav, som gav anledning til, at foranstaltningerne blev anvendt.

Stk. 3. En afgørelse efter stk. 1 kan af den væsentlige teleudbyder eller den fysiske person, som afgørelsen vedrører, forlanges indbragt for domstolene. Styrelsen for Samfundssikkerhed anlægger i givet fald sag inden for rammerne af den civile retspleje mod den teleudbyder eller person, som har forlangt sagen indbragt.

Stk. 4. Ministeren for samfundssikkerhed og beredskab fastsætter regler om, hvilke certificeringer og godkendelser, der er omfattet af stk. 1, nr. 1.

Tilsyns- og kontrolforanstaltninger for vigtige teleudbydere

§ 22. Styrelsen for Samfundssikkerhed kan som led i sit tilsyn, hvis der er indikationer på, at en vigtig teleudbyder ikke overholder eller ikke har overholdt denne lov eller regler udstedt i medfør af loven anvende følgende tilsyns- og kontrolforanstaltninger:

1) Uden retskendelse og mod behørig legitimation foretage kontrol hos teleudbydere samt deres samarbejdspartnere, leverandører eller underleverandører i relation til outsourcet aktivitet og eksternt tilsyn, herunder foretage stikprøvekontroller og eksternt efterfølgende tilsyn.
2) Foretage målrettede sikkerhedsaudits eller stille krav om, at udbyderen får et kvalificeret uafhængigt organ til at foretage disse audits, og at resultaterne heraf stilles til rådighed for Styrelsen for Samfundssikkerhed.
3) Foretage sikkerhedsscanninger.
4) Kræve at få udleveret oplysninger, der er nødvendige for efterfølgende at vurdere de foranstaltninger til styring af sikkerhedsrisici, som den berørte udbyder har indført.
5) Kræve at få adgang til data, dokumenter og oplysninger, der er nødvendige for udførelsen af tilsynsopgaven, herunder til afgørelse af, om et forhold er omfattet af denne lov eller regler udstedt i medfør af loven.
6) Kræve at få udleveret dokumentation for gennemførelsen af sikkerhedspolitikker.
7) Kræve at få skriftlige udtalelser og redegørelser om faktiske forhold af betydning for Styrelsen for Samfundssikkerheds tilsynsvirksomhed.

Stk. 2. Ved anvendelse af tiltagene i stk. 1, nr. 4-7, skal Styrelsen for Samfundssikkerhed angive formålet med tiltaget og præcisere, hvilke oplysninger der kræves udleveret og hvordan og i hvilken form oplysningerne og materialet nævnt i stk. 1, nr. 4-7, skal udleveres.

§ 23. Styrelsen for Samfundssikkerhed kan anvende følgende håndhævelsesforanstaltninger over for en vigtig teleudbyder:

1) Udstede advarsler om teleudbyderens overtrædelse af kapitel 2-4, og regler udstedt i medfør heraf.
2) Udstede bindende instrukser, herunder vedrørende foranstaltninger, der er nødvendige for at forhindre eller afhjælpe en hændelse, samt frister for gennemførelse af sådanne foranstaltninger og for rapportering om deres gennemførelse eller pålægge de pågældende enheder at afhjælpe de konstaterede mangler eller overtrædelserne af lovens kapitel 2-4, og regler udstedt i medfør af bestemmelser i disse kapitler.
3) Meddele teleudbyderen påbud og forbud for at sikre overholdelsen af de krav, der er fastsat i loven eller regler udstedt i medfør af loven.
4) Påbyde teleudbyderen at underrette de fysiske eller juridiske personer, som udbyderen leverer tjenester til eller udfører aktiviteter for, og som potentielt kan være berørt af en væsentlig trussel, om denne trussels karakter samt om eventuelle beskyttelsesforanstaltninger eller afhjælpende foranstaltninger, som de fysiske eller juridiske personer kan træffe som reaktion på denne trussel.
5) Påbyde teleudbyderen at gennemføre de anbefalinger, der er fremsat i forbindelse med en gennemført sikkerhedsaudit.

6) Påbyde teleudbyderen i ikke-anonymiseret form og på en nærmere angiven måde at offentliggøre afgørelser om håndhævelsesforanstaltninger efter nr. 1-3, samt resumeer af domme eller bødevedtagelser, hvor der idømmes eller vedtages en bøde.

Høring af væsentlige og vigtige teleudbydere

§ 24. Inden Styrelsen for Samfundssikkerhed træffer afgørelse om at anvende håndhævelsesforanstaltninger efter §§ 20, 21 og 23 underrettes den væsentlige eller vigtige teleudbyder om de påtænkte håndhævelsesforanstaltninger og begrundelsen herfor. Styrelsen for Samfundssikkerhed skal give teleudbyderen en rimelig frist til at fremsætte bemærkninger, undtagen i tilfælde, hvor formålet med foranstaltningen ellers ville forspildes.

Offentliggørelse

§ 25. Styrelsen for Samfundssikkerhed kan i ikke-anonymiseret form offentliggøre følgende:

1) Afgørelser om påbud meddelt i medfør af § 13, stk. 5 og 7 og 18, stk. 1 og 2, og afgørelser truffet i medfør af regler, der er udstedt i medfør af § 7, stk. 5, nr. 1-3, § 13, stk. 5, 2. pkt., og § 18, stk. 2, 2. pkt.
2) Resultater af tilsyn efter §§ 19 og 22.
3) Resuméer af domme eller bødevedtagelser, hvor der idømmes eller vedtages en bøde for overtrædelse af denne lov eller regler, der er udstedt i medfør af denne lov.
4) Resuméer af domme i retssager, hvor Styrelsen for Samfundssikkerhed er part om forhold omfattet af denne lov.

Stk. 2. Offentliggørelse efter stk. 1 må ikke indeholde følgende:

1) Oplysninger om tekniske indretninger eller fremgangsmåder eller om drifts- eller forretningsforhold eller lignende, for så vidt det er af væsentlig økonomisk betydning for den væsentlige eller vigtige teleudbyder, som oplysningerne angår.
2) Oplysninger, der er af væsentlig betydning for statens sikkerhed eller rigets forsvar.
3) Klassificerede informationer.
4) Fortrolige oplysninger, der hidrører fra nationale tilsynsmyndigheder i andre EU-medlemsstater, medmindre de myndigheder, der har afgivet oplysningerne, har givet deres udtrykkelige tilladelse til offentliggørelse.
5) Oplysninger om enkeltpersoners private forhold.

Stk. 3. Ministeren for samfundssikkerhed og beredskab kan fastsætte regler om sagsbehandlingen i forbindelse med offentliggørelse efter stk. 1.

Kapitel 8

Videregivelse af oplysninger, gensidig bistand, gennemførelsesretsakter, digital kommunikation m.v.

§ 26. De forpligtelser, der er fastsat i denne lov eller i regler udstedt i medfør af loven, omfatter ikke meddelelse af oplysninger, hvis videregivelse ville stride mod væsentlige interesser af hensyn til den nationale sikkerhed, offentlige sikkerhed eller forsvar.

Stk. 2. Oplysninger, der modtages eller hidrører fra myndigheder i andre EU-medlemsstater, behandles som fortrolige, såfremt den afgivende myndighed betragter oplysningerne som fortrolige i henhold til EU-regler eller nationale regler.

§ 27. Styrelsen for Samfundssikkerhed kan hos væsentlige og vigtige teleudbydere indsamle oplysninger med henblik på at videregive disse til Kommissionen, Den Europæiske Unions Agentur for Cybersikkerhed eller nationale tilsynsmyndigheder i andre EU-medlemsstater, i det omfang det er nødvendigt for, at disse kan opfylde deres opgaver i forhold til traktatmæssige forpligtelser eller forpligtelser i henhold til den gældende EU-ret.

Stk. 2. Styrelsen for Samfundssikkerhed orienterer de væsentlige og vigtige teleudbydere som der er indsamlet oplysninger fra efter stk. 1, forud for videregivelse af oplysningerne til Kommissionen, Den Europæiske Unions Agentur for Cybersikkerhed eller nationale tilsynsmyndigheder i andre EU-medlemsstater.

§ 28. Hvor en væsentlig eller vigtig teleudbyder leverer tjenester i mere end én medlemsstat i Den Europæiske Union, eller hvor udbyderen leverer tjenester i en eller flere medlemsstater, og udbyderens net- og informationssystemer er beliggende i en eller flere andre medlemsstater, samarbejder Styrelsen for Samfundssikkerhed med de andre medlemsstaters kompetente myndigheder i relevant omfang. Samarbejdet indebærer følgende:

1) Styrelsen for Samfundssikkerhed underretter de kompetente myndigheder i relevante medlemsstater om tilsyns- og håndhævelsesforanstaltninger iværksat overfor teleudbydere i Danmark.
2) Styrelsen for Samfundssikkerhed kan anmode en anden medlemsstats kompetente myndigheder om at anvende tilsyns- og håndhævelsesforanstaltninger.
3) Styrelsen for Samfundssikkerhed yder i rimeligt omfang bistand til en anden medlemsstats kompetente myndighed efter modtagelse af en begrundet anmodning om at anvende tilsyns- og håndhævelsesforanstaltninger.

Stk. 2 Styrelsen for Samfundssikkerhed kan efter nærmere aftale gennemføre fælles tilsynstiltag med kompetente myndigheder fra andre medlemsstater i Den Europæiske Union.

§ 29. Ministeren for samfundssikkerhed og beredskab kan fastsætte regler, som er nødvendige for at gennemføre retsakter udstedt af Europa-Kommissionen i medfør af NIS 2-direktivet.

§ 30. Ministeren for samfundssikkerhed og beredskab kan fastsætte regler om digital kommunikation, herunder om anvendelsen af bestemte it-systemer og særlige digitale formater samt digital signatur eller lignende.

Kapitel 9

Straf

§ 31. Med bøde straffes den, der

1) overtræder § 5, stk. 1, eller 2, § 7, stk. 1-3, § 8, stk. 2, jf. stk. 3, § 9, stk. 1 og § 11, stk. 1 og 2,
2) undlader at efterkomme Styrelsen for Samfundssikkerheds afgørelse efter § 21, stk. 1, nr. eller 2.
3) undlader at efterkomme Styrelsen for Samfundssikkerheds påbud efter § 13, stk. 5, eller § 18, stk. 1 og 2,
4) undlader at efterkomme Styrelsen for Samfundssikkerheds krav efter § 19, stk. 1, nr. 5-8, eller § 22, stk. 1, nr. 4-7 eller
5) hindrer Styrelsen for Samfundssikkerhed i at føre tilsyn efter bestemmelserne i § 19, stk. 1, nr. 1-4, eller § 22, stk. 1, nr. 1-3.

Stk. 2. Der kan pålægges selskaber mv. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.

Stk. 3. I forskrifter, der udstedes i medfør af loven kan der fastsættes straf af bøde for overtrædelse af bestemmelserne i forskrifterne.

Kapitel 10

Ikrafttrædelse, overgangsbestemmelser og ændringer i anden lovgivning m.v.

§ 32. Loven træder i kraft den 1. juli 2025.

Stk. 2. Lov om sikkerhed i net og tjenester, jf. lovbekendtgørelse nr. 153 af 1. februar 2021, ophæves.

Stk. 3. Oplysningerne efter § 7, stk. 1, skal indgives senest den 1. oktober 2025.

§ 33. Loven gælder ikke for Færøerne og Grønland.

§ 34. I lov nr. 1156 af 8. juni 2021 om leverandørsikkerhed i den kritiske teleinfrastruktur foretages følgende ændringer:

1. *§ 1, nr. 3,* affattes således:
»3) Vigtig teleudbyder: En teleudbyder, som er identificeret som en vigtig teleudbyder i henhold til lov om sikkerhed og beredskab i telesektoren.«

2. I § 1 indsættes som *nr. 4:*
»4) Væsentlig teleudbyder: En teleudbyder, som er identificeret som en væsentlig teleudbyder i henhold til lov om sikkerhed og beredskab i telesektoren.«

3. I *§ 2, stk. 1, § 3, stk. 1* og *2*, og *§ 15*, ændres »væsentlig erhvervsmæssig udbyder af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester« til: »væsentlig eller vigtig teleudbyder«.

Bemærkninger til lovforslaget

Almindelige bemærkninger

Indholdsfortegnelse

1. Indledning

Danmark er blandt de mest digitaliserede samfund i verden. Et stærkt digitaliseret samfund som Danmark er i stigende grad afhængigt af telenettet, der bl.a. anvendes som platform for telefoni og datakommunikation. Det samlede telenet er således en af de mest kritiske dele af samfundets informations- og kommunikationsteknologiske infrastruktur. Det er en forudsætning for det digitale samfund, at mennesker og maskiner kan kommunikere digitalt på en sikker og effektiv måde. Tilgængelighed, fortrolighed og integritet af teletjenesterne er af kritisk betydning for samfundets funktion og sikkerhed.

Dermed er samfundet også særdeles sårbart, hvis dele af telenettet i kortere eller længere perioder er ude af drift.

Hertil kommer, at Danmark står over for et mere sammensat og komplekst trusselsbillede end for blot få år siden. Det gælder ikke mindst på cybersikkerhedsområdet, hvilket understreges af Center for Cybersikkerheds trusselsvurdering fra 2024. Det fremgår bl.a. heraf, at niveauet for cyberkriminalitet er MEGET HØJT, og at truslen fra cyberaktivisme er HØJ. Truslen fra destruktive cyberangreb er tidligere på året blevet hævet fra LAV til MIDDEL. Niveauet blev hævet på baggrund af en udvikling i Ruslands risikovillighed i forhold til at anvende hybride virkemidler, herunder destruktive cyberangreb, mod europæiske NATO-lande. Hertil kommer risikoen for sabotage og hærværk mod kritiske dele af teleinfrastrukturen. De store datamængder, som sendes via telenettet, indebærer desuden, at telenettet er et oplagt mål for aktører, der vil udøve industrispionage mod virksomheder eller spionage mod myndigheder og personer. I dag er

truslen fra cyberspionage blandt de mest alvorlige trusler, som vores samfund står overfor.

Danmarks sårbarhed over for bl.a. cybertruslen vil øges i takt med den fortsatte digitale udvikling. Den fortsatte digitale udvikling stiller nye og større krav til vores håndtering af sikkerheden i teleinfrastrukturen. Det gælder ikke kun i Danmark, men på tværs af EU. Net- og informationssystemer har udviklet sig til et centralt element i hverdagen med den hurtige digitale omstilling og forbundethed i samfundet, herunder i forbindelse med grænseoverskridende udvekslinger. Denne udvikling har ført til en udvidelse af antallet og typen af cybertrusler og skabt nye udfordringer, som kræver tilpassede, koordinerede og innovative svar i alle medlemsstater.

Dette er bl.a. baggrunden for, at Europa-Parlamentet og Rådet har vedtaget direktiv (EU) 2022/2555 af 14. december 2022 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen, om ændring af forordning (EU) nr. 910/2014 og direktiv (EU) 2018/1972 og om ophævelse af direktiv (EU) 2016/2259 (NIS 2-direktivet).

NIS 2-direktivet har til formål at skabe et højere og mere ensartet cybersikkerhedsniveau på tværs af medlemsstaterne. Direktivet stiller bl.a. cybersikkerhedskrav til virksomheder, myndigheder og organisationer (enheder) inden for en lang række samfundskritiske sektorer, som bl.a. omfatter energi, transport, bankvirksomhed, sundhed, drikke- og spildevand, digital infrastruktur og den offentlige forvaltning. Samtidig fastsættes en række oplysnings- og underretningspligter over for myndighederne, herunder underretning ved væsentlige hændelser samt pligt til at oplyse enhedernes brugere om bl.a. væsentlige hændelser og eventuelle modforholdsregler, som brugerne kan træffe. Direktivet styrker desuden myndighedernes tilsynsbeføjelser og håndhævelsesmuligheder.

Formålet med dette lovforslag er at implementere NIS 2-direktivet for telesektoren. Telesektoren spiller en afgørende rolle i et højt digitaliseret samfund som det danske. Der eksisterer derfor allerede omfattende regulering af informationssikkerhed og beredskab i telesektoren, herunder navnlig lov om sikkerhed i net og tjenester, jf. lovbekendtgørelse nr. 153 af 1. februar 2021, som ændret ved § 18 i lov nr. 1156 af 8. juni 2021. På visse områder, herunder navnlig i forhold til leverandørsikkerhed, vurderes den nuværende regulering om sikkerhed og beredskab i telesektoren at sikre et højere sikkerhedsniveau end det, der følger af NIS 2-direktivet.

Det er derfor Ministeriet for Samfundssikkerhed og Beredskabs vurdering, at implementeringen af NIS 2-direktivet for telesektoren bør ske særskilt, således at implementeringen af NIS 2-direktivets minimumskrav ikke medfører, at kravene i den eksisterende regulering for sikkerheden og beredskabet i telesektoren sænkes.

Forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau, der implementerer NIS 2-direktivet i de øvrige omfattede sektorer, fremsættes samtidig med nærværende lovforslag.

2. Baggrund

2.1. Formål

Formålet med lovforslaget er at implementere NIS 2-direktivet i telesektoren. Med dette lovforslag foreslås det, at implementeringen af NIS 2-direktivet i telesektoren sker gennem en integration med den eksisterende regulering på området, herunder navnlig lov om sikkerhed i net og tjenester, jf. lovbekendtgørelse nr. 153 af 1. februar 2021, som ændret ved § 18 i lov nr. 1156 af 8. juni 2021.

Med henblik på at skabe et ensartet og overskueligt regelsæt på teleområdet foreslås det derfor, at lov om sikkerhed i net og tjenester ophæves, og at implementeringen af NIS 2-direktivet i telesektoren og den eksisterende regulering på området samles i én lov.

Lov om sikkerhed i net og tjenester fastsætter en overordnet ramme for de informationssikkerheds- og beredskabskrav samt oplysnings- og underretningspligter, der gælder for teleudbydere, ligesom loven regulerer tilsyns- og håndhævelsesbeføjelser samt sanktionsmuligheder. Lovens bestemmelser om informationssikkerheds- og beredskabskrav samt oplysnings- og underretningspligter er primært udformet som bemyndigelser, der er udmøntet i fire bekendtgørelser.

Lov om sikkerhed i net og tjenester suppleres i øvrigt af lov nr. 1156 af 8. juni 2021 om leverandørsikkerhed i den kritiske teleinfrastruktur, som bl.a. giver myndighederne mulighed for at forbyde konkrete leverandøraftaler vedrørende den kritiske teleinfrastruktur, hvis aftalerne vurderes at udgøre en trussel mod statens sikkerhed.

Dele af lov om sikkerhed i net og tjenester og de bekendtgørelser, der er udstedt i medfør af loven, bygger på EU-regulering. Lovgivningen implementerer således en række bestemmelser i Europa-Parlamentets og Rådets direktiv (EU) 2018/1972 af 11. december 2018 om oprettelse af en europæisk kodeks for elektronisk kommunikation (EU's telekodeks).

2.1.1. Generelt om EU's telekodeks

Den 11. december 2018 vedtog Europa-Parlamentet og Rådet direktiv (EU) 2018/1972 om oprettelse af en europæisk kodeks for elektronisk kommunikation (EU's telekodeks). EU's telekodeks samler og reviderer de fire centrale EU-direktiver på teleområdet, herunder bl.a. rammedirektivet og forsyningspligtsdirektivet.

EU's telekodeks har til formål at forenkle EU-reguleringens struktur, således at der skabes en mere sammenhængende regulering af elektroniske kommunikationsnet og -tjenester. Samtidig tager EU's telekodeks højde for den samfundsmæssige udvikling, hvor forbrugere og virksomheder i stadig stigende grad anvender digitale, internetbaserede tje-

nester frem for traditionelle teletjenester. Samtidig har EU's telekodeks til formål at sikre, at digitale internetbaserede tjenester bliver omfattet af bl.a. passende informationssikkerhedskrav.

EU's telekodeks fastlægger en retlig ramme for reguleringen af elektronisk kommunikation og indeholder bl.a. bestemmelser om sikkerheden i offentlige elektroniske kommunikationsnet og offentligt tilgængelige elektroniske kommunikationstjenester. EU's telekodeks fastlægger således bl.a. overordnede sikkerhedskrav til samt oplysnings- og underretningspligter for teleudbydere.

Derudover fastlægger EU's telekodeks en generel forpligtelse for medlemsstaterne til at sikre, at der er kompetente myndigheder, som fører tilsyn med bl.a. teleudbydernes overholdelse af sikkerhedskravene- samt oplysnings- og underretningspligterne, ligesom direktivet – med henblik på at sikre overholdelsen heraf – fastlægger tilsyns- og håndhævelsesbeføjelser. Den centrale bestemmelse i den henseende er direktivets artikel 41, der ligeledes er implementeret i lov om sikkerhed i net og tjenester.

Endvidere indeholder EU's telekodeks mulighed for, at medlemsstaterne kan fastsætte sanktioner, herunder bøder, for overtrædelse af de fastsatte sikkerhedskrav samt oplysnings- og underretningspligter, som ligeledes er implementeret i lov om sikkerhed i net og tjenester.

De sikkerhedskrav samt oplysnings- og underretningspligter mv., der gælder for teleudbydere i dag, har således på EU-plan hidtil været fastlagt i EU's telekodeks, som nu suppleres af kravene i NIS 2-direktivet.

2.1.2. Generelt om NIS 2-direktivet

NIS 2-direktivet ophæver og erstatter Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (NIS 1-direktivet).

NIS 1-direktivet fastlægger for det første krav til rammerne for arbejdet med sikkerhed i net- og informationssystemer både nationalt og på EU-niveau, herunder krav til samarbejdsorganer og myndighedsstruktur. For det andet stiller direktivet krav om, at der fastsættes sikkerhedskrav og underretningspligter for operatører af væsentlige tjenester og udbydere af digitale tjenester. Med NIS 1-direktivet er der således allerede taget skridt hen mod at øge cybersikkerheden på tværs af EU.

Baggrunden for NIS 2-direktivet er, at der fra EU's side er konstateret store forskelle i medlemsstaternes gennemførelse af NIS 1-direktivet, herunder med hensyn til, hvilke enheder der anses for omfattet af direktivet, da afgrænsningen heraf i vid udstrækning blev overladt til medlemsstaternes skøn. NIS 1-direktivet giver også medlemsstaterne meget vide skønsbeføjelser med hensyn til gennemførelsen af direktivets sikkerheds- og hændelsesrapporteringsforpligtelser samt bestemmelserne om tilsyn og håndhævelse.

Formålet med NIS 2-direktivet er derfor at skabe et højere og mere ensartet cybersikkerhedsniveau på tværs af medlemsstaterne. NIS 2-direktivet omfatter også telesektoren og indebærer derfor bl.a., at artikel 40 og 41 i EU's telekodeks ophæves. Fremadrettet vil det således primært være NIS 2-direktivet, der på EU-plan fastlægger krav til og forpligtelser for teleudbydernes sikkerhed, ligesom medlemsstaternes tilsyns- og håndhævelsesbeføjelser samt sanktionsmuligheder over for teleudbyderne vil følge heraf.

Det følger af NIS 2-direktivets præambelbetragtning nr. 92, at baggrunden for ophævelsen af artikel 40 og 41 i EU's telekodeks er et ønske fra EU's side om at strømline de krav og forpligtelser til cybersikkerhed, der pålægges teleudbydere, med de krav og forpligtelser, der pålægges enheder i de øvrige sektorer mv., som omfattes af NIS 2-direktivets anvendelsesområde. Derudover er der fra EU's side et ønske om at gøre det muligt for teleudbyderne og myndighederne at drage fordel af de retlige rammer, der er fastsat i NIS 2-direktivet i forhold til samarbejdsorganer og myndighedsstruktur.

NIS 2-direktivet fastsætter på den baggrund nærmere regler for cybersikkerhedsforanstaltninger (artikel 21) og rapporteringsforpligtelser (artikel 23) og mekanismer for effektivt samarbejde på nationalt plan og på EU-plan (kapitel II og III), ligesom direktivet tilvejebringer styrkede tilsyns- og håndhævelsesbeføjelser (kapitel VII), der skal bidrage til at sikre en effektiv overholdelse og håndhævelse af forpligtelserne i direktivet.

2.1.3. Implementering af NIS 2-direktivet for telesektoren

Henset til, at NIS 2-direktivet omfatter telesektoren og ændrer i EU's telekodeks, er der behov for at tilpasse den gældende lov om sikkerhed i net og tjenester. Foruden bestemmelser, der implementerer EU's telekodeks, indeholder lov om sikkerhed i net og tjenester også nationale særregler, herunder skærpede krav til teleudbydernes informationssikkerhed og beredskab. Der er tale om krav, der på visse områder går videre end de krav, der følger af EU-reguleringen på området.

Baggrunden for indførelsen af de skærpede nationale særregler var navnlig at sikre, at kravene til teleudbydernes sikkerhed i højere grad tog højde for samfundets afhængighed af telenettet og afspejlede det aktuelle trusselsbillede, idet Forsvarets Efterretningstjeneste vurderede, at truslen fra især cyberangreb og avanceret industrispionage var stærkt stigende, jf. Folketingstidende 2015-16, tillæg A, L 10 som fremsat, side 5. Center for Cybersikkerhed har i centerets seneste trusselsvurdering om cybertruslen mod Danmark 2024 bl.a. vurderet, at truslen fra cyberspionage og cyberkriminalitet er MEGET HØJ, at truslen fra cyberaktivisme mod Danmark er HØJ, og at truslen fra destruktive cyberangreb er MIDDEL.

På baggrund af det skærpede trusselsbillede på cyberområdet og telesektorens samfundsmæssige kritikalitet som følge af danske myndigheders, virksomheders og borgeres afhængighed af en velfungerende teleinfrastruktur er det Ministeriet for Samfundssikkerhed og Beredskabs vurdering, at de eksisterende nationale særregler bør videreføres med henblik på at sikre en opretholdelse af det nuværende høje sikkerhedsniveau i telesektoren.

Idet de eksisterende nationale særregler ønskes videreført, finder Ministeriet for Samfundssikkerhed og Beredskab, at implementeringen af NIS 2-direktivet bør ske ved et sektorspecifikt lovforslag. Dermed vil kravene og forpligtelserne, der følger af NIS 2-direktivet, kunne integreres med den eksisterende regulering af sikkerheden og beredskab i telesektoren. Henset til, at implementeringen af NIS 2-direktivet vil berøre et større antal af bestemmelserne i den gældende lov om sikkerhed i net og tjenester, har Ministeriet for Samfundssikkerhed og Beredskab valgt at fremsætte forslag til en ny hovedlov frem for en ændring af den gældende lov. Det vurderes, at en ny hovedlov vil bidrage til at gøre den nye regulering mere overskuelig for teleudbyderne og andre aktører på området.

De nye cybersikkerhedskrav samt oplysnings- og underretningspligter, som følger af NIS 2-direktivet, vil blive gennemført ud fra princippet om direktivnær implementering. Dette lovforslag vil således ikke medføre, at teleudbydere i Danmark vil blive pålagt nye krav eller pligter, der vil gå videre end det, der følger af et NIS 2-direktivets minimumskrav. Henset til det aktuelle trusselsbillede, vil der dog ske en videreførelse af nationale regler, med henblik på at det aktuelle høje sikkerhedsniveau ikke lempes med implementeringen af NIS 2-direktivet.

Telesektoren er således ikke omfattet af forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau, som fremsættes af Ministeriet for Samfundssikkerhed og Beredskab samtidig med nærværende lovforslag, og som skaber en fælles lovgivningsramme på tværs af en række af de øvrige sektorer, der er omfattet af NIS 2-direktivet.

Det følger således af den foreslåede § 1, stk. 2, 2. pkt., i det samtidigt fremsatte forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS 2-loven), at loven ikke finder anvendelse på enheder i det omfang, de er omfattet af lov om cybersikkerhed i telesektoren. Det følger af bestemmelsens 3. pkt., at lovens § 17 dog finder anvendelse for bl.a. telesektoren.

Den foreslåede § 17 i lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau implementerer NIS 2-direktivets artikel 10, som forpligter medlemsstaterne til at oprette eller udpege en eller flere nationale kompetente myndigheder, et nationalt centralt kontaktpunkt samt en eller flere nationale CSIRT'er (Computer Security Incident Response Teams, dvs. enheder der håndterer it-sikkerhedshændelser).

Center for Cybersikkerhed blev ved implementeringen af NIS 1-direktivet udpeget som CSIRT i Danmark, og opgaven har hidtil været varetaget som en del af Netsikkerhedstjenesten i Center for Cybersikkerhed.

Med den kongelige resolution af 29. august 2024 er Center for Cybersikkerhed, bortset fra bl.a. Netsikkerhedstjenesten, blevet overdraget til Ministeriet for Samfundssikkerhed og Beredskab. Det bemærkes, at Center for Cybersikkerhed den 29. januar 2025 er blevet en del af den nyoprettede Styrelse for Samfundssikkerhed.

Med nærværende lovforslag lægges der op til, at bl.a. hændelser skal indberettes til både Styrelsen for Samfundssikkerhed og CSIRT'en. Det forudsættes på den baggrund, at der vil være et tæt samarbejde mellem Styrelsen for Samfundssikkerhed og CSIRT'en. En nærmere fastlæggelse af rammerne for samarbejdet vil kunne ske i en samarbejdsaftale.

Der henvises i øvrigt til kapitel 5 i det samtidigt fremsatte forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS 2-loven) og bemærkningerne hertil.

2.2. Sammenhængen med CER-direktivet

NIS 2-direktivet skal ses i sammenhæng med Europa-Parlamentets og Rådets direktiv (EU) 2022/2557 af 14. december 2022 om kritiske enheders modstandsdygtighed og om ophævelse af Rådets direktiv 2008/114/EF (CER-direktivet).

Ministeriet for Samfundssikkerhed og Beredskab fremsætter samtidig med nærværende lovforslag et lovforslag om kritiske enheders modstandsdygtighed, der vil implementere CER-direktivet på tværs af de omfattede sektorer med undtagelse af energisektoren.

CER-direktivet har til formål at styrke kritiske enheders modstandsdygtighed, således at de er bedre i stand til at håndtere risiciene for deres drift, som kan føre til forstyrrelse i leveringen af væsentlige tjenester. CER-direktivet fastlægger derfor bl.a. overordnede sikkerhedskrav og oplysnings- og underretningspligter samt tilsyns- og håndhævelsesbeføjelser, herunder sanktioner, i forhold til enheder, som medlemsstaterne identificerer som kritiske enheder inden for en række sektorer og delsektorer, ligesom direktivet fastsætter krav til myndighedsopgaver, herunder myndighedsstruktur og samarbejdsorganer.

Det følger imidlertid bl.a. af CER-direktivets artikel 8, at medlemsstaterne skal sikre, at direktivets sikkerhedskrav og oplysnings- og underretningspligter (kapitel III) samt tilsyns- og håndhævelsesbeføjelser, herunder sanktioner (kapitel VI), ikke finder anvendelse for enheder, der er omfattet af den digitale infrastruktur. Til denne kategori hører bl.a. teleudbydere.

Det følger af NIS 2-direktivets præambelbetragtning nr. 31, at baggrunden for denne undtagelse i CER-direktivets artikel 8 er, at teleudbydere i det væsentligste er baseret på net- og informationssystemer, og derfor bør de krav og for-

pligtelser, der pålægges disse i medfør af NIS 2-direktivet, omhandle sådanne systemers fysiske sikkerhed. Det følger endvidere af CER-direktivets præambelbetragtning nr. 20, at trusler mod sikkerheden i net- og informationssystemer kan have forskellig oprindelse, og NIS 2-direktivet anvender derfor en tilgang, der omfatter alle farer, og som omfatter net- og informationssystemers modstandsdygtighed samt disse systemers fysiske komponenter og fysiske miljø. Eftersom kravene og forpligtelserne i NIS 2-direktivet mindst svarer til de tilsvarende krav og forpligtelser i CER-direktivet, bør kravene og forpligtelserne ikke finde anvendelse på teleudbydere for at undgå dobbeltarbejde og unødvendige administrative byrder. Da disse spørgsmål således er omfattet af NIS 2-direktivet, finder de nævnte kapitler i CER-direktivet ikke anvendelse for teleudbydere.

Det skal imidlertid bemærkes, at medlemslandene ikke desto mindre skal identificere, hvilke teleudbydere der skal anses for kritiske enheder i henhold til CER-direktivets artikel 6.

3. Lovforslagets hovedpunkter

3.1. Teleudbyderbegrebet

3.1.1. Gældende ret

Der er i lov om sikkerhed i net og tjenester bl.a. fastsat regler om informationssikkerheds- og beredskabskrav til samt oplysnings- og underretningspligter for de teleudbydere, der er omfattet af artikel 40 og 41 i EU's telekodeks omkring sikkerhed i net og tjenester.

3.1.1.1. Kategorisering af typer af udbydere

I lov om sikkerhed i net og tjenester skelnes mellem udbyder, erhvervsmæssige udbydere og udbydere af nummeruafhængige interpersonelle kommunikationstjenester (NU-IK-tjenester).

En udbyder defineres i lov om sikkerhed i net og tjenesters § 2, nr. 4, som den, der med et kommercielt formål stiller produkter, elektroniske kommunikationsnet eller -tjenester til rådighed for andre. Det fremgår af bemærkningerne til lovens § 2, nr. 4, jf. Folketingstidende 2015-16, A, L 10 som fremsat den 7. oktober 2015, at definitionen indholdsmæssigt er identisk med den tilsvarende definition i telelovens § 2, nr. 1, og skal fortolkes i overensstemmelse med denne bestemmelses forarbejder og relevante praksis.

Det fremgår af bemærkningerne til telelovens § 2, nr. 1, jf. Folketingstidende 2015-16, A, L 10 som fremsat den 7. oktober 2015, at enhver, der markedsfører og sælger produkter og elektroniske kommunikationsnet eller -tjenester omfattet af lovforslaget til andre, anses for at være udbydere med de rettigheder, dette giver bl.a. i relation til netadgang. Det vil sige, at alle virksomheder, som på kommercielt grundlag betjener andre slutbrugere eller udbydere af elektroniske kommunikationsnet eller -tjenester med henblik på at formidle dele af disses teletrafik, er omfattet af lovens udbyderbegreb.

Det er i den forbindelse uden betydning, om de pågældende har anlagt egen infrastruktur eller baserer deres aktiviteter fuldt ud på lejet infrastrukturkapacitet. Det er ligeledes uden betydning, om de pågældende udbyder offentligt tilgængelige tjenester eller tjenester eksempelvis i form af lukkede net, herunder virtuelle lukkede net, til andre.

Endelig er det uden betydning, hvilken form for tjenester der udbydes, herunder om der eventuelt alene tilbydes formidling af internettrafik, håndtering af udgående samtaler via operatørforvalg og fast operatørvalg, gensalg af andre virksomheders tjenester, et eller flere netadgangs- eller samtrafikprodukter til andre udbydere af elektroniske kommunikationsnet eller -tjenester eller lignende.

Det fremgår endvidere af de specielle bemærkninger til telelovens § 2, nr. 1, at boligforeninger, hoteller, cafeer mv., som udbyder elektroniske kommunikationsnet eller -tjenester, vil kunne være omfattet af definitionen, hvis udbuddet sker med et kommercielt formål. Det afgørende ved vurderingen heraf er, om udbuddet af nettet eller tjenesten sker på markedsmæssige vilkår, herunder som led i markedsføringen af virksomheden eller foreningen. Således kan også indirekte kommerciel tilrådighedsstillelse være omfattet af definitionen, eksempelvis hvis en virksomhed som et direkte eller indirekte led i markedsføringen stiller for eksempel en internettjeneste gratis til rådighed for virksomhedens kunder eller gæster.

Erhvervsmæssige udbydere defineres i lov om sikkerhed i net og tjenesters § 2, nr. 5, som udbydere, der med et kommercielt formål udbyder produkter, elektroniske kommunikationsnet og -tjenester som sin hovedydelse eller som en ikke-accessorisk del af virksomheden. Det fremgår af bemærkningerne til bestemmelsen, at definitionen er identisk med den tilsvarende definition i telelovens § 2, nr. 2, og skal fortolkes i overensstemmelse med denne bestemmelses forarbejder og relevante praksis. Det fremgår af de specielle bemærkninger til telelovens § 2, nr. 2, at erhvervsmæssige udbydere skal anses som en underkategori til udbyderbegrebet i nr. 1, som har til formål at nuancere udbyderbegrebet, således at der tages højde for den teknologiske udvikling og de niveauer af rettigheder og forpligtelser, som knytter sig til loven og anden lovgivning. I forlængelse heraf fremgår det af bemærkningerne, at den teknologiske udvikling bl.a. indebærer, at det i dag er relativt mange, der er udbydere af elektroniske kommunikationsnet eller -tjenester. Dette omfatter ifølge bemærkningerne bl.a. tilfælde, hvor en virksomhed etablerer trådløs infrastruktur med henblik på at levere internetadgang til deres kunder eller lignende.

Etableringen af underkategorien 'erhvervsmæssige udbydere' skal således ifølge bemærkningerne ses i lyset af, at det ikke vurderes hensigtsmæssigt at anvende det brede udbyderbegreb i telelovens § 2, nr. 1, uden yderligere afgrænsning. Begrebet erhvervsmæssige udbydere omfatter ifølge bemærkningerne til telelovens § 2, nr. 2, udbydere, der driver virksomhed omfattet af loven som deres hovedvirksomhed eller som en selvstændig del af virksomheden. Udbyde-

re, der har mobiltelefoni, fastnettelefoni, bredbånd mv. som deres hovedvirksomhed, vil således være omfattet af denne kategori. Ved 'som ikke accessorisk del af virksomheden' forstås, at udbuddet ikke kun er en accessorisk del af virksomheden. Et hotel, der eksempelvis tilbyder sine kunder adgang til trådløst internet, vil som udgangspunkt ikke være erhvervsmæssig udbyder, idet udbuddet i den forbindelse må anses for at være en integreret del af at leje et hotelværelse. Det følger dog af bemærkningerne, at der altid vil være tale om en konkret vurdering.

3.1.1.2. Offentligt tilgængelige elektroniske kommunikationsnet og -tjenester

Lov om sikkerhed i net og tjenester finder kun anvendelse for udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester.

I lov om sikkerhed i net og tjenesters § 2, nr. 1, defineres et elektronisk kommunikationsnet som et transmissionssystem, uanset om det bygger på en permanent infrastruktur eller en centraliseret administrationskapacitet, og, hvor det er relevant, koblings- og dirigeringsudstyr og andre ressourcer, herunder netelementer, der ikke er aktive, som gør det muligt at overføre signaler ved hjælp af trådforbindelse, radiobølger, lyslederteknik eller andre elektromagnetiske midler, herunder satellitnet, jordbaserede fastnet (kredsløbs- og pakkekoblede, herunder i internettet) og mobilnet, elkabelsystemer, i det omfang de anvendes til transmission af signaler, net, som anvendes til radio- og tv-spredning, og kabel-tv-net, uanset hvilken type information der overføres. Lovens § 2, nr. 1, implementerer artikel 2, nr. 1, i EU's telekodeks.

En elektronisk kommunikationstjeneste defineres i lovens § 2, nr. 2, som en tjeneste, der helt eller delvis består i elektronisk overførsel af kommunikation i form af lyd, billeder, tekst eller kombinationer heraf ved hjælp af radio- eller telekommunikationsteknik mellem nettermineringspunkter.

Offentligt tilgængelige elektroniske kommunikationsnet og -tjenester skal anses som en underkategori til elektroniske kommunikationsnet og -tjenester, og defineres i lovens § 2, nr. 3, som elektroniske kommunikationsnet og -tjenester, der stilles til rådighed for en ikke på forhånd afgrænset kreds af slutbrugere eller udbydere.

Det fremgår af bemærkningerne til bestemmelsen, jf. Folketingstidende 2015-16, A, L 10 som fremsat, at definitionen skal fortolkes i overensstemmelse med såvel offentlige elektroniske kommunikationsnet i telelovens § 2, nr. 5, som offentlig elektronisk kommunikationstjeneste i telelovens § 2, nr. 8, og at bestemmelsen derfor skal fortolkes i overensstemmelse med disse bestemmelsers forarbejder og relevant praksis.

Det fremgår af bemærkningerne til telelovens § 2, nr. 5, jf. Folketingstidende 2010-11, A, L 59 som fremsat den 17. november 2010, at for at være et offentligt elektronisk kommunikationsnet skal udbuddet af nettet ske til en ikke på forhånd afgrænset kreds af slutbrugere eller udbydere af elektroniske kommunikationsnet eller -tjenester. Enhver kan derfor principielt anmode om at købe ydelserne i modsætninger til net eller tjenester, der alene tilbydes til specifikke, afgrænsede kundesegmenter, herunder eksempelvis banker, forsikringsselskaber, skoler eller andre undervisningsinstitutioner. Lukkede net eller tjenester, herunder virtuelle lukkede net eller tjenester, er således heller ikke omfattet af definitionen af offentlige elektroniske kommunikationsnet.

Det fremgår i forlængelse heraf af bemærkningerne til telelovens § 2, nr. 5, at det er uden betydning, om der er tale om et landsdækkende udbud eller udbud i en mindre del af landet, eller om der udbydes tjenester, der i praksis alene er relevante for mindre grupper af brugere. Infrastrukturselskaber, der alene udbyder for eksempel infrastrukturkapacitet til andre udbydere af elektroniske kommunikationsnet eller -tjenester, vil således også blive betragtet som udbydende offentlige elektroniske kommunikationsnet, i det omfang der er tale om udbud af elektroniske kommunikationsydelser til en ikke på forhånd afgrænset gruppe af brugere.

For så vidt angår telelovens definition af offentlige elektroniske kommunikationstjenester, fremgår det af bemærkningerne til telelovens § 2, nr. 9, at for at være en offentlig elektronisk kommunikationstjeneste skal udbuddet af tjenesten ske til en ikke på forhånd afgrænset kreds af slutbrugere eller udbydere af elektroniske kommunikationsnet eller -tjenester. Bemærkningerne henviser herudover til bemærkningerne til lovens § 2, nr. 5, som er anført ovenfor.

3.1.2. NIS 2-direktivet

3.1.2.1. Anvendelsesområde

NIS 2-direktivet finder ifølge direktivets artikel 2, nr. 1, anvendelse på offentlige eller private enheder af den type, der er omfattet af direktivets bilag I eller II, som udgør mellemstore virksomheder i henhold til artikel 2 i bilaget til henstilling 2003/361/EF, eller overskrider tærsklerne for mellemstore virksomheder fastsat i direktivets stk. 2, og som leverer deres tjenester eller udfører deres aktiviteter inden for Unionen. Det fremgår af direktivets bilag I, at direktivet bl.a. finder anvendelse for sektoren for digital infrastruktur, herunder bl.a. udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester.

Som hovedregel finder direktivet således kun anvendelse for udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester, såfremt udbyderen opfylder størrelseskravet som defineret i direktivets artikel 2, stk. 1.

Det fremgår af direktivets artikel 2, stk. 2, litra a, nr. i, at direktivet uanset enhedens størrelse, finder anvendelse på enheder af den type, der er omhandlet i bilag I eller II, hvor tjenester leveres af udbydere af offentlige elektroniske kommunikationsnet eller af offentligt tilgængelige elektroniske kommunikationstjenester.

Direktivets artikel 6, nr. 37, definerer en elektronisk kommunikationstjeneste som en elektronisk kommunikationstje-

neste som defineret i artikel 2, nr. 4, i direktiv (EU) 2018/1972, altså EU's telekodeks. En elektronisk kommunikationstjeneste defineres i EU's telekodeks som en tjeneste, som normalt ydes mod betaling via elektroniske kommunikationsnet, og som med undtagelse af tjenester, der består i tilrådighedsstillelse af eller udøvelse af redaktionel kontrol over indhold fremført via elektroniske kommunikationsnet og -tjenester omfatter a) internetadgangstjenester, b) interpersonelle kommunikationstjenester og c) tjenester, der udelukkende eller overvejende består i overføring af signaler, som f.eks. transmissionstjenester, der anvendes til levering af maskine-til-maskine-tjenester og til radio- og tv-spredning.

EU's telekodeks' artikel 2, nr. 5, definerer interpersonelle kommunikationstjenester som en tjeneste, som normalt ydes mod betaling, og som muliggør direkte interpersonel og interaktiv informationsudveksling via elektroniske kommunikationsnet mellem et afgrænset antal personer, hvor de personer, der indleder eller deltager i kommunikationen, bestemmer hvem modtageren eller modtagerne skal være, og omfatter ikke tjenester, der blot muliggør interpersonel og interaktiv kommunikation som en mindre støttefunktion, der er tæt knyttet til en anden tjeneste.

Ifølge EU's telekodeks omfatter interpersonelle kommunikationstjenester, to typer af tjenester, herunder både nummerbaserede- og nummeruafhængige kommunikationstjenester.

Det forudsættes, at definitionen af en interpersonel kommunikationstjeneste fortolkes i overensstemmelse med den tilsvarende definition i EU's telekodeks.

Et offentligt elektronisk kommunikationsnet defineres i direktivets artikel 6, nr. 36, som et offentligt elektronisk kommunikationsnet som defineret i artikel 2, nr. 8, i direktiv (EU) 2018/1972, altså EU's telekodeks. I EU's telekodeks defineres et offentligt elektronisk kommunikationsnet, som et elektronisk kommunikationsnet, som udelukkende eller overvejende bruges til udbud af elektroniske kommunikationstjenester, der er tilgængelige for offentligheden, og som danner grundlag for overførsel af information mellem netterminingspunkter.

Direktivet indeholder ikke en nærmere definition af, hvem der anses for at være udbydere af offentligt tilgængelige kommunikationsnet og -tjenester.

3.1.2.2. Opdeling i væsentlige- og vigtige enheder

NIS 2-direktivet sondrer grundlæggende mellem væsentlige og vigtige enheder. De materielle regler for de to typer af enheder er som udgangspunkt ens, men sondringen har navnlig betydning for tilsynet med enhederne og de håndhævelsesforanstaltninger, der kan anvendes over for enhederne.

Væsentlige enheder defineres i NIS 2-direktivets artikel 3, stk. 1, og omfatter bl.a. udbydere af offentlige elektroniske kommunikationsnet eller af offentligt tilgængelige elektroniske kommunikationstjenester, der udgør mellemstore virksomheder i henhold til artikel 2, i bilaget til henstilling 2003/361/EF, eller overskrider tærsklerne for mellemstore virksomheder i henhold til den nævnte henstilling.

I artikel 2, stk. 1, i bilaget til henstilling 2003/361/EF af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder afgrænses kategorien af mikrovirksomheder, små og mellemstore virksomheder (SMV'er) som virksomheder, som beskæftiger under 250 personer, og har en årlig omsætning på ikke over 50 mio. EUR eller en årlig samlet balance på ikke over 43 mio. EUR.

I kategorien for SMV'er defineres små virksomheder i henstillingen som virksomheder, som beskæftiger under 50 personer, og som har en årlig omsætning eller en samlet årlig balance på ikke over 10 mio. EUR. Tilsvarende defineres mikrovirksomheder i henstillingen som virksomheder, som beskæftiger under 10 personer og som har en årlig omsætning eller en samlet årlig balance på ikke over 2 mio. EUR.

Virksomheder falder således inden for definitionen af mellemstore virksomheder, når virksomheden har 50 ansatte eller derover eller en årlig omsætning på 10 mio. EUR eller derover og en årlig balance på 10 mio. EUR eller derover.

Det følger af NIS 2-direktivets artikel 3, stk. 2, at enheder som omhandlet i direktivets bilag I eller II, der ikke opfylder kriterierne for at være væsentlige enheder, anses for at være vigtige enheder.

3.1.3. Ministeriet for Samfundssikkerhed og Beredskabs overvejelser

NIS 2-direktivet finder som hovedregel kun anvendelse for udbydere af offentlige elektroniske kommunikationsnet eller af offentligt tilgængelige elektroniske kommunikationstjenester, som overstiger tærsklerne for mellemstore virksomheder og som leverer deres tjenester eller udfører deres aktiviteter inden for Unionen.

Det fremgår imidlertid af direktivets artikel 2, stk. 2, litra a), nr. i, at direktivet uanset størrelse bl.a. finder anvendelse på enheder, hvor tjenester leveres af udbydere af offentlige elektroniske kommunikationsnet eller af offentligt tilgængelige elektroniske kommunikationstjenester.

Det er Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at direktivet skal fortolkes således, at direktivet også finder anvendelse for interpersonelle kommunikationstjenester, herunder både nummerbaserede- og nummeruafhængige interpersonelle kommunikationstjenester (NUIK-tjenester).

Der lægges med NIS 2-direktivet endvidere op til, at enheder, der er omfattet af direktivet med henblik på overholdelse af foranstaltninger til styring af cybersikkerhedsrisici og rapporteringsforpligtelser, bør inddeles i to kategorier som henholdsvis væsentlige og vigtige enheder.

Det er Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at udbydere af offentlige elektroniske kommunikationsnet eller af offentligt tilgængelige elektroniske kommunikationstjenester alene skal anses for at være væsentlige og vigtige teleudbydere, hvis teleudbyderen med et kommercielt formål udbyder offentlige elektroniske kommunikationsnet eller offentligt tilgængelige kommunikationstjenester som sin hovedydelse eller som en ikke-accessorisk del af virksomheden. Definitionen svarer til definitionen af 'erhvervsmæssige udbydere' i den gældende lov om sikkerhed i net og tjenester og skal fortolkes i overensstemmelse hermed.

Formålet med denne præcisering af udbyderbegrebet er at sikre, at de nye skærpede regler efter NIS 2-direktivet ikke finder anvendelse for udbydere, der ikke meningsfuldt kan siges at falde ind under kategorien væsentlige eller vigtige teleudbydere efter NIS 2-direktivet. Disse typer udbydere bør derfor i stedet falde ind under kategorien "teleudbydere" med en videreførelse af de samme krav, som gælder for disse udbydere i dag.

Henset til overskueligheden af reguleringen er det Ministeriet for Samfundssikkerhed og Beredskabs vurdering, at der bør foretages konsekvensrettelser af teleudbyderbegrebet i den gældende regulering for telesektoren på Ministeriet for Samfundssikkerhed og Beredskabs område, herunder navnlig i lov om leverandørsikkerhed i den kritiske teleinfrastruktur.

3.1.4. Den foreslåede ordning

Det foreslås, at loven finder anvendelse for samtlige udbydere af offentlige elektroniske kommunikationsnet eller af offentligt tilgængelige elektroniske kommunikationstjenester uanset deres størrelse.

Af hensyn til differentieringen af de forskellige krav til udbydere afhængigt af deres kritikalitet foreslås det, at loven bør skelne mellem henholdsvis teleudbydere, vigtige teleudbydere og væsentlige teleudbydere.

Det foreslås, at den eksisterende definition af en 'erhvervsmæssig teleudbyder' i lov om sikkerhed i net og tjenesters § 2, nr. 5, videreføres, dog således, at begrebet ændres til 'teleudbydere'. Ved teleudbyder forstås således en udbyder, der med et kommercielt formål stiller produkter af offentlige elektroniske kommunikationsnet og offentligt tilgængelige elektroniske kommunikationstjenester til rådighed for andre. Kategorien vil bl.a. omfatte udbydere af radiobaserede lokalnet (RLAN).

Det foreslås endvidere, at kredsen af væsentlige teleudbydere afgrænses til at omfatte udbydere af offentlige elektroniske kommunikationsnet eller af offentligt tilgængelige elektroniske kommunikationstjenester, som overskrider tærsklerne for mellemstore virksomheder, og som med et kommercielt formål udbyder offentlige elektroniske kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester som deres hovedydelse, eller som en ikke accessorisk del af virksomheden.

Desuden vil teleudbydere i overensstemmelse med NIS 2-direktivet i særlige tilfælde uanset størrelse skulle anses som værende væsentlige teleudbydere, herunder hvis teleudbyderen er den eneste udbyder i en medlemsstat af en tjeneste, der er væsentlig for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter. Dette gælder dog kun, hvis teleudbyderen med et kommercielt formål udbyder offentlige elektroniske kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester som deres hovedydelse eller som en ikke-accessorisk del af virksomheden.

Det foreslås endvidere, at teleudbydere, der ikke opfylder kriterierne for at være væsentlige udbydere, bør anses som vigtige teleudbydere, såfremt de med et kommercielt formål udbyder offentlige elektroniske kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester som deres hovedydelse, eller som en ikke-accessorisk del af virksomheden.

Det er derudover Ministeriet for Samfundssikkerhed og Beredskabs vurdering, at teleudbydere uanset deres størrelse bør anses som væsentlige, hvis 1) enheden er den eneste udbyder i en medlemsstat af en tjeneste, der er væsentlig for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter, 2) en forstyrrelse af den tjeneste, enheden leverer, vil kunne have væsentlig indvirkning på den offentlige sikkerhed eller folkesundheden, 3) en forstyrrelse af den tjeneste, enheden leverer, vil kunne medføre en væsentlig systemisk risiko, navnlig for sektorer, hvor en sådan forstyrrelse kan have grænseoverskridende virkning eller 4) enheden er kritisk på grund af sin specifikke betydning på nationalt eller regionalt plan for den pågældende sektor eller type af tjeneste eller for andre indbyrdes afhængige sektorer i medlemsstaten.

Det bemærkes, at udbyderbegrebet i nærværende lov vil adskille sig fra de gældende definitioner på telesektoren, herunder bl.a. udbyderbegrebet i lov om elektroniske kommunikationsnet og -tjenester, jf. lovbekendtgørelse nr. 955 af 17. juni 2022, som hører under Digitaliseringsministeriers område. Dette skyldes navnlig, at lov om elektroniske kommunikationsnet og -tjenester – ligesom lovgivningen om sikkerhed og beredskab i telesektoren i dag – primært opererer med to udbyderbegreber, navnlig udbydere og erhvervsmæssige udbydere.

Der henvises i øvrigt til bemærkningerne til de foreslåede §§ 3 og 4.

3.2. Foranstaltninger til styring af sikkerhedsrisici mv.

3.2.1. Gældende ret

Efter § 3, stk. 1, i lov om sikkerhed i net og tjenester fastsætter Styrelsen for Samfundssikkerhed (tidligere Center for Cybersikkerhed) regler om minimumskrav til sikkerhed i net

og tjenester for udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester og udbydere af NUIK-tjenester. Reglerne kan omfatte krav om passende tekniske, processuelle og organisatoriske foranstaltninger med henblik på risikostyring i forhold til sikkerhed i net og tjenester og opretholdelse af et passende sikkerhedsniveau, herunder krav om, at sådanne foranstaltninger gennemføres på baggrund af dokumenterede og ledelsesforankrede processer.

Bestemmelsen i § 3, stk. 1, implementerer artikel 40, stk. 1, i EU's telekodeks.

Bemyndigelsen i § 3, stk. 1, i lov om sikkerhed i net og tjenester er udmøntet i bekendtgørelse nr. 259 af 22. februar 2021 om sikkerhed og beredskab i net og tjenester.

3.2.2. NIS 2-direktivet

Med artikel 43 i NIS 2-direktivet ophæves bl.a. artikel 40, stk. 1, i EU's telekodeks.

NIS 2-direktivets artikel 21 indeholder overordnet en forpligtelse til at foretage risikostyring og træffe passende tekniske, operationelle og organisatoriske foranstaltninger for at sikre et passende sikkerhedsniveau hos enhederne.

Direktivet foreskriver således i artikel 21, stk. 2, at foranstaltningerne skal baseres på en tilgang, der omfatter alle farer og sigter på at beskytte net- og informationssystemer og disse systemers fysiske miljø mod hændelser, og mindst omfatter følgende: a) politikker for risikoanalyse og informationssystemsikkerhed, b) håndtering af hændelser, c) driftskontinuitet, såsom backup-styring og reetablering efter en katastrofe, og krisestyring, d) forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem den enkelte enhed og dens direkte leverandører eller tjenesteudbydere, e) sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer, herunder håndtering og offentliggørelse af sårbarheder, f) politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici, g) grundlæggende cyberhygiejnepraksisser og cybersikkerhedsuddannelse, h) politikker og procedurer vedrørende brug af kryptografi og, hvor det er relevant, kryptering, i) personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver og j) brug af løsninger med multifaktorautentificering eller kontinuerlig autentificering, sikret tale-, video- og tekstkommunikation og sikrede nødkommunikationssystemer internt i enheden, hvor det er relevant.

Foranstaltningerne skal være proportionale og tilvejebringe et sikkerhedsniveau i enhedens net- og informationssystemer, der står i forhold til risiciene under hensyntagen til sådanne foranstaltningers aktuelle teknologiske stade og i givet fald til relevante europæiske og internationale standarder samt gennemførelsesomkostningerne. Det er desuden forudsat i direktivet, at foranstaltningerne bør stå i et passende forhold til de væsentlige og vigtige enheders risikoeksponering, deres størrelse og til den samfundsmæssige og økonomiske indvirkning, som en hændelse ville have. Foranstaltningerne skal desuden tage hensyn til bl.a. leverandørsikkerhed og sårbarheder i den anledning.

Det påhviler i medfør af direktivet en enhed, der finder, at den ikke overholder direktivets krav til foranstaltninger i artikel 21, stk. 2, uden unødigt ophold at træffe alle nødvendige, passende og forholdsmæssige korrigerende foranstaltninger.

Direktivets artikel 20 stiller desuden krav til enhedernes ledelsesorganer, herunder bl.a. om ledelsesgodkendelse af foranstaltningerne til styring af cybersikkerhedsrisici, ledelsens tilsyn med foranstaltningernes gennemførelse, samt ledelsens deltagelse i kurser. Enhederne tilskyndes desuden til at tilbyde kurser til deres ansatte.

Det følger herudover af NIS 2-direktivets artikel 24, at medlemsstaterne kan kræve, at væsentlige og vigtige enheder – for at påvise overensstemmelse med bestemte krav i direktivets artikel 21 – bruger særlige informations- og kommunikationsprodukter, -tjenester og -processer (IKT-produkter, -tjenester og -processer), der er udviklet af den væsentlige eller vigtige enhed eller indkøbt fra tredjeparter, og som er certificeret i henhold til den europæiske cybersikkerhedscertificeringsordning, der er vedtaget i henhold til Europa-Parlamentets og Rådets forordning 2019/881 af 17. april 2019 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed), om cybersikkerhedscertificering af informations- og kommunikationsteknologi og om ophævelse af forordning (EU) nr. 526/2013 (forordningen om cybersikkerhed).

Europa-Kommissionen er i medfør af NIS 2-direktivets artikel 24, stk. 2, tillagt beføjelser til at vedtage delegerede retsakter, der præciserer hvilke kategorier af væsentlige og vigtige enheder, der skal anvende visse certificerede IKT-produkter, -tjenester og -processer eller indhente en attest i henhold til forordningen om cybersikkerhed. Det er forudsat i direktivet, at der først vedtages delegerede retsakter, hvis der konstateres utilstrækkelige cybersikkerhedsniveauer.

3.2.3. Ministeriet for Samfundssikkerhed og Beredskabs overvejelser

NIS 2-direktivets bestemmelse om foranstaltninger fastsætter et minimumsniveau for foranstaltninger.

I overensstemmelse med NIS 2-direktivets præambelbetragtning nr. 82 forudsættes det således, at der ved fastlæggelsen af foranstaltninger til styring af cybersikkerhedsrisici, der er tilpasset væsentlige og vigtige enheder, bør der tages behørigt hensyn til væsentlige og vigtige enheders forskellige risikoeksponering, herunder enhedens kritiske betydning, de risici, herunder samfundsmæssige risici, som den er eksponeret for, enhedens størrelse og sandsynligheden for hændelser og deres alvor, herunder deres samfundsmæssige og økonomiske indvirkning. Der vil således i overensstemmelse med NIS 2-direktivets forudsætninger kunne differentieres i kravene til teleudbyderne henset til forskelle i teleudbydernes risikoeksponering, deres størrelse og den potentielle

samfundsmæssige og økonomiske betydning af eventuelle hændelser.

Henset til, at der ved implementeringen af NIS 2-direktivet i telesektoren skal ske en integration af den eksisterende regulering på teleområdet, er det Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at foranstaltningerne – som det også er tilfældet i dag – tillige bør omfatte generelle sikkerhedsrisici som led i teleudbydernes beredskab og ikke alene cybersikkerhedsrisici. Det skyldes bl.a., at der foruden foranstaltninger på cybersikkerhedsområdet er behov for andre sikkerhedsforanstaltninger, som f.eks. kan beskytte de kritiske dele af teleinfrastrukturen mod sabotage og hærværk.

Det er endvidere Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at en nærmere konkretisering bør ske i bekendtgørelsesform med henblik på at sikre, at der løbende og smidigt kan ske en tilpasning af kravene i takt med den teknologiske udvikling og udviklingen i trusselsbilledet. Det samme gør sig gældende for så vidt angår anvendelse af særlige IKT-produkter, -tjenester og -processer med henblik på at sikre, at kravene løbende og smidigt kan tilpasses og målrettes, og således at det kan sikres, at kravene er i overensstemmelse med eventuelle delegerede retsakter, som Europa-Kommissionen måtte vedtage.

3.2.4. Den foreslåede ordning

Det foreslås, at der fastsættes en pligt for væsentlige og vigtige teleudbydere til at træffe passende og forholdsmæssige tekniske, operationelle og organisatoriske foranstaltninger for at styre risiciene for sikkerheden i net- og informationssystemer, som disse teleudbydere anvender til deres operationer eller til at levere deres tjenester, og for at forhindre hændelser eller minimere deres indvirkning på modtagere af deres tjenester og på andre tjenester.

Det foreslås endvidere, at foranstaltningerne som minimum skal omfatte eller tage højde for de elementer, der fremgår af NIS 2-direktivets artikel 21, stk. 2.

Det foreslås i forlængelse heraf, at ministeren for samfundssikkerhed og beredskab kan fastsætte nærmere regler om krav til foranstaltninger efter NIS 2-direktivet og yderligere generelle foranstaltninger, som væsentlige og vigtige teleudbydere skal træffe til styring af sikkerhedsrisici. Ministeriet for Samfundssikkerhed og Beredskab vil i den forbindelse bl.a. kunne fastsætte nærmere regler om sikkerhedsforanstaltninger for så vidt angår teleudbydernes beredskab, således at indholdet af de skærpede nationale særregler herom opretholdes som hidtil. Der er med videreførelsen ikke tilsigtet materielle ændringer af de nuværende bestemmelsers indhold eller anvendelsesområde og det forventes således, at ministeriet i vidt omfang vil videreføre de gældende regler i bekendtgørelse nr. 259 af 22. februar 2021 om sikkerhed og beredskab i net og tjenester.

Det foreslås endvidere, at en væsentlig eller vigtig teleudbyder, der finder, at den ikke overholder krav til foranstaltninger, som følger af loven eller regler udstedt i medfør af loven, uden unødigt ophold skal træffe alle nødvendige, passende og forholdsmæssige korrigerende foranstaltninger. Det foreslås desuden, at de foranstaltninger, der træffes, skal være godkendte af teleudbyderens ledelsesorgan, at ledelsesorganet skal føre tilsyn med foranstaltningernes gennemførelse og sikre, at foranstaltningerne har den fornødne effekt, samt at medlemmer af ledelsesorganet skal deltage i relevante kurser om styring af cybersikkerhedsrisici.

Derudover foreslås det, at Ministeriet for Samfundssikkerhed og Beredskab kan fastsætte regler om, at væsentlige og vigtige teleudbydere skal anvende særlige informations- og kommunikationsprodukter, -tjenester og -processer (IKT-produkter, -tjenester og -processer), som er certificeret i henhold til en europæisk cybersikkerhedscertificeringsordning for at påvise overensstemmelse med bestemte krav i reglerne om foranstaltninger til styring af cybersikkerhedsrisici, herunder de nærmere regler herom, som fastsættes i bekendtgørelsesform. Produkterne kan udvikles af den væsentlige eller vigtige teleudbyder eller indkøbes fra tredjeparter.

3.3. Hændelsesrapportering samt oplysnings- og underretningspligter

3.3.1. Gældende ret

Efter § 4 i lov om sikkerhed i net og tjeneste kan Styrelsen for Samfundssikkerhed (tidligere Center for Cybersikkerhed) bl.a. fastsætte regler om underretningspligter for udbydere og udbydere af NUIK-tjenester.

Disse regler kan efter lovens § 4, nr. 3, omfatte krav om udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenesters og udbydere af NUIK-tjenesters underretning af Styrelsen for Samfundssikkerhed (tidligere Center for Cybersikkerhed) uden unødigt ophold om sikkerhedshændelser, der har haft væsentlig indvirkning på driften af net eller tjenester.

Efter § 4, nr. 4, i lov om sikkerhed i net og tjenester kan Styrelsen for Samfundssikkerhed (tidligere Center for Cybersikkerhed) desuden fastsætte regler om udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenesters og udbydere af NUIK-tjenesters underretning af offentligheden ved sikkerhedshændelser, der har haft væsentlig indvirkning på driften af net eller tjenester.

Det bemærkes, at lovens § 4, nr. 3 og 4, implementerer artikel 40, stk. 2, i EU's telekodeks.

Efter § 4, nr. 5, i lov om sikkerhed i net og tjenester kan Styrelsen for Samfundssikkerhed (tidligere Center for Cybersikkerhed) herudover fastsætte regler om udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenesters og udbydere af NUIK-tjenesters informering af deres potentielt berørte brugere om mulige beskyttelsesforanstaltninger eller afhjælpende foranstaltninger, som brugerne kan træffe i tilfælde af en særlig og betydelig trussel om

en sikkerhedshændelse i udbyderens net eller tjenester. Der kan endvidere stilles krav om, at de pågældende udbydere skal informere deres brugere om selve truslen. Lovens § 4, nr. 5, implementerer artikel 40, stk. 3, i EU's telekodeks.

Bemyndigelserne i § 4, nr. 3, 4 og 5, i lov om sikkerhed i net og tjenester er udmøntet i bekendtgørelse nr. 1414 af 30. november 2023 om oplysnings- og underretningspligter vedrørende sikkerhed i net og tjenester. De nærmere regler følger af bekendtgørelsens §§ 7-13.

Underretninger om hændelser indgives i dag via selvbetjeningsløsningen Virk.dk. Når teleudbydere indgiver en hændelsesunderretning på Virk.dk, fordeles denne automatisk til Styrelsen for Samfundssikkerhed (tidligere Center for Cybersikkerhed). Styrelsen for Samfundssikkerhed kan anvende hændelsesunderretningerne til arbejdet med at styrke cybersikkerheden samt til at vurdere, om styrelsen som tilsynsmyndighed skal iværksætte opfølgende skridt, herunder indlede tilsyn.

§ 4, nr. 2, og § 5, stk. 2, i lov om sikkerhed i net og tjenester indeholder derudover nationale særregler, der ikke er implementering af EU-regulering, hvorefter der kan fastsættes yderligere underretningspligter for teleudbyderne.

Efter § 4, nr. 2, i lov om sikkerhed i net og tjenester fastsætter Styrelsen for Samfundssikkerhed (tidligere Center for Cybersikkerhed) regler om erhvervsmæssige udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenesters underretning af Styrelsen for Samfundssikkerhed ved påtænkt indgåelse af aftaler om leverancer, der vedrører væsentlige dele af udbyderens net eller tjenester eller driften heraf. Der kan endvidere stilles krav om, at udbyderne skal indsende et endeligt aftaleudkast til Styrelsen for Samfundssikkerhed umiddelbart forud for indgåelse af aftalen, og at aftalen først kan indgås op til 25 arbejdsdage efter styrelsens modtagelse af dette udkast.

Med lov nr. 1156 af 8. juni 2021 om leverandørsikkerhed i den kritiske teleinfrastruktur (telesikkerhedsloven) blev § 4, nr. 2, i lov om sikkerhed i net og tjenester suppleret med et ekstra værktøj. Efter telesikkerhedsloven kan Styrelsen for Samfundssikkerhed forhindre, at en væsentlig erhvervsmæssig udbyder indgår eller opretholder en aftale, såfremt indgåelsen eller opretholdelsen af aftalen vurderes at udgøre en trussel eller en væsentlig trussel mod statens sikkerhed. Styrelsen for Samfundssikkerhed har således med telesikkerhedsloven fået mulighed for at nedlægge forbud mod henholdsvis indgåelse og opretholdelse af en aftale. Standstill-perioden blev i forbindelse med loven ændret fra 10 arbejdsdage til 25 arbejdsdage.

Bemyndigelsen i § 4, nr. 2, i lov om sikkerhed i net og tjenester er udmøntet i bekendtgørelse nr. 1414 af 30. november 2022 om oplysnings- og underretningspligter vedrørende sikkerhed i net og tjenester. De nærmere regler følger af bekendtgørelsens §§ 3-6 om underretning af Styrelsen for Samfundssikkerhed om aftaleforhandlinger.

Det fremgår af § 5, stk. 2, i lov om sikkerhed i net og tjenester, at for erhvervsmæssige udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester kan det i regler efter § 5, stk. 1, endvidere fastsættes, at udbyderne med henblik på at sikre elektronisk kommunikation i beredskabssituationer og i andre ekstraordinære situationer skal 1) udarbejde beredskabsplaner baseret på en dokumenteret og ledelsesforankret risikostyringsproces og 2) planlægge og deltage i øvelsesaktiviteter.

Bemyndigelsen i § 5, stk. 2, i lov om sikkerhed i net og tjenester er udmøntet i bekendtgørelse nr. 259 af 22. februar 2022 om sikkerhed og beredskab i net og tjenester. De nærmere regler følger af bekendtgørelsens kapitel 5 om krisestyring i beredskabssituationer og i andre ekstraordinære situationer.

3.3.2. NIS 2-direktivet

Med artikel 43 i NIS 2-direktivet ophæves bl.a. artikel 40, stk. 2 og 3, i EU's telekodeks.

Det følger af NIS 2-direktivets artikel 3, stk. 4, at væsentlige og vigtige enheder, skal indgive følgende oplysninger til de kompetente myndigheder: a) enhedens navn, b) adresse og ajourførte kontaktoplysninger, herunder e-mailadresser, IP-intervaller og telefonnumre, c) i givet fald den relevante sektor eller delsektor i direktivets bilag I eller II, samt d) i givet fald en liste over de medlemsstater, hvor enheden leverer tjenester, der er omfattet af dette direktivs anvendelsesområde.

NIS 2-direktivets artikel 23, stk. 1, 1. pkt., fastsætter en pligt for væsentlige og vigtige enheder til uden unødigt ophold at underrette deres Computer Incident Response Team (CSIRT) eller kompetente myndighed om enhver hændelse, der har væsentlig indvirkning på leveringen af enhedens tjenester. Direktivet fastsætter i artikel 23, stk. 3, nærmere kriterier for, hvornår en hændelse anses for at være væsentlig, herunder a) hvis den har forårsaget eller er i stand til at forårsage alvorlige driftsforstyrrelser af tjenesterne eller økonomiske tab for den berørte enhed, eller b) den har påvirket eller er i stand til at påvirke andre fysiske eller juridiske personer ved at forårsage betydelig materiel eller immateriel skade.

Det følger desuden af NIS 2-direktivets præambelbetragtning nr. 101, at vurderingen bl.a. bør tage de berørte net- og informationssystemer i betragtning, navnlig deres betydning for leveringen af enhedens tjenester, alvoren og de tekniske karakteristika af en cybertrussel, eventuelle underliggende sårbarheder, der udnyttes, samt enhedens erfaring med tilsvarende hændelser. Indikatorer såsom graden af påvirkning af tjenestens funktionsdygtighed, varigheden af en hændelse eller antallet af berørte tjenestemodtagere vil kunne spille en vigtig rolle med hensyn til at fastslå, om den driftsmæssige forstyrrelse af tjenesten er alvorlig.

Den grundlæggende tilgang i NIS 2-direktivets artikel 23, stk. 1, 1. pkt., svarer i det væsentligste til tilgangen i arti-

kel 40, stk. 2, i EU's telekodeks, og der vil således fortsat skulle ske underretning af Styrelsen for Samfundssikkerhed ved en hændelse med »væsentlig indvirkning«. NIS 2-direktivet bygger imidlertid videre herpå og tilføjer yderligere elementer, der skal lægges vægt på ved fastlæggelsen af en hændelses indvirkning. Der vil som noget nyt eksempelvis skulle lægges vægt på, om hændelsen har påvirket eller er i stand til at påvirke andre fysiske eller juridiske personer ved at forårsage betydelig fysisk eller ikke fysisk skade.

NIS 2-direktivet fastsætter i artikel 23, stk. 4 – som noget nyt i forhold til EU's telekodeks – hvad de berørte enheder i forbindelse med en underretning skal fremsende til CSIRT'en eller den kompetente myndighed. Det drejer sig om en tidlig varsling, en ajourføring heraf, en foreløbig rapport, eventuelt en statusrapport og en endelig rapport. Direktivet fastsætter i den forbindelse ligeledes frister for fremsendelserne heraf.

Det påhviler efter NIS 2-direktivets artikel 23, stk. 5 – i modsætning til EU's telekodeks – CSIRT'en eller den kompetente myndighed at give den underrettende enhed en tilbagemelding, herunder – såfremt det ønskes – operativ rådgivning og vejledning om mulige foranstaltninger, som enheden kan træffe for at håndtere den væsentlige hændelse, og supplerende teknisk bistand.

Efter NIS 2-direktivets artikel 23, stk. 1, 2. pkt., skal væsentlige og vigtige enheder, hvor det er relevant, uden unødigt ophold underrette modtagerne af deres tjenester om væsentlige hændelser, der sandsynligvis vil påvirke leveringen af disse tjenester negativt. NIS 2-direktivet medfører således – sammenholdt med artikel 40, stk. 2 og 3, i EU's telekodeks – en yderligere underretningspligt for teleudbyderne over for modtagerne af deres tjenester.

Det følger endvidere af NIS 2-direktivets artikel 23, stk. 2, at væsentlige og vigtige enheder uden unødigt ophold skal meddele modtagerne af deres tjenester, som potentielt er berørt af en væsentlig cybertrussel, eventuelle foranstaltninger og modforholdsregler, som disse kan træffe som reaktion på den pågældende trussel. Hvor det er relevant, skal enhederne også informere de pågældende modtagere om selve den væsentlige trussel.

NIS 2-direktivet ændrer således ikke ved, at teleudbydernes modtagere af deres tjenester skal have meddelelse om bl.a. eventuelle foranstaltninger, som disse kan træffe, men NIS 2-direktivet anvender begrebet »væsentlig cybertrussel« som kriterium for meddelelsen i modsætning til det hidtidige begreb i EU's telekodeks »særlig og betydelig trussel«. Samtidig tilføjes der – som noget nyt – et krav om, at meddelelsen skal ske uden unødigt ophold. NIS 2-direktivet viderefører i øvrigt forpligtelsen fra artikel 40, stk. 3, i EU's telekodeks om informering af modtagerne – hvor det er relevant – om selve truslen, dog med det ændrede trusselsbegreb, som er beskrevet ovenfor.

Herudover foreskriver NIS 2-direktivets artikel 23, stk. 7, at CSIRT'en eller den kompetente myndighed efter høring af den berørte enhed kan informere offentligheden om en væsentlig hændelse eller kræve, at enheden gør det, såfremt dette er nødvendigt eller i øvrigt i offentlighedens interesse. Dette svarer – med den justering, at der desuden kan ske offentliggørelse, såfremt »det er nødvendigt« – således til forpligtelsen i artikel 40, stk. 2, i EU's telekodeks. Det vil – som hidtil – skulle sikres, at offentligheden informeres på en ansvarlig måde, som ikke kompromitterer kommercielt fortrolige oplysninger.

3.3.3. Ministeriet for Samfundssikkerhed og Beredskabs overvejelser

NIS 2-direktivet indeholder forskellige oplysnings- og underretningspligter for væsentlige og vigtige udbydere.

Samtidig indeholder den gældende lov om sikkerhed i net og tjenester regler om underretningsforpligtelser for udbydere, der er omfattet af loven.

Det er Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at NIS 2-direktivets krav om underretningspligter vedrørende væsentlige hændelser bør implementeres direktivnært, således at direktivets krav om hændelsesindberetninger samt oplysnings- og underretningspligter overføres direkte til loven. Henset til kriteriernes kvalitative og skønsprægede karakter vurderes det endvidere, at der i bekendtgørelsesform skal fastsættes nærmere regler om, hvornår en hændelse anses for at være væsentlig inden for telesektoren, herunder ved fastsættelse af kvantitative kriterier vedrørende eksempelvis hændelsens varighed eller skadens omfang.

Det er samtidig Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at direktivets krav bør bygge ovenpå de krav, der i forvejen gælder for hændelsesindberetning mv. på teleområdet. Det indebærer bl.a., at begrebet "væsentlig cybertrussel" vil skulle anvendes som kriterium for meddelelsen, der vil skulle ske til Styrelsen for Samfundssikkerhed uden unødigt ophold.

Det er på denne baggrund Ministeriet for Samfundssikkerhed og Beredskabsopfattelse opfattelse, at de gældende oplysnings- og underretningspligter, herunder vedrørende beredskabssituationer og andre ekstraordinære situationer i lov om sikkerhed i net og tjenester, bør videreføres. Der forudsættes ikke en ændring af den eksisterende praksis.

3.3.4. Den foreslåede ordning

Det foreslås, at væsentlige og vigtige teleudbydere skal registrere sig hos Styrelsen for Samfundssikkerhed og i den forbindelse oplyse a) enhedens navn, b) adresse og ajourførte kontaktoplysninger, herunder e-mailadresser, IP-intervaller og telefonnumre, c) i givet fald den relevante sektor eller delsektor i direktivets bilag I eller II, samt d) i givet fald en liste over de medlemsstater, hvor enheden leverer tjenester, der er omfattet af dette direktivs anvendelsesområde. Det foreslås, at de nævnte oplysninger skal indgives til Styrelsen for Samfundssikkerhed senest den 1. oktober 2025. En

væsentlig eller vigtig teleudbyder, der omfattes af lovens anvendelsesområde efter denne dato, vil skulle indgive oplysningerne senest to uger efter, at teleudbyderen omfattes af loven, jf. den foreslåede 7, stk. 2.

Det foreslås, at alle teleudbydere uden unødigt ophold skal underrette Styrelsen for Samfundssikkerhed og CSIRT'en om enhver væsentlig hændelse, og at kravene til fremgangsmåden og fristerne for underretningerne indholdsmæssigt svarer til NIS 2-direktivets.

Det foreslås endvidere, at Ministeriet for Samfundssikkerhed og Beredskab kan fastsætte nærmere regler om, hvornår en hændelse anses for at være væsentlig. Henset til kriteriernes generelle udformning finder Ministeriet for Samfundssikkerhed og Beredskab det således hensigtsmæssigt, at der gives mulighed for, at Styrelsen for Samfundssikkerhed vil kunne fastsætte nærmere regler om væsentlige hændelser, herunder f.eks. af hensyn til særligt kritiske systemer.

Det foreslås desuden, at ministeren for samfundssikkerhed og beredskab bemyndiges til at fastsætte nærmere regler om oplysnings- og underretningspligter for væsentlige og vigtige teleudbydere, herunder krav om 1) afgivelse af oplysninger om væsentlige dele teleudbyderens net eller tjenester eller driften heraf, 2) krav om underretning ved påtænkt indgåelse af aftaler om leverancer, der vedrører væsentlige dele af udbyderens net eller tjenester eller driften heraf, samt 3) regler om, at teleudbyderen skal indsende et endeligt aftaleudkast til Styrelsen for Samfundssikkerhed umiddelbart forud for indgåelse af aftalen, og at aftalen først kan indgås op til 25 arbejdsdage efter centerets modtagelse af dette udkast.

Det foreslås herudover, at væsentlige og vigtige teleudbydere uden unødigt ophold skal underrette modtagerne af deres tjenester om væsentlige hændelser, der sandsynligvis vil påvirke leveringen af deres tjenester negativt. Teleudbyderne skal endvidere uden unødigt ophold oplyse modtagerne af deres tjenester, som potentielt er berørt af en væsentlig cybertrussel, om eventuelle foranstaltninger eller modforholdsregler, som modtagerne kan træffe som reaktion på den pågældende trussel, og eventuelt også informere om selve truslen.

Endvidere foreslås det, at Styrelsen for Samfundssikkerhed under visse betingelser kan informere offentligheden om den væsentlige hændelse eller kræve, at teleudbyderen gør det.

I overensstemmelse med principperne i betænkning nr. 1516 om offentlige myndigheders offentliggørelse af kontrolresultater, afgørelser mv. forudsættes det, at Styrelsen for Samfundssikkerhed ved beslutningen om, hvilke oplysninger en udbyder pålægges at offentliggøre, i fornødent omfang bl.a. iagttager de hensyn til fortrolighed, der fremgår af forvaltningslovens § 27 om offentlig ansattes tavshedspligt, herunder bl.a. hensynene til enkeltpersoners private forhold, forretningshemmeligheder samt forebyggelse, efterforskning og forfølgning af lovovertrædelser. Det bemærkes, at offentliggørelsesordningen efter Ministeriet for Samfundssikkerhed og Beredskabs opfattelse må begrundes i hensynet til offentlighedens interesse, herunder således, at andre udbydere og privatpersoner, der potentielt er påvirket af hændelsen, har mulighed for at varetage deres interesser.

I tilfælde, hvor hændelsen berører flere samfundsvigtige sektorer, herunder eventuelt også sektorer uden for lovens anvendelsesområde, eller hvor der er tale om en hændelse i en anden EU-medlemsstat, vil det dog være CSIRT'en, som vil kunne informere offentligheden om den væsentlige hændelse.

Forud for orientering af offentligheden foreslås det, at Styrelsen for Samfundssikkerhed hører den væsentlige eller vigtige teleudbyder, der har underrettet om hændelsen, herunder med henblik på vurdering af, hvilke oplysninger, der må betragtes som fortrolige. Det forudsættes, at offentliggørelse vil skulle ske inden for rammerne af forvaltningslovens § 27.

Dette omfatter bl.a. hensynet til enkeltpersoners private forhold, forretningshemmeligheder samt hensynet til forebyggelse, efterforskning og forfølgning af lovovertrædelser.

Som nærmere beskrevet under pkt. 3.3.1 indeholder lov om sikkerhed i net og tjenester i § 4, nr. 2, og § 5, stk. 2, yderligere underretningspligter for teleudbyderne, der går videre end NIS 2-direktivet. Med henblik på at sikre en opretholdelse af det nuværende høje sikkerhedsniveau for telesektoren finder Ministeriet for Samfundssikkerhed og Beredskab, at indholdet af § 4, nr. 2, og § 5, stk. 2, i lov om sikkerhed i net og tjenester bør videreføres. Ministeriet for Samfundssikkerhed og Beredskab vurderer, at dette er væsentligt henset til det generelt høje trusselsbillede på cyberområdet og telesektorens samfundsmæssige kritikalitet.

3.4. Beredskabs situationer og andre ekstraordinære situationer

3.4.1. Gældende ret

Efter § 5, stk. 1, i lov om sikkerhed i net og tjenester fastsætter Styrelsen for Samfundssikkerhed (tidligere Center for Cybersikkerhed) regler om, at udbydere skal foretage nødvendig planlægning og træffe nødvendige foranstaltninger for i videst muligt omfang at sikre elektronisk kommunikation i beredskabssituationer og i andre ekstraordinære situationer.

Det fremgår af § 5, stk. 2, i lov om sikkerhed i net og tjenester, at for erhvervsmæssige udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester kan det i regler efter stk. 1, endvidere fastsættes, at udbyderne med henblik på at sikre elektronisk kommunikation i beredskabssituationer og i andre ekstraordinære situationer skal 1) udarbejde beredskabsplaner baseret på en dokumenteret og ledelsesforankret risikostyringsproces og 2) planlægge og deltage i øvelsesaktiviteter.

Bemyndigelserne i § 5, stk. 1 og 2, i lov om sikkerhed i net og tjenester er udmøntet i bekendtgørelse nr. 259 af 22. februar 2021 om sikkerhed og beredskab i net og tjenester. De nærmere regler følger af bekendtgørelsens kapitel 5 om krisestyring i beredskabssituationer og i andre ekstraordinære situationer.

Det følger af § 5, stk. 3, i lov om sikkerhed i net og tjenester, at Styrelsen for Samfundssikkerhed (tidligere Center for Cybersikkerhed) koordinerer og prioriterer beredskabsaktørernes behov for samfundsvigtig elektronisk kommunikation i beredskabssituationer og i andre ekstraordinære situationer. Styrelsen for Samfundssikkerhed kan endvidere fastsætte regler om, at erhvervsmæssige udbydere skal sikre, at de foretagne prioriteringer gennemføres i net og tjenester.

Bemyndigelsen er udmøntet i bekendtgørelse nr. 261 om beredskabsaktørers adgang til elektronisk kommunikation i beredskabssituationer mv af 22. februar 2021.

Det følger endvidere af § 5 a i lov om sikkerhed i net og tjenester, at Styrelsen for Samfundssikkerhed kan fastsætte regler om, at udbydere, som i medfør af lov om elektroniske kommunikationsnet og -tjenester skal udsende offentlige advarsler om overhængende eller truende alvorlige nødsituationer og katastrofer, skal træffe alle nødvendige foranstaltninger til at sikre uafbrudt transmission af advarslerne. Bemyndigelsen er ikke udnyttet.

3.4.2. Ministeriet for Samfundssikkerhed og Beredskabs overvejelser

Det er Ministeriet for Samfundssikkerhed og Beredskabs vurdering, at bestemmelserne i kapitel 3 om elektronisk kommunikation i beredskabssituationer og i andre ekstraordinære situationer i lov om sikkerhed i net og tjenester bør videreføres med nærværende lov.

Videreførelsen skal navnlig ses i lyset af, at elektronisk kommunikation i stigende grad er en forudsætning for opretholdelse af samfundets funktioner, hvilket stiller krav til en robust teleinfrastruktur. I beredskabssituationer og i andre ekstraordinære situationer, hvor samfundet rammes af naturskabte eller menneskeskabte ulykker eller katastrofer, vil den elektroniske kommunikation og dermed en fungerende teleinfrastruktur være nødvendig for, at samfundsvigtige funktioner kan opretholdes.

Ikke mindst de forskellige aktører, der indgår i samfundets beredskab, kan i beredskabssituationer og i andre ekstraordinære situationer have behov for elektronisk kommunikation for at udføre en række af deres opgaver, ligesom elektronisk kommunikation er en forudsætning for, at de kan koordinere deres indsats.

Det er derfor nødvendigt med et beredskab på teleområdet, som sikrer, at den elektroniske kommunikation i videst muligt omfang opretholdes i beredskabssituationer og i andre ekstraordinære situationer, og som tilgodeser beredskabsaktørernes behov for elektronisk kommunikation.

3.4.3. Den foreslåede ordning

Det foreslås, at ministeren for samfundssikkerhed og beredskab kan fastsætte regler om, at væsentlige og vigtige teleudbydere skal sikre, at de foretagne prioriteringer gennemføres i net og tjenester. Det foreslås endvidere, at ministeren for samfundssikkerhed og beredskab kan fastsætte regler om, at væsentlige- og vigtige teleudbydere skal underrette Styrelsen for Samfundssikkerhed i tilfælde, hvor udbyderen aktiverer sit beredskab, eller hvor udbyderen bliver bekendt med en hændelse, som vurderes at kunne føre til en beredskabssituation eller en anden ekstraordinær situation for teleudbyderen selv eller for en anden udbyder, herunder regler om, hvordan underretningen skal foretages.

Det foreslås desuden, at ministeren for samfundssikkerhed og beredskab kan fastsætte regler om, at udbydere, som i medfør af lov om elektroniske kommunikationsnet og -tjenester skal udsende offentlige advarsler om overhængende eller truende alvorlige nødsituationer og katastrofer, skal træffe alle nødvendige foranstaltninger til at sikre uafbrudt transmission af advarslerne.

Den foreslåede ordning vil ikke medføre en ændring af gældende ret, idet bestemmelserne i kapitel 3 i lov om sikkerhed i net og tjenester bør videreføres.

3.5. Aktindsigt i oplysninger og underretninger

3.5.1. Gældende ret

Lov om sikkerhed i net og tjenester fastsætter i lovens kapitel 5 regler om aktindsigt i underretninger mv.

Det følger således af lovens § 7, at det i regler udstedt i medfør af lovens § 4 kan fastsættes, at underretninger og afgivelse af oplysninger efter lovens § 4, nr. 1-3, er undtaget fra aktindsigt efter lov om offentlighed i forvaltningen og partsaktindsigt efter forvaltningsloven.

Dette indebærer, at underretninger til Styrelsen for Samfundssikkerhed om 1) væsentlige dele af teleudbyderens net eller tjenester eller driften heraf, 2) indgåelse af aftaler om leverancer, der vedrører væsentlige dele af udbyderens net eller tjenester eller driften heraf og sikkerhedshændelser, der har haft væsentlig indvirkning på driften af net eller tjenester, kan undtages fra aktindsigt efter lov om offentlighed i forvaltningen og partsaktindsigt efter forvaltningsloven.

Bemyndigelsen til at fastsætte regler om aktindsigt er i dag udmøntet i bekendtgørelse nr. 258 af 22. februar 2021 om oplysnings- og underretningspligter vedrørende sikkerhed i net og tjenester. De nærmere regler følger af bekendtgørelsens § 14.

Det følger endvidere af den nævnte lovs § 8, stk. 2, at underretninger fra myndigheder og virksomheder vedrørende hændelser, der negativt påvirker eller vurderes at ville kunne påvirke tilgængelighed, integritet eller fortrolighed af data, informationssystemer, digitale netværk eller digitale

servicer, er undtaget fra aktindsigt efter lov om offentlighed i forvaltningen og partsaktindsigt efter forvaltningsloven.

3.5.2. Ministeriet for Samfundssikkerhed og Beredskabs overvejelser

Det er Ministeriet for Samfundssikkerhed og Beredskabs vurdering, at de eksisterende regler om aktindsigt i underretninger mv. bør videreføres.

De oplysninger, som Styrelsen for Samfundssikkerhed som led i indberetningsordningen modtager fra væsentlige og vigtige teleudbydere vedrørende væsentlige dele af udbyderens net og tjenester eller varetagelsen af driften heraf, vil ofte indeholde oplysninger om fejl eller sårbarheder i net eller tjenester, som kan misbruges af potentielle angribere, hvis de kommer til uvedkommendes kendskab. Det vurderes derfor, at oplysningerne i deres helhed bør undtages fra aktindsigt, herunder partsaktindsigt efter forvaltningsloven, således at aktindsigtsanmodninger ikke – som det ellers ville være tilfældet – behandles efter principperne i offentlighedsloven. Undtagelsen kan omfatte underretningssagen som helhed.

Underretning af Styrelsen for Samfundssikkerhed skaber de bedst mulige forudsætninger for, at styrelsen kan udnytte erfaringer med cybertrusler og sikkerhedsrisici på tværs af samfundet – og dermed skabe et samlet overblik over den aktuelle sikkerhedstilstand på den danske del af internettet. Underretningerne sætter således Styrelsen for Samfundssikkerhed i stand til at varsle hurtigere om trusler og styrke grundlaget for styrelsens rådgivning om risici og passende sikkerhedstiltag.

Oplysninger om, at der f.eks. er gennemført et vellykket hackerangreb, hvor en virksomhed har mistet data, kan imidlertid i høj grad skade virksomhedens omdømme, og risikoen for, at oplysningerne via aktindsigt bliver offentligt tilgængelige, kan i praksis afholde mange virksomheder fra at underrette Styrelsen for Samfundssikkerhed om et sådant hackerangreb. Derfor bør også disse særlige underretninger være undtaget fra aktindsigt.

Undtagelsen fra aktindsigt bør efter ministeriets opfattelse også gælde i de tilfælde, hvor oplysningerne videregives til Kommissionen, Det Europæiske Agentur for Net- og Informationssikkerhed eller nationale tilsynsmyndigheder i andre EU-medlemsstater.

Efter Ministeriet for Samfundssikkerhed og Beredskabs opfattelse bør der endvidere ikke være adgang til aktindsigt i de udkast til aftaler, som væsentlige og vigtige teleudbydere indsender til Styrelsen for Samfundssikkerhed i medfør af regler fastsat efter denne lov. Aftalerne vil således ofte indeholde en lang række oplysninger om udbydernes net og tjenester samt aftaleforhold, som dels er kommercielt fortrolige, dels kan misbruges af potentielle angribere.

Undtagelsen fra aktindsigt omfatter ikke teleudbydernes adgang til at gøre sig bekendt med oplysninger, der vedrører deres egne forhold.

3.5.3. Den foreslåede ordning

Det foreslås, at teleudbyderes underretninger til Styrelsen for Samfundssikkerhed og CSIRT'en vedrørende væsentlige hændelser efter den foreslåede § 8, stk. 2, jf. stk. 3, og hændelser, nærvedhændelser og cybertrusler efter den foreslåede § 10 er undtaget fra reglerne om aktindsigt.

Det foreslås derudover, at det i regler udstedt i medfør af bemyndigelsesbestemmelserne i lovens § 7, stk. 5, kan fastsættes, at underretninger og afgivelse af oplysninger efter denne bestemmelse er undtaget fra aktindsigt efter lov om offentlighed i forvaltningen og partsaktindsigt efter forvaltningsloven

Den foreslåede ordning har til formål at videreføre de eksisterende regler om aktindsigt i lov om sikkerhed i net og tjenester.

Videreførelsen skal navnlig ses i lyset af, at en velfungerende underretningsordning forudsætter, at der ikke er risiko for, at de ofte særligt kommercielt følsomme oplysninger, som vil blive modtaget fra teleudbyderne, kan tilgå teleudbydernes konkurrenter eller potentielle angribere.

Der henvises i øvrigt til bemærkninger til de foreslåede §§ 14 og 15 samt bemærkningerne hertil.

3.6. Sikkerhedsgodkendelser

3.6.1. Gældende ret

3.6.1.1. Sikkerhedsgodkendelser efter lov om sikkerhed i net og tjenester

Lov om sikkerhed i net og tjenester indeholder i lovens kapitel 4 regler om sikkerhedsgodkendelser. Det følger således af lovens § 6, stk. 1, at en udbyder skal indstille medarbejdere og repræsentanter for udbyderen til sikkerhedsgodkendelse hos sikkerhedsmyndigheden, når de pågældende som led i deres konkrete opgaveløsning for udbyderen skal behandle klassificerede informationer eller andre informationer, der er særligt beskyttelsesværdige i relation til sikkerhed i net og tjenester eller beredskab.

Det fremgår derudover at bestemmelsens stk. 2, at erhvervsmæssige udbydere af offentligt tilgængelige elektroniske kommunikationsnet skal sikre, at medarbejdere eller repræsentanter for udbyderen, der varetager kontakten til Styrelsen for Samfundssikkerhed i relation til beredskabet i henhold til regler, der er udstedt i medfør af lovens § 5, stk. 2, i fornødent omfang sikkerhedsgodkendes efter stk. 1.

Det følger af bestemmelsens stk. 3, at udbydere, hvis medarbejdere eller repræsentanter sikkerhedsgodkendes efter stk. 1, skal sikre overholdelse af sikkerhedsmyndighedens anvisninger om behandling af klassificerede informationer.

Det fremgår derudover af bestemmelsens stk. 4, at udbydere, hvis medarbejdere eller repræsentanter sikkerhedsgodkendes efter stk. 1, uden ugrundet ophold skal underrette sikkerhedsmyndigheden, når sikkerhedsgodkendte personer ikke længere varetager de opgaver for udbyderen, som lå til grund for sikkerhedsgodkendelsen.

Det fremgår endvidere af bestemmelsens stk. 5, at sikkerhedsmyndigheden kan tilbagekalde en sikkerhedsgodkendelse, når betingelserne for sikkerhedsgodkendelse ikke længere er til stede.

Endelig giver bestemmelsens stk. 6 ministeren for samfundssikkerhed og beredskab hjemmel til at fastsætte regler om sikkerhedsgodkendelse af udbyderes medarbejdere eller repræsentanter for udbydere, der har adgang til udstyr eller systemer, som benyttes i forbindelse med indgreb i meddelelseshemmeligheden.

3.6.1.2. Sikkerhedsgodkendelser efter sikkerhedscirkulæret

Cirkulære nr. 10338 af 17. december 2014 om sikkerhedsbeskyttelse af informationer af fælles interesse for landene i NATO eller EU, andre klassificerede informationer samt informationer af sikkerhedsmæssig beskyttelsesinteresse i øvrigt (sikkerhedscirkulæret) indeholder de almindelige regler for bl.a. sikkerhedsundersøgelser og sikkerhedsgodkendelser af ansatte i offentlige myndigheder og ansatte i private firmaer, der arbejder for en offentlig myndighed. Sikkerhedsgodkendelsen har kun gyldighed for den sikkerhedsgodkendte persons arbejde for den pågældende myndighed. Det fremgår af stk. 3, at Politiets Efterretningstjeneste foretager en sikkerhedsundersøgelse til brug for den offentlige myndigheds afgørelse om sikkerhedsgodkendelse af ansatte.

Afgørelse om sikkerhedsgodkendelse træffes i medfør af sikkerhedscirkulærets § 14 på grundlag af en konkret vurdering af alle de oplysninger, der foreligger om personen. Der lægges herved navnlig vægt på, om den pågældende har udvist ubestridt loyalitet, og om den pågældende har en sådan adfærd og karakter, herunder vaner, forbindelser og diskretion, at der ikke kan være tvivl om den pågældendes pålidelighed i forbindelse med håndtering af klassificerede informationer.

3.6.2. Ministeriet for Samfundssikkerhed og Beredskabs overvejelser

Det er Ministeriet for Samfundssikkerhed og Beredskabs vurdering, at de gældende regler for sikkerhedsgodkendelser i § 6 i lov om sikkerhed i net og tjenester i et vist omfang bør videreføres, dog således, at loven alene fastsætter de overordnede rammer for den personkreds, der skal være omfattet af kravet om sikkerhedsgodkendelse, mens de nærmere regler herom vil blive fastsat i en bekendtgørelse. Dette vil skabe fleksibilitet i regelsættet i forhold til nye udviklinger, trusselsvurderinger mv., der kan have betydning for vurderingen af, hvilken personkreds der bør sikkerhedsgodkendes.

Videreførelsen skal ses i lyset af det aktuelle trusselsbillede, herunder navnlig behovet for at vurdere medarbejdere i væsentlige og vigtige enheders pålidelighed og imødegå risikoen for bl.a. spionage og sabotage.

3.6.3. Den foreslåede ordning

Det foreslås, at medarbejdere eller repræsentanter for en væsentlig eller vigtig teleudbyder skal sikkerhedsgodkendes, når 1) det er nødvendigt i forhold til den pågældendes adgang til klassificeret information eller til de funktioner, som den pågældende skal varetage, eller 2) den pågældende varetager kontakten til Styrelsen for Samfundssikkerhed i relation til beredskabet i henhold til regler, der er udstedt i medfør af § 13, stk. 3.

Endvidere foreslås det, at ministeren for samfundssikkerhed og beredskab kan fastsætte nærmere regler for sikkerhedsgodkendelser, herunder regler om ansøgninger vedrørende sikkerhedsgodkendelser, herunder betingelser for indgivelse af sådanne ansøgning samt meddelelse og tilbagekaldelse af sikkerhedsgodkendelser. Det foreslås, at reglerne skal fastsættes efter forhandling med justitsministeren.

3.7. Tilsyn

3.7.1. Gældende ret

Styrelsen for Samfundssikkerhed varetager Ministeriet for Samfundssikkerhed og Beredskabs myndighedsopgaver i relation til informationssikkerhed og beredskab for telesektoren. Der er på den baggrund i § 9, stk. 1, i lov om sikkerhed i net og tjenester fastsat en forpligtelse for Styrelsen for Samfundssikkerhed (tidligere Center for Cybersikkerhed) til at føre tilsyn med overholdelsen af loven og regler, der er udstedt af medfør i loven.

Efter § 9, stk. 2, i lov om sikkerhed i net og tjenester kan Styrelsen for Samfundssikkerhed (tidligere Center for Cybersikkerhed) som led i sit tilsyn kræve, at udbydere og udbydere af NUIK-tjenester fremlægger alle de oplysninger og det materiale om sikkerhed i net og tjenester, beredskab og sikkerhedsgodkendelse, der er nødvendige for styrelsens tilsynsvirksomhed, herunder til afgørelse af, om et forhold falder ind under denne lov eller regler, der er udstedt i medfør af loven.

Bestemmelsen suppleres af lovens § 4, hvorefter Styrelsen for Samfundssikkerhed (tidligere Center for Cybersikkerhed) mere generelt med henblik på at sikre informationssikkerheden i net og tjenester kan fastsætte regler om oplysnings- og underretningspligter for udbydere af offentligt tilgængelige net og tjenester.

Efter § 9, stk. 3, i lov om sikkerhed i net og tjenester kan Styrelsen for Samfundssikkerhed (tidligere Center for Cybersikkerhed) stille krav om, hvordan og i hvilken form oplysninger og materiale efter § 9, stk. 2, skal afgives.

Lovens § 9, stk. 2 og 3, i lov om sikkerhed i net og tjenester

er delvis implementering af artikel 20, stk. 1, i EU's telekodeks.

I forbindelse med tilsynet med udbydernes overholdelse af reglerne kan Styrelsen for Samfundssikkerhed (tidligere Center for Cybersikkerhed) efter § 9, stk. 5, i lov om sikkerhed i net og tjenester desuden stille krav om, at udbydere og udbydere af NUIK-tjenester skal foranstalte en uafhængig sikkerhedsrevision og stille resultaterne heraf til rådighed for styrelsen.

Lovens § 9, stk. 5, i lov om sikkerhed i net og tjenester er delvis implementering af artikel 41, stk. 2, litra b, i EU's telekodeks.

Lov om sikkerhed i net og tjenester indeholder derudover i § 9, stk. 4, 6 og 7 nationale særregler, der ikke implementerer EU-regulering, hvorefter Styrelsen for Samfundssikkerhed (tidligere Center for Cybersikkerhed) er tillagt yderligere tilsynsbeføjelser overfor teleudbyderne.

Efter § 9, stk. 4, i lov om sikkerhed i net og tjenester kan Styrelsen for Samfundssikkerhed (tidligere Center for Cybersikkerhed) afkræve udbydere skriftlige udtalelser og redegørelser om faktiske forhold af betydning for styrelsens tilsynsvirksomhed.

Efter § 9, stk. 6, i lov om sikkerhed i net og tjenester har Styrelsen for Samfundssikkerhed (tidligere Center for Cybersikkerhed), såfremt det er nødvendigt af hensyn til sikkerheden i net og tjenester, efter et skriftligt varsel på mindst 7 arbejdsdage uden retskendelse mod behørig legitimation adgang til udbyderes forretningslokaler med henblik på at påse overholdelsen af loven og regler, der er udstedt i medfør af loven. Styrelsen for Samfundssikkerhed (tidligere Center for Cybersikkerhed) kan ikke i forbindelse med adgang til forretningslokaler tilgå kommunikation til, fra eller mellem udbyderens kunder.

Efter § 9, stk. 7, i lov om sikkerhed i net og tjenester, har Styrelsen for Samfundssikkerhed (tidligere Center for Cybersikkerhed) endvidere, såfremt det er nødvendigt af hensyn til sikkerheden i net og tjenester, efter et skriftligt varsel på mindst 7 arbejdsdage uden retskendelse mod behørig legitimation adgang til forretningslokaler hos udbyderes samarbejdspartnere, leverandører eller underleverandører med henblik på at påse overholdelsen af loven og regler, der er udstedt i medfør af loven, i relation til outsourcet aktivitet. Styrelsen for Samfundssikkerhed (tidligere Center for Cybersikkerhed) kan ikke i forbindelse med adgang til forretningslokaler tilgå kommunikation til, fra eller mellem udbyderens kunder.

Ved tilsynsbesøg hos samarbejdspartnere, leverandører eller underleverandører gælder de samme betingelser som efter lovens § 9, stk. 6.

3.7.2. NIS 2-direktivet

Med artikel 43 i NIS 2-direktivet ophæves bl.a. artikel 41, stk. 2, litra b, i EU's telekodeks.

NIS 2-direktivets artikel 31, stk. 1, fastsætter herefter en pligt for medlemsstaterne til at sikre, at deres kompetente myndigheder effektivt overvåger og træffer de nødvendige foranstaltninger til at sikre, at direktivet overholdes. I medfør af direktivets artikel 31, stk. 2, kan medlemsstaterne dog tillade, at de kompetente myndigheder prioriterer deres tilsynsopgaver baseret på en risikobaseret tilgang. Efter direktivets artikel 32, stk. 1, og 33, stk. 1, skal bl.a. tilsynsforanstaltningerne være effektive, stå i et rimeligt forhold til overtrædelsen og have en afskrækkende virkning under hensyntagen til omstændighederne i hver enkelt sag.

Efter NIS 2-direktivets præambelbetragtning nr. 95 kan medlemsstaterne tildele de kompetente myndigheder efter EU's telekodeks samme rolle efter NIS 2-direktivet med henblik på at sikre videreførelsen af den nuværende praksis og for at bygge videre på den viden og erfaring, der er opnået som et resultat af gennemførelsen af EU's telekodeks.

Sondringen mellem væsentlige og vigtige enheder i NIS 2-direktivet ses bl.a. at være relevant i relation til tilsyn. Det er i NIS 2-direktivet således forudsat, at tilsynet med henholdsvis væsentlige og vigtige enheder kan differentieres med henblik på at sikre en rimelig balance mellem forpligtelser for disse enheder og for de kompetente myndigheder. Direktivet forudsætter, at væsentlige enheder underlægges et omfattende forudgående og efterfølgende tilsyn, mens vigtige enheder derimod underlægges et lettere og rent reaktivt tilsyn, hvor de ikke er forpligtet til systematisk at dokumentere overholdelsen af foranstaltninger til styring af cybersikkerhedsrisici, og hvor de kompetente myndigheder ikke har en generel forpligtelse til at føre løbende tilsyn med disse enheder. Det reaktive tilsyn med vigtige enheder vil eksempelvis kunne aktiveres, hvis der modtages oplysninger fra andre myndigheder, enheder, borgere eller medier, eller hvis myndigheden i forbindelse med udførelsen af dennes opgaver i øvrigt kommer i besiddelse af oplysninger, der peger på mulige overtrædelser af reguleringen, jf. NIS 2-direktivets præambelbetragtning nr. 122.

NIS 2-direktivet oplister i artikel 32, stk. 2 og 3, og 33, stk. 2 og 3, en række tilsynsbeføjelser, som de kompetente myndigheder som minimum skal kunne anvende ved deres tilsyn med henholdsvis væsentlige og vigtige enheder. Der er navnlig tale om, at de kompetente myndigheder skal kunne føre kontrol på stedet hos enhederne, foretage målrettede sikkerhedsaudits og sikkerhedsscanninger samt kræve at få udleveret oplysninger og dokumentation, der er nødvendige for udførelsen af myndighedernes tilsynsopgaver.

Oplistningerne af tilsynsbeføjelser for henholdsvis væsentlige og vigtige enheder er i vidt omfang identiske, idet NIS 2-direktivets forudsætning om en differentieret tilgang til tilsynet med væsentlige og vigtige enheder dog afspejler sig i visse forskelle i de beføjelser, der som minimum skal kunne anvendes. Direktivet foreskriver eksempelvis, at

myndighederne skal kunne foretage stikprøvekontrol med væsentlige enheder, hvilket ikke gør sig gældende for vigtige enheder. De målrettede sikkerhedsaudits, som skal kunne pålægges både væsentlige og vigtige enheder, skal efter direktivet kun for de væsentlige enheder kunne være regelmæssige. Herudover foreskriver direktivet, at væsentlige enheder under visse omstændigheder skal kunne pålægges sikkerhedsaudits ad hoc, hvilket ikke er tilfældet for vigtige enheder.

3.7.3. Ministeriet for Samfundssikkerhed og Beredskabs overvejelser

Den grundlæggende tilgang i NIS 2-direktivet og EU's telekodeks i forhold til tilsyn svarer i det væsentligste til hinanden. Som beskrevet ovenfor giver EU's telekodeks i artikel 20 og artikel 41, stk. 2, litra b, medlemsstaterne beføjelse til – som led i deres tilsyn – at kræve, at der fremlægges oplysninger og materiale, ligesom der kan kræves en uafhængig sikkerhedsrevision. NIS 2-direktivet bygger imidlertid videre herpå og indeholder en minimumsliste over tilsynsbeføjelser, der foruden de beføjelser, der følger af EU's telekodeks, navnlig som noget nyt omfatter kontrol på stedet – og stikprøvekontrol for de væsentlige teleudbydere – samt sikkerhedsscanninger.

Hertil kommer, at § 9, stk. 4, 6 og 7, i lov om sikkerhed i net og tjenester indeholder yderligere tilsynsbeføjelser for Styrelsen for Samfundssikkerhed, der går videre end de tilsynsbeføjelser, der følger af direktivet.

Med henblik på at sikre et effektivt tilsyn med teleudbydernes efterlevelse af loven og de regler, der er udstedt i medfør af loven, finder Ministeriet for Samfundssikkerhed og Beredskab, at indholdet af lovens § 9, stk. 4, 6 og 7, bør videreføres.

I det omfang der er tale om videreførelse af gældende ret, tilsigtes der ikke en ændring af gældende ret.

Videreførelsen skal navnlig ses i lyset af det generelt høje trusselsbillede på cyberområdet og telesektorens samfundsmæssige kritikalitet.

3.7.4. Den foreslåede ordning

Det foreslås, at Styrelsen for Samfundssikkerhed – som hidtil – inden for telesektoren fører tilsyn med teleudbyderes efterlevelse af loven og de regler, der udstedes i medfør af loven.

Det foreslås i forlængelse heraf, at Styrelsen for Samfundssikkerhed tillægges tilsynsbeføjelser, der indholdsmæssigt svarer til det, som NIS 2-direktivet foreskriver, herunder med de forudsatte forskelle i tilgangen til væsentlige og vigtige teleudbydere. I overensstemmelse med forudsætningerne i direktivet foreslås det derfor, at Styrelsen for Samfundssikkerhed ved tilrettelæggelsen af sit tilsyn anlægger en risikobaseret tilgang, hvor der kan anvendes forskellige tilgange til tilsyn med henholdsvis væsentlige og vigtige teleudbydere.

Tilsynsbesøgene vil alene blive gennemført, hvis det er nødvendigt af hensyn til informationssikkerheden. Styrelsen for Samfundssikkerheds adgang til at foretage tilsynsbesøg – der kun forudsættes anvendt, såfremt et tilsvarende resultat ikke kan opnås ved anvendelse af andre og mindre indgribende tilsynsmuligheder – kan derfor kun anvendes i forbindelse med styrelsens tilsynsvirksomhed.

For effektivt at kunne konstatere, om væsentlige teleudbydere i praksis har gennemført de nødvendige foranstaltninger til at sikre deres net- og informationssystemer, er det nødvendigt, at Styrelsen for Samfundssikkerhed som led i et tilsyn har adgang til forretningslokaler hos væsentlige teleudbydere. Det foreslås derfor, at der skal være adgang til kontrol på stedet uden retskendelse og mod behørig legitimation.

Styrelsen for Samfundssikkerheds tilsynsbesøg vil skulle varsles skriftligt, herunder via e-mail, mindst syv arbejdsdage forud for besøget, og styrelsen kan således ikke med hjemmel i bestemmelsen foretage uanmeldte tilsynsbesøg.

Det forudsættes endvidere, at Styrelsen for Samfundssikkerheds i forbindelse med tilsynsbesøgene i videst muligt omfang tager hensyn til den væsentlige eller den vigtige udbyderes virksomhed og tilrettelægger besøgene således, at styrelsen alene skaffer sig kendskab til forhold, der er af betydning for gennemførelsen af styrelsens tilsynsvirksomhed. Tilsynsbesøgene vil typisk tage udgangspunkt i oplysninger og materiale fra udbyderne, herunder oplysninger om de iværksatte tekniske, operationelle og organisatoriske foranstaltninger.

Endelig foreslås det, at indholdet af de skærpede nationale særregler omkring Styrelsen for Samfundssikkerheds beføjelser til at kræve skriftlige udtalelser og redegørelser samt adgang til teleudbyderes samt deres samarbejdspartneres, leverandørers eller underleverandørers forretningslokaler opretholdes som hidtil. Der er med videreførelsen således ikke tilsigtet materielle ændringer af de nuværende bestemmelsers indhold.

Det er Ministeriet for Samfundssikkerhed og Beredskabs vurdering, at de foreslåede tilsynsforanstaltninger vil være omfattet af lov om retssikkerhed ved forvaltningens anvendelse af tvangsindgreb og oplysningspligter. Dette indebærer, at retten til ikke at inkriminere sig selv, jf. kapitel 4 i nævnte lov, skal overholdes. Det bemærkes dog, at det af bemærkningerne til § 10 i lov om retssikkerhed ved forvaltningens anvendelse af tvangsindgreb og oplysningspligter fremgår, at bestemmelsen om forbud mod selvinkrimineringer ikke til hinder for, at den mistænkte kan pålægges at give (faktuelle) oplysninger, som er uden betydning for bedømmelsen af, hvorvidt den pågældende har begået en lovovertrædelse, der kan medføre straf. Bestemmelsen vil således ikke være til hinder for at anvende en oplysningspligt

til at kræve oplysninger om navn, adresse mv., jf. herved også retsplejelovens § 750, hvorefter enhver på forlangende er forpligtet til over for politiet at opgive navn, adresse og fødselsdato. Der henvises til Folketingstidende 2003-04, tillæg A, side 3097.

3.8. Håndhævelse

3.8.1. Gældende ret

Center for Cybersikkerhed (nu Styrelsen for Samfundssikkerhed) kan som led i varetagelsen af myndighedsopgaver i relation til informationssikkerhed og beredskab for telesektoren iværksætte tiltag med henblik på at sikre sikkerheden i net og tjenester, som kan vise sig nødvendige på baggrund af eksempelvis tilsyn.

Efter § 3, stk. 3, i lov om sikkerhed i net og tjenester kan Styrelsen for Samfundssikkerhed påbyde udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester og udbydere af NUIK-tjenester at træffe konkrete foranstaltninger, der er nødvendige for at afhjælpe en sikkerhedshændelse eller hindre en sådan i at forekomme, når en betydelig trussel er identificeret. Styrelsen fastsætter nærmere regler herom.

Bemyndigelsen i § 3, stk. 3, i lov om sikkerhed i net og tjenester er udmøntet i bekendtgørelse nr. 259 af 22. februar 2021 om sikkerhed og beredskab i net og tjenester. De nærmere regler følger af bekendtgørelsens kapitel 4 vedrørende påbud om konkrete informationssikkerhedsforanstaltninger.

Bestemmelsen – og de dele af bekendtgørelsen, der er udstedt i medfør heraf – implementerer artikel 41, stk. 1, i EU's telekodeks.

Lov om sikkerhed i net og tjenester indeholder derudover i § 3, stk. 2 og 4, samt § 5, stk. 4 nationale særregler, der ikke er implementering af EU-regulering, hvorefter Styrelsen for Samfundssikkerhed kan udstede yderligere påbud til teleudbyderne.

Efter § 3, stk. 2, i lov om sikkerhed i net og tjenester kan Styrelsen for Samfundssikkerhed (tidligere Center for Cybersikkerhed) påbyde udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester at inddrage nærmere angivne områder af deres virksomhed og nærmere angivne trusler mod sikkerheden i net og tjenester i deres risikostyringsprocesser efter lovens § 3, stk. 1.

Efter § 3, stk. 4, i lov om sikkerhed i net og tjenester kan Styrelsen for Samfundssikkerhed (tidligere Center for Cybersikkerhed), såfremt det er af væsentlig samfundsmæssig betydning, påbyde udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester at træffe konkrete foranstaltninger med henblik på at sikre sikkerheden i net og tjenester. Styrelsen fastsætter nærmere regler herom.

Bemyndigelsen i § 3, stk. 4, i lov om sikkerhed i net og tjenester er udmøntet i bekendtgørelse nr. 259 af 22. februar 2021 om sikkerhed og beredskab i net og tjenester. De nærmere regler følger af bekendtgørelsens kapitel 4 vedrørende påbud om konkrete informationssikkerhedsforanstaltninger.

Efter § 5, stk. 4, i lov om sikkerhed i net og tjenester kan Styrelsen for Samfundssikkerhed (tidligere Center for Cybersikkerhed) i beredskabssituationer og i andre ekstraordinære situationer påbyde erhvervsmæssige udbydere uden unødigt ophold at iværksætte nærmere angivne sikkerhedsforanstaltninger i tilfælde af en hændelse eller trussel, der i betydeligt omfang påvirker eller kan påvirke udbuddet af net eller tjenester negativt.

3.8.2. NIS 2-direktivet

Med artikel 43 i NIS 2-direktivet ophæves bl.a. artikel 41, stk. 1, i EU's telekodeks.

Der er i NIS 2-direktivets artikel 31-33 fastsat bestemmelser om tilsyn og håndhævelse. Medlemsstaterne forpligtes i disse bestemmelser til at sikre, at deres kompetente myndigheder effektivt overvåger og træffer de nødvendige foranstaltninger til at sikre, at direktivet overholdes.

Foranstaltningerne skal være effektive, stå i et rimeligt forhold til overtrædelsen og have en afskrækkende virkning under hensyntagen til omstændighederne i hver enkelt sag.

NIS 2-direktivets sondring mellem væsentlige og vigtige enheder er navnlig relevant i relation til tilsyn og håndhævelse. Direktivet oplister i henholdsvis artikel 32, stk. 4, og artikel 33, stk. 4, de håndhævelsesforanstaltninger, der som minimum skal kunne anvendes over for henholdsvis væsentlige og vigtige enheder, herunder for så vidt angår vigtige teleudbydere a) udstede advarsler om de pågældende enheders overtrædelser af direktivet, b) udstede bindende instrukser eller pålægge de pågældende enheder at afhjælpe de konstaterede mangler eller overtrædelserne af direktivet, c) pålægge de pågældende enheder at ophøre med at udvise adfærd, der overtræder dette direktiv, og afstå fra at gentage denne adfærd, d) pålægge de pågældende enheder, på en nærmere angivet måde og inden for en nærmere angivet frist at sikre, at deres foranstaltninger til styring af cybersikkerhedsrisici overholder artikel 21, eller at efterleve underretningsforpligtelserne i artikel 23, e) pålægge de pågældende enheder at underrette de fysiske eller juridiske personer med hensyn til hvilke de leverer tjenester eller udfører aktiviteter, som potentielt er berørt af en væsentlig cybertrussel, om denne trussels karakter samt om eventuelle beskyttelsesforanstaltninger eller afhjælpende foranstaltninger, som disse fysiske eller juridiske personer kan træffe som reaktion på denne trussel, f) pålægge de pågældende enheder at gennemføre de anbefalinger, der er fremsat som følge af en sikkerhedsaudit, inden for en rimelig frist og g) pålægge de pågældende enheder at offentliggøre aspekter af overtrædelser af dette direktiv på en nærmere angivet måde, og h) pålægge eller anmode de relevante organer eller domstole om i overensstemmelse med national ret at pålægge en

administrativ bøde i henhold til artikel 34 ud over enhver af de foranstaltninger, der er omhandlet i artikel 33, stk. 4, litra a)-g).

Overfor væsentlige enheder kan kompetente myndighed dog efter direktivets artikel 32, stk. 4, litra g, som noget særligt udpege en monitoreringsansvarlig med veldefinerede opgaver til i en nærmere fastsat periode at føre tilsyn med de pågældende enheders overholdelse af kravene til foranstaltninger til styring af cybersikkerhedsrisici og underretningsforpligtelser.

Den grundlæggende tilgang i NIS 2-direktivet og EU's telekodeks om, at teleudbyderne skal kunne pålægges håndhævelsesforanstaltninger svarer i vidt omfang til hinanden. Artikel 41, stk. 1, i EU's telekodeks giver imidlertid alene medlemsstaterne beføjelse til at pålægge teleudbydere at træffe foranstaltninger med henblik på at afhjælpe en sikkerhedshændelse eller hindre en sådan i at forekomme. Med den minimumsliste, som NIS 2-direktivet indeholder, tillægges medlemsstaterne dermed en række nye håndhævelsesforanstaltninger. Derudover er det med NIS 2-direktivet imidlertid alene væsentlige enheder, der kan pålægges at træffe foranstaltninger, der er nødvendige for at forhindre eller afhjælpe en hændelse.

NIS 2-direktivet foreskriver nærmere, hvilke hensyn der skal indgå i en afgørelse om at iværksætte håndhævelsesforanstaltninger. I direktivets artikel 32, stk. 7, er følgende hensyn oplistet: 1) Overtrædelsens grovhed og vigtigheden af de overtrådte bestemmelser, idet bl.a. følgende under alle omstændigheder skal betragtes som alvorlige overtrædelser: a) Gentagne overtrædelser, b) manglende underretning om eller afhjælpning af væsentlige hændelser, c) manglende afhjælpning af mangler efter bindende instrukser fra kompetente myndigheder, d) hindringer for audits eller overvågningsaktiviteter beordret af den kompetente myndighed efter konstatering af en overtrædelse og e) afgivelse af urigtige eller klart unøjagtige oplysninger vedrørende cybersikkerhedsrisikostyringsforanstaltninger eller rapporteringsforpligtelser, der er fastsat i artiklerne 21 og 23, 2) overtrædelsens varighed, 3) den pågældende enheds relevante tidligere overtrædelser, 4) enhver materiel eller immateriel skade, der er forårsaget, herunder ethvert finansielt eller økonomisk tab, virkninger for andre tjenester og antallet af brugere, der er berørt, 5) hvorvidt der ved overtrædelsen er handlet forsætligt eller uagtsomt, 6) enhver foranstaltning truffet af enheden for at forebygge eller afbøde den materielle eller immaterielle skade, 7) hvorvidt godkendte adfærdskodekser eller godkendte certificeringsmekanismer er overholdt, og 8) i hvilken udstrækning de fysiske eller juridiske personer, der holdes ansvarlige for overtrædelsen, samarbejder med de kompetente myndigheder.

3.8.2.1. Særligt om midlertidige suspensioner

For så vidt angår væsentlige enheder indeholder direktivet i artikel 32, stk. 5, et særligt virkemiddel i tilfælde, hvor en række mindre indgribende midler har vist sig ikke at være tilstrækkelige. I så fald skal de kompetente myndigheder – efter udløbet af en fastsat frist for at afhjælpe manglerne eller opfylde myndighedens krav – kunne a) midlertidigt suspendere eller anmode et certificerings- eller godkendelsesorgan eller en domstol om i overensstemmelse med national ret midlertidigt at suspendere en certificering eller godkendelse vedrørende dele af eller alle de relevante tjenester, der leveres, eller aktiviteter, der udføres af en væsentlig enhed, og b) anmode de relevante organer eller domstole om i overensstemmelse med national ret midlertidigt at forbyde enhver fysisk person med ledelsesansvar på direktionsniveau eller som juridisk repræsentant i den pågældende væsentlige enhed at udøve ledelsesfunktioner i den pågældende enhed.

Det følger endvidere af direktivets artikel 32, stk. 5, 2. led, at de midlertidige suspensioner eller forbud alene må anvendes, indtil den pågældende enhed træffer de nødvendige tiltag til at afhjælpe manglerne eller opfylde den kompetente myndigheds krav, som gav anledning til, at suspensionen eller forbuddet blev anvendt.

Efter direktivets artikel 32, stk. 5, 3. led, kan sådanne midlertidige suspensioner eller midlertidige forbud mod, at fysiske personer må udøve ledelsesfunktioner, ikke anvendes på offentlige forvaltningsenheder, der er omfattet af NIS 2-direktivet.

3.8.3. Ministeriet for Samfundssikkerhed og Beredskabs overvejelser

NIS 2-direktivet sonderer mellem håndhævelsesforanstaltninger for henholdsvis væsentlige og vigtige teleudbydere.

Derudover indeholder § 3, stk. 2 og 4, samt § 5, stk. 4, i lov om sikkerhed i net og tjenester yderligere håndhævelsesbeføjelser for Styrelsen for Samfundssikkerhed (tidligere Center for Cybersikkerhed), der går videre end de håndhævelsesbeføjelser, som følger af direktivet. Det drejer sig f.eks. om, at Styrelsen for Samfundssikkerhed har mulighed for at påbyde, at udbyderen skal inddrage nærmere angivne områder af dens virksomhed og nærmere angivne trusler mod sikkerheden i net og tjenester i deres risikostyringsprocesser eller muligheden for, såfremt det er af væsentlig samfundsmæssig betydning, at påbyde udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester at træffe konkrete foranstaltninger med henblik på at sikre sikkerheden i net og tjenester. Ministeriet vurderer, at Styrelsen for Samfundssikkerhed fortsat har brug for disse yderligere håndhævelsesforanstaltninger som supplement til de håndhævelsesforanstaltninger, der fremgår af NIS 2-direktivet.

Med henblik på at sikre en opretholdelse af det nuværende høje sikkerhedsniveau for telesektoren finder Ministeriet for Samfundssikkerhed og Beredskab, at indholdet af lovens § 3, stk. 2 og 4, samt § 5, stk. 4, bør videreføres. Ministeriet for Samfundssikkerhed og Beredskabs vurderer, at dette er

væsentligt henset til det generelt høje trusselsbillede på cyberområdet og telesektorens samfundsmæssige kritikalitet.

Det er Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at det er mest hensigtsmæssigt, at en afgørelse om midlertidigt at suspendere en certificering eller godkendelse eller midlertidigt at forbyde en fysisk person med ledelsesansvar på niveau med administrerende direktør eller den juridiske repræsentant hos enheden at udøve ledelsesfunktioner i den væsentlige enhed vil blive truffet af Styrelsen for Samfundssikkerhed, der vil kunne belyse og begrunde, hvorfor indgrebet vurderes påkrævet.

3.8.4. Den foreslåede ordning

Det foreslås, at Styrelsen for Samfundssikkerhed tillægges håndhævelsesforanstaltninger, der indholdsmæssigt svarer til det, som NIS 2-direktivet foreskriver, herunder med de forudsatte forskelle i tilgangen til væsentlige og vigtige teleudbydere, dog således, at indholdet af de skærpede nationale særregler omkring Styrelsen for Samfundssikkerhed beføjelser til at påbyde teleudbydere at inddrage, træffe og iværksætte nærmere foranstaltninger opretholdes som hidtil. Der er med videreførelsen således ikke tilsigtet materielle ændringer af de nuværende bestemmelsers indhold.

Det foreslås i forlængelse heraf i forhold til den særlige suspensions- og forbudsordning, som NIS 2-direktivet foreskriver i forhold til væsentlige teleudbydere, at såfremt Styrelsen for Samfundssikkerhed vurderer, at allerede pålagte håndhævelsesforanstaltninger har vist sig at være utilstrækkelige, kan styrelsen fastsætte en frist, inden for hvilken den væsentlige teleudbyder skal foretage de nødvendige tiltag for at afhjælpe manglerne eller opfylde styrelsens krav. Er tiltagene ikke foretaget inden for den fastsatte frist, kan Styrelsen for Samfundssikkerhed træffe afgørelse om 1) midlertidigt at suspendere en certificering eller godkendelse vedrørende dele af eller alle de relevante tjenester, udbyderen leverer, eller aktiviteter, der udføres af udbydere, og 2) midlertidigt at forbyde enhver fysisk person med ledelsesansvar på niveau med administrerende direktør eller den juridiske repræsentant hos udbyderen at udøve ledelsesfunktioner i den pågældende udbyder.

Det foreslås endvidere, at Styrelsen for Samfundssikkerhed skal kunne fastsætte nærmere regler for, hvilke certificeringer og godkendelser som skal kunne midlertidigt suspenderes. Det forudsættes ligeledes, at der ikke vil ske midlertidige suspensioner af certificeringer eller godkendelser, før Styrelsen for Samfundssikkerhed har anvendt den tillagte bemyndigelse.

Det vil være en forudsætning for anvendelse af ordningen, at mindre indgribende midler i form af anvendte håndhævelsesforanstaltninger har vist sig utilstrækkelige.

I overensstemmelse med direktivet foreslås det, at sådanne midlertidige suspensioner eller midlertidige forbud mod, at fysiske personer må udøve ledelsesfunktioner, kun kan anvendes, indtil teleudbyderen træffer de nødvendige tiltag for at afhjælpe de mangler eller opfylde de krav, som gav anledning til, at tiltagene blev anvendt.

Det foreslås endvidere, at teleudbyderen eller den fysiske person, som afgørelsen vedrører, kan forlange, at en afgørelse om suspension eller et midlertidigt forbud mod at fysiske personer må udøve ledelsesfunktioner, indbringes for domstolene.

Styrelsen for Samfundssikkerhed anlægger i givet fald sag inden for rammerne af den civile retspleje mod den teleudbyder eller person, som har forlangt sagen indbragt.

3.9. Ansvar og sanktioner

3.9.1. Gældende ret

Efter § 14, stk. 1, i lov om sikkerhed i net og tjenester straffes med bøde, medmindre strengere straf er forskyldt efter den øvrige lovgivning, den, der 1) undlader at efterkomme Styrelsen for Samfundssikkerhed (tidligere Center for Cybersikkerhed) påbud efter § 3, stk. 2, 3 eller 4, eller § 5, stk. 4, 2) overtræder § 6, stk. 1-4, 3) undlader at efterkomme Styrelsen for Samfundssikkerheds krav efter § 9, stk. 2, 4 eller 5, eller 4) hindrer Styrelsen for Samfundssikkerhed i at få adgang efter § 9, stk. 6 eller 7.

Efter § 14, stk. 2, i lov om sikkerhed i net og tjenester kan der i regler, som udfærdiges i medfør af § 3, stk. 1, 3 eller 4, § 4, § 5, stk. 1, 2 eller 3, § 5 a eller § 6, stk. 6, fastsættes straf i form af bøde for overtrædelse af bestemmelserne i reglerne.

Bemyndigelsen i § 14, stk. 2, i lov om sikkerhed i net og tjenester er, for så vidt angår lovens § 3, stk. 1, 3 og 4, og § 5, stk. 1 og 2, udmøntet i bekendtgørelse nr. 259 af 22. februar 2021 om sikkerhed og beredskab i net og tjenester. De nærmere regler følger af bekendtgørelsens kapitel 6 om straffebestemmelser og ikrafttrædelse.

Derudover er bemyndigelsen, for så vidt angår lovens § 4, udmøntet i bekendtgørelse nr. 1414 af 11. november 2023 om oplysnings- og underretningspligter vedrørende sikkerhed i net og tjenester. De nærmere regler følger af bekendtgørelsens § 15 om straffebestemmelser.

Bemyndigelsen er endvidere, for så vidt angår lovens 5, stk. 3, udmøntet i bekendtgørelse nr. 261 om beredskabsaktørers adgang til elektronisk kommunikation i beredskabssituationer mv. De nærmere regler følger af bekendtgørelsens kapitel 6 om straffebestemmelser og ikrafttrædelse.

Endeligt er bemyndigelsen, for så vidt angår lovens § 6, stk. 6, udmøntet i bekendtgørelse nr. 260 af 22. februar 2021 om sikkerhedsgodkendelse af medarbejdere på området for sikkerhed i net og tjenester. De nærmere regler følger af bekendtgørelsens § 2.

Efter § 14, stk. 3, i lov om sikkerhed i net og tjenester kan der pålægges selskaber mv. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.

Lov om sikkerhed i net og tjenester indeholder derimod ikke nærmere bestemmelser om ansvar for bestemte fysiske personer.

Lovens § 14, stk. 1-3, og de dele af bekendtgørelserne, der er udstedt i medfør af lovens § 14, stk. 2, er delvis implementering af artikel 29 i EU's telekodeks.

Det bemærkes således, at visse af de bestemmelser, der efter § 14 i lov om sikkerhed i net og tjenester er strafbelagte, udgør en del af den nationale særregulering, der ikke er implementering af EU-regulering, og som er fastsat for at sikre, at der tages højde for det generelt høje trusselsbillede på cyberområdet og telesektorens samfundsmæssige kritikalitet, jf. pkt. 2.1.3 ovenfor.

3.9.2. NIS 2-direktivet

NIS 2-direktivets artikel 36 fastsætter en forpligtelse for medlemsstaterne til at fastsætte regler om sanktioner, der skal anvendes i tilfælde af overtrædelse af de nationale foranstaltninger, der er vedtaget i medfør af direktivet, ligesom medlemsstaterne skal træffe alle nødvendige foranstaltninger for at sikre, at de gennemføres. Sanktionerne skal være effektive, stå i et rimeligt forhold til overtrædelsen og have afskrækkende virkning.

NIS 2-direktivets artikel 34 indeholder imidlertid – som noget nyt i forhold til EU's telekodeks – regler om generelle betingelser for pålæggelse af administrative bøder til væsentlige og vigtige enheder.

Det følger af NIS 2-direktivets artikel 34, stk. 2, at (administrative) bøder vil kunne blive pålagt i tillæg til en hvilken som helst af håndhævelsesforanstaltningerne vedrørende væsentlige og vigtige enheder, herunder – for så vidt angår væsentlige enheder – også den særlige suspensions- og forbudsordning.

NIS 2-direktivets artikel 34, stk. 3, foreskriver desuden nærmere, hvilke hensyn, der skal indgå i beslutningen om, hvorvidt der skal pålægges en bøde samt bødens størrelse. Hensynene er de samme som de hensyn, der skal indgå i en afgørelse om at træffe håndhævelsesforanstaltninger efter artikel 32, stk. 7, jf. pkt. 3.4.2 ovenfor.

Efter NIS 2-direktivets artikel 34, stk. 4, skal væsentlige enheders overtrædelse af direktivets artikel 21 (foranstaltninger til styring af cybersikkerhedsrisici) eller artikel 23 (rapporteringsforpligtelser) straffes med et maksimum på mindst 10.000.000 EUR eller et maksimum på mindst 2 pct. af den samlede globale årsomsætning i det foregående regnskabsår i den virksomhed, som den væsentlige enhed tilhører, alt efter, hvad der er højest.

Efter NIS 2-direktivets artikel 34, stk. 5, skal vigtige enheders overtrædelse af direktivets artikel 21 (foranstaltninger til styring af cybersikkerhedsrisici) eller artikel 23 (rapporteringsforpligtelser) straffes med et maksimum på mindst 7.000.000 EUR eller et maksimum på mindst 1,4 pct. af den samlede globale årsomsætning i det foregående regnskabsår i den virksomhed, som den vigtige enhed tilhører, alt efter, hvad der er højest.

Der lægges således i NIS 2-direktivets artikel 34 op til, at bøder pålægges administrativt – det vil sige af de kompetente myndigheder – medmindre medlemsstaternes nationale retssystem ikke giver mulighed herfor. I givet fald skal bestemmelserne om administrative bøder efter direktivets artikel 34, stk. 8, anvendes således, at disse i sidste ende pålægges af de nationale domstole. Det skal sikres, at virkningen svarer til virkningen af administrative bøder.

3.9.3. Ministeriet for Samfundssikkerhed og Beredskabs overvejelser

Indførelsen af administrative bøder giver i dansk ret anledning til forfatningsmæssige betænkeligheder. Det er i øvrigt i dansk retspleje et grundlæggende princip, at bødestraf kun kan pålægges under domstolenes medvirken og – som klart udgangspunkt – i strafferetsplejens former, der sikrer den sigtede en effektiv beskyttelse.

Det er på den baggrund Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at NIS 2-direktivets undtagelsesbestemmelse i artikel 34, stk. 8, i forhold til administrative bøder finder anvendelse. Direktivets bestemmelser om administrative bøder vil således skulle fortolkes og implementeres på en måde, hvor bøder ikke pålægges administrativt, men af de nationale domstole i det almindelige strafferetlige system, idet det samtidig sikres, at virkningen heraf svarer til virkningen af administrative bøder. Det indebærer, at Styrelsen for Samfundssikkerhed i givet fald vil skulle indgive politianmeldelse, såfremt de konstaterer strafbelagte overtrædelser af denne lov eller regler udstedt i medfør af denne lov, mens bøder kan pålægges og udmåles af domstolene i det almindelige straffeprocessuelle system.

Efter ministeriets opfattelse forudsættes det i den forbindelse, at omstændighederne i hver enkelt sag og sanktionsregimets effektivitet, forholdsmæssighed og afskrækkende virkning indgår i Styrelsen for Samfundssikkerhed beslutning om politianmeldelse af et forhold samt i politi- og anklagemyndighedens samt domstolenes vurdering af sagen, herunder ved udmålingen af en eventuel bøde.

Derudover gælder der i dansk ret typisk ikke noget lovbestemt maksimum for bødestørrelse. Det er dog Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at der bør fastsættes maksimale bødeniveauer svarende til de niveauer, der er fastsat i direktivet, idet der så vidt muligt foretages en direktivnær implementering af direktivet. Dermed vil der ikke kunne straffes med højere bøder end det minimumsniveau, der er forudsat i direktivet.

Der henvises til de bemærkningerne til den foreslåede § 31.

3.9.3.1. Særligt om fysiske personers strafansvar, herunder valg af ansvarssubjekt

NIS 2-direktivets artikel 34 indeholder generelle betingelser for pålæggelse af bøder rettet mod væsentlige og vigtige enheder, og dermed de juridiske personer som sådan. De forudsatte bødeniveauer udmåles bl.a. på baggrund af virksomhedens årsomsætning.

Det følger dog af NIS 2-direktivets artikel 32, stk. 6 – som noget nyt i forhold til EU's telekodeks – at medlemsstaterne sikrer, at enhver fysisk person, der er ansvarlig for eller optræder som juridisk repræsentant for en væsentlig enhed på grundlag af beføjelsen til at repræsentere den, beføjelsen til at træffe afgørelser på dennes vegne eller beføjelsen til at udøve kontrol over den, har beføjelse til at sikre, at den overholder NIS 2-direktivet. Medlemsstaterne sikrer, at det er muligt at drage sådanne fysiske personer til ansvar for tilsidesættelse af deres forpligtelser til at sikre overholdelse af dette direktiv.

Det er i NIS 2-direktivets præambelbetragtning nr. 130 forudsat, at hvor en bøde pålægges en person, der ikke er en virksomhed, bør den kompetente myndighed ved fastsættelsen af en passende bødestørrelse tage hensyn til det generelle indkomstniveau i den pågældende medlemsstat og personens økonomiske stilling.

Efter NIS 2-direktivets artikel 20, stk. 1, skal væsentlige og vigtige enheders ledelsesorganer kunne gøres ansvarlige for enhedernes overtrædelser af forpligtelserne i artikel 21 (om foranstaltninger til styring af cybersikkerhedsrisici). Artikel 20, stk. 1, berører dog ikke national ret for så vidt angår de ansvarsregler, der gælder for offentlige institutioner, samt ansvaret for embedsmænd og personer valgt eller udnævnt til offentlige hverv, jf. bestemmelsens 2. led.

Det følger af rigsadvokatmeddelelsen om strafansvar for juridiske personer, at udgangspunktet ved valg af ansvarssubjekt i særlovgivningen er, at tiltalen rejses mod den juridiske person.

Det er i den forbindelse en forudsætning for at pålægge en juridisk person ansvar, at der inden for dens virksomhed er begået en overtrædelse, der kan tilregnes en eller flere til virksomheden knyttede personer eller virksomheden som sådan, jf. straffelovens § 27, stk. 1.

Det fremgår dog også af rigsadvokatmeddelelsen, at der i en række tilfælde kan være anledning til – ud over tiltalen mod den juridiske person – tillige at rejse tiltale mod en eller flere fysiske personer, såfremt den eller de pågældende har handlet forsætligt eller udvist grov uagtsomhed. Der angives endvidere retningslinjer for anklagemyndighedens afgørelsen herom.

Det beskrives i den forbindelse, at der på en række områder er fastsat særlige regler, som pålægger enkeltpersoner et selvstændigt og individuelt strafansvar i kraft af deres særlige stilling eller funktion, eksempelvis piloter og besætningsmedlemmer. I så fald er udgangspunktet, at der rejses tiltale mod den pågældende person samt i almindelighed tillige mod den juridiske person. I visse tilfælde indeholder lovgivningen endvidere mulighed for et selvstændigt og individuelt strafansvar, selv om overtrædelsen ikke kan tilregnes de pågældende som forsætlig eller uagtsom (objektivt individualansvar).

Ministeriet for Samfundssikkerhed og Beredskab finder ikke på dette område anledning til at fastsætte særlige regler om et selvstændigt og individuelt strafansvar for fysiske personer, herunder regler, som går videre end strafansvaret for juridiske personer. Det er således Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at NIS 2-direktivets krav om, at nærmere bestemte fysiske personer kan drages til ansvar for tilsidesættelse af deres forpligtelser efter direktivet ikke synes at stille krav, der går videre end det, der allerede følger af de gældende regler.

Dermed vil et eventuelt strafansvar for fysiske personer følge det almindelige udgangspunkt i særlovgivningen, hvorefter der i tillæg til den juridiske person efter nærmere retningslinjer kan rejses tiltale mod en fysisk person, såfremt denne har handlet forsætligt eller groft uagtsomt. Bøder vil i givet fald skulle udmåles i overensstemmelse med direktivets forudsætninger om størrelsen heraf.

3.9.3.2. Særligt om brud på persondatasikkerheden

Det følger af NIS 2-direktivets artikel 35, stk. 1, at hvor de kompetente myndigheder i forbindelse med tilsyn eller håndhævelse bliver opmærksomme på, at en væsentlig eller vigtig enheds overtrædelse af forpligtelserne i dette direktivs artikel 21 og 23 kan medføre et brud på persondatasikkerheden som defineret i artikel 4, nr. 12), i forordning (EU) 2016/679, som skal anmeldes i henhold til nævnte forordnings artikel 33, underretter de uden unødigt ophold tilsynsmyndigheder som omhandlet i nævnte forordnings artikel 55 eller 56.

Det følger endvidere af direktivets artikel 35, stk. 2, at der ikke kan straffes med (administrativ) bøde for overtrædelser af de ovenfor nævnte bestemmelser i medfør af NIS 2-direktivet, såfremt den samme adfærd straffes med (administrativ) bøde efter databeskyttelsesforordningen.

Henset til, at der ikke anvendes administrative bøder i dansk ret, jf. ovenfor, vil bestemmelserne skulle fortolkes og gennemføres i lyset heraf.

Det bemærkes, at databeskyttelsesloven supplerer og gennemfører databeskyttelsesforordningen i dansk ret, og at lovens § 41 indeholder bestemmelser om straf for overtrædelser af databeskyttelsesforordningen og databeskyttelsesloven.

Henset til, at et brud på cybersikkerheden efter omstændighederne også kan udgøre et brud på persondatasikkerheden, er bestemmelsen i NIS 2-direktivets artikel 35, stk. 2, udtryk for det almindelige forbud mod dobbelt strafforfølgning. Det anføres således i præambelbetragtning nr. 131, at pålæggelse af sanktioner for overtrædelse af de nationale regler, der gennemfører NIS 2-direktivet, ikke bør føre til et brud på

princippet om *ne bis in idem* som fortolket af Den Europæiske Unions Domstol.

Det følger af NIS 2-direktivet, at de kompetente myndigheder ikke er afskåret fra at anvende håndhævelsesforanstaltninger i de pågældende situationer.

For at sikre, at myndighederne har mulighed for at undgå, at den samme adfærd straffes dobbelt, forpligter NIS 2-direktivets artikel 35, stk. 1, de kompetente myndigheder efter NIS 2-direktivet til uden unødigt ophold at underrette tilsynsmyndighederne efter databeskyttelsesforordningen. Det følge af databeskyttelseslovens § 27, stk. 1, at Datatilsynet fører tilsyn med enhver behandling, der er omfattet af denne lov, databeskyttelsesforordningen og anden lovgivning, som ligger inden for databeskyttelsesforordningens rammer for særregler om behandling af personoplysninger. Det fremgår dog samtidig af databeskyttelseslovens § 1, stk. 3, at regler om behandling af personoplysninger i anden lovgivning, som ligger inden for databeskyttelsesforordningens rammer for særregler om behandling af personoplysninger, går forud for reglerne i denne lov.

Sådanne særregler er bl.a. fastsat i telelovens § 8, stk. 2, nr. 2 og bekendtgørelse om persondatasikkerhed i forbindelse med udbud af offentlige elektroniske kommunikationstjenester og nummeruafhængige interpersonelle kommunikationstjenester. Disse regler forpligter udbydere af offentlige elektroniske kommunikationstjenester og nummeruafhængige interpersonelle kommunikationstjenester til at underrette Digitaliseringsstyrelsen om brud på persondatasikkerheden, når bruddet opstår i relation til udbuddet af sådanne tjenester.

Der skal således i sådanne tilfælde ske anmeldelse af brud på persondatasikkerheden til Digitaliseringsstyrelsen og ikke Datatilsynet.

Det omfatter tilfælde, hvor de kompetente myndigheder i forbindelse med deres tilsyn eller håndhævelse bliver opmærksomme på, at en væsentlig eller vigtig enheds overtrædelse af forpligtelserne i NIS 2-direktivets artikel 21 (foranstaltninger til styring af cybersikkerhedsrisici) eller 23 (rapporteringsforpligtelser) kan medføre et brud på persondatasikkerheden, som skal anmeldes i henhold til artikel 33 i databeskyttelsesforordningen.

Ministeriet for Samfundssikkerhed og Beredskab bemærker i forlængelse heraf, at det af databeskyttelsesforordningens artikel 4, nr. 12, følger, at »brud på persondatasikkerheden« er defineret som et brud på sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet. Bestemmelsen i forordningens artikel 33, stk. 1, indebærer, at den dataansvarlige skal anmelde et brud på persondatasikkerheden til Datatilsynet, »medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder«. Som beskrevet ovenfor vil anmeldelse i dette tilfælde skulle ske til Digitaliseringsstyrelsen.

Styrelsen for Samfundssikkerhed vil derfor alene skulle foretage underretning af Digitaliseringsstyrelsen på baggrund af NIS 2-direktivets artikel 35, stk. 1, om mulige brud på persondatasikkerheden, hvis det ikke er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder. Der må overlades Styrelsen for Samfundssikkerhed et bredt skøn ved foretagelsen af denne vurdering.

Det forudsættes, at Styrelsen for Samfundssikkerhed i relevant omfang hører Digitaliseringsstyrelsen om, hvorvidt den adfærd, der var genstand for overtrædelsen af NIS 2-direktivet, er eller vil blive straffet med bøde for overtrædelse af databeskyttelsesforordningen eller databeskyttelsesloven med henblik på, at NIS 2-direktivets hensigt om at undgå dobbelt strafforfølgning kan indfries i praksis.

3.9.4. Den foreslåede ordning

Det foreslås, at der indsættes sanktionsbestemmelser i loven med det formål, at overtrædelse af alle materielle og processuelle krav i loven eller regler udstedt i medfør af loven til væsentlige og vigtige udbydere kan straffes med bøde.

På den baggrund foreslås det først og fremmest, at den, der overtræder § 5, stk. 1, eller 2, § 7, stk. 1-3, § 8, stk. 2, jf. stk. 3, § 9, stk. 1 og § 11, stk. 1 og 2, undlader at efterkomme en afgørelse efter § 21, stk. 1, nr. eller 2, undlader at efterkomme påbud efter § 13, stk. 5, eller § 18, stk. 1 og 2, undlader at efterkomme krav efter § 19, stk. 1, nr. 5-8, eller § 22, stk. 1, nr. 4-7, eller hindrer Styrelsen for Samfundssikkerhed i at føre tilsyn efter bestemmelserne i § 19, stk. 1, nr. 1-4, eller § 22, stk. 1, nr. 1-3, straffes med bøde.

Det foreslås i den forbindelse, at der ikke anvendes administrative bøder, men at Styrelsen for Samfundssikkerhed indstiller til bøde gennem politianmeldelse, og at bøder pålægges og udmåles af domstolene i det almindelige strafferprocessuelle system.

Det foreslås desuden, at bøder vil kunne pålægges fysiske personer og selskaber mv. (juridiske personer), i det omfang de omfattes af lovens anvendelsesområde.

Det forudsættes i overensstemmelse med NIS 2-direktivets artikel 34, stk. 4 og 5, at bødens størrelse for så vidt angår væsentlige teleudbyderes overtrædelse af bestemmelserne i § 5, stk. 1 eller 2, §§ 8, 9, stk. 1, § 10, stk. 1 eller 2, eller § 12, og reglerne udstedt i medfør af § 33, stk. 4, maksimalt vil kunne udgøre et beløb svarende til 10.000.000 euro eller 2 pct. af udbyderens samlede globale årsomsætning i det foregående regnskabsår, alt efter, hvad der er højest. Det forudsættes desuden, at bødens størrelse for så vidt angår vigtige teleudbyderes overtrædelse af de samme bestemmelser maksimalt vil kunne udgøre et beløb svarende til 7.000.000 euro eller 1,4 pct. af udbyderens samlede glo-

bale årsomsætning i det foregående regnskabsår, alt efter, hvad der er højest.

NIS 2-direktivet indeholder ikke særlige forudsætninger for så vidt angår det maksimale bødeniveau for manglende efterlevelse af forpligtelser i direktivet ud over artikel 21 (foranstaltninger til styring af cybersikkerhedsrisici) og artikel 23 (rapporteringsforpligtelser). På den baggrund fastsættes der ikke maksimale bødeniveauer for overtrædelse af lovens øvrige bestemmelser.

Bøderne vil kunne pålægges i tillæg til håndhævelsesforanstaltningerne i de foreslåede §§ 20, 21 og 23.

Det foreslås, at Styrelsen for Samfundssikkerhed påser overholdelsen af denne lov og regler udstedt i medfør af loven, herunder undersøger mulige lovovertrædelser.

Den foreslåede ordning vil indebære, at såfremt Styrelsen for Samfundssikkerhed i en konkret sag vurderer, at der er sket en strafbar overtrædelse af loven eller regler udstedt i medfør af loven, indgiver styrelsen politianmeldelse.

Det vil herefter være politiet og anklagemyndigheden, der vurderer, hvorvidt man vil rejse tiltale i sagen.

Ved Styrelsen for Samfundssikkerheds afgørelse om at politianmelde et forhold samt i politi- og anklagemyndighedens samt domstolenes vurdering af sagen, herunder ved udmålingen af en eventuel bøde, forudsættes det, at der lægges vægt på de i pkt. 3.9.3 beskrevne hensyn, herunder omstændighederne i hver enkelt sag og sanktionsregimets effektivitet, forholdsmæssighed og afskrækkende virkning.

Det foreslås endvidere i overensstemmelse med direktivet, at hvor der er pålagt en bøde for overtrædelse af databeskyttelsesforordningen eller databeskyttelsesloven, kan der ikke pålægges en bøde for overtrædelse af denne lov eller regler udstedt i medfør af loven, hvis overtrædelsen skyldes den samme adfærd.

Endeligt foreslås det, at de skærpede nationale særregler, der foreslås videreført i §§ 18 og 13, stk. 5 og 7, fortsat skal være strafbelagte som hidtil. Der er med videreførelsen således ikke tilsigtet materielle ændringer af de nuværende bestemmelsers indhold. Det indebærer, at for overtrædelse af de nævnte bestemmelser vil det således fortsat være de hidtidige bødeniveauer, der vil skulle udmåles efter.

4. Forholdet til databeskyttelsesforordningen og databeskyttelsesloven

Med lovforslaget gennemføres NIS 2-direktivet i telesektoren.

Lovforslaget indebærer en række forpligtelser for omfattede teleudbydere samt myndighedsopgaver for Styrelsen for Samfundssikkerhed, der i et vist omfang vil indebære behandling af personoplysninger.

Der kan således indgå almindelige personoplysninger i de oplysninger, som teleudbyderne som led i overholdelsen af registreringsforpligtelsen i den foreslåede bestemmelse i § 7, sk. 1, skal indgive til Styrelsen for Samfundssikkerhed, eksempelvis i form af visse kontaktoplysninger på medarbejdere hos teleudbyderen.

Derudover kan der indgå almindelige personoplysninger i en teleudbyders hændelsesunderretning til Styrelsen for Samfundssikkerhed i medfør af de foreslåede bestemmelser i §§ 8 og 9. Dette vil eksempelvis kunne være i forbindelse med en redegørelse for hændelsens faktiske forløb, eller ved at der vedlægges e-mails, logningsoplysninger eller andet materiale, der belyser hændelsens forløb, karakter eller håndtering.

Der kan endvidere i forbindelse med anvendelsen af tilsyns- og håndhævelsesforanstaltninger i medfør af de foreslåede bestemmelser i §§ 19-21 samt §§ 22 og 23 blive behandlet almindelige personoplysninger. Det er Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at de oplysninger, der måtte blive behandlet i denne forbindelse, vil udgøre oplysninger om teleudbyderens medarbejdere. Disse oplysninger vil primært udgøre kontaktoplysninger på teleudbyderens kontaktpersoner, ligesom der eksempelvis kan være tale om oplysninger om, hvilke medarbejdere, der har adgang til teleudbyderens net- og informationssystemer.

Det følger af NIS 2-direktivets artikel 2, stk. 14, 1. led, at enheder, de kompetente myndigheder, de centrale kontaktpunkter og CSIRT'erne behandler personoplysninger i det omfang, det er nødvendigt med henblik på dette direktiv og i overensstemmelse med databeskyttelsesforordningen, navnlig på grundlag af artikel 6 deri.

Det er Ministeriet for Samfundssikkerhed og Beredskab opfattelse, at Styrelsen for Samfundssikkerheds behandling af almindelige personoplysninger i forbindelse med overholdelsen af registreringsforpligtelsen i § 7 og underretningsforpligtelserne i § 8 og § 9 samt i forbindelse med Styrelsen for Samfundssikkerheds anvendelse af tilsyns- og håndhævelsesforanstaltninger efter §§ 19-21 samt §§ 22 og 23 for private virksomheder vil kunne ske i medfør af databeskyttelsesforordningens artikel 6, stk. 1, litra c og e. Det følger af artikel 6, stk. 1, litra c, at behandling er lovlig, hvis den er nødvendig for at overholde en retlig forpligtelse, som påhviler den dataansvarlige, ligesom det følger af litra e, at behandling er lovlig, hvis den er nødvendig af hensyn til udførelse af en opgave i samfundets interesse.

Ministeriet for Samfundssikkerhed og Beredskab skal afslutningsvis bemærke, at det forudsættes, at de øvrige bestemmelser i databeskyttelsesforordningen og databeskyttelsesloven, herunder de grundlæggende principper i databeskyttelsesforordningens artikel 5, også iagttages, når der behandles personoplysninger i medfør af de foreslåede bestemmelser.

5. Økonomiske konsekvenser og implementeringskonsekvenser for det offentlige

Styrelsen for Samfundssikkerhed, som er myndighed for informationssikkerhed og beredskab i telesektoren, vil fortsat skulle føre tilsyn med teleudbyderes overholdelse af loven, og regler, der er udstedt i medfør heraf. Styrelsen for Samfundssikkerhed vil imidlertid i medfør af de foreslåede §§ 19 og 22, der bl.a. implementerer NIS 2-direktivet, kunne foretage et mere omfattende og – for så vidt angår de væsentlige teleudbydere – forudgående tilsyn end hidtil. Som følge heraf kan der være visse administrative meromkostninger forbundet hermed, men disse vil blive afholdt inden for den eksisterende bevillingsmæssige ramme.

I det omfang staten udbyder offentlige elektroniske kommunikationsnet og offentligt tilgængelige elektroniske kommunikationstjenester, vil de krav, der efter lovforslaget stilles til udbydere af disse net og tjenester, også omfatte staten. Det vil kunne medføre økonomiske konsekvenser og implementeringskonsekvenser i samme omfang som for private udbydere.

Det bemærkes i den forbindelse, at kommuner og regioner, der udbyder offentlige elektroniske kommunikationsnet og offentligt tilgængelige elektroniske kommunikationstjenester, ikke er omfattet af nærværende lovforslag, men derimod foreslås omfattet af forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau.

5.4.1. De syv principper for digitaliseringsklar lovgivning

Det er Ministeriet for Samfundssikkerhed og Beredskabs vurdering, at lovforslaget er i overensstemmelse med principperne for digitaliseringsklar lovgivning.

Princip nr. 1 om enkle og klare regler er efter Ministeriet for Samfundssikkerhed og Beredskab opfattelse iagttaget, idet det i lovforslaget – inden for NIS 2-direktivets rammer – klart fremgår, hvilke forpligtelser der påhviler omfattede teleudbydere, og hvilke beføjelser Styrelsen for Samfundssikkerhed har i sit tilsyn med teleudbydernes efterlevelse af deres forpligtelser.

Det er desuden Ministeriet for Samfundssikkerhed og Beredskab opfattelse, at lovforslaget er udarbejdet i overensstemmelse med princip nr. 2 om digital kommunikation, idet § 35 indfører hjemmel til at fastsætte regler om digital kommunikation.

Derudover er det Ministeriet for Samfundssikkerhed og Beredskab opfattelse, at lovforslaget er i overensstemmelse med princip nr. 5 om tryg og sikker datahåndtering henset til, at lovforslaget indeholder en grundig beskrivelse af forholdet til databeskyttelsesretten, ligesom NIS 2-direktivet fremmer et højere og mere ensartet cybersikkerhedsniveau på tværs af EU's medlemslande.

Det bemærkes navnlig i relation til registrerings- og underretningspligterne i § 7 og § 10, at der med lovforslaget forudsættes anvendt digitale selvbetjeningsløsninger såsom Virk.dk. Dermed anvendes eksisterende offentlig it-infrastruktur til digital kommunikation mellem teleudbyderne og Styrelsen for Samfundssikkerhed, hvilket vurderes at være i overensstemmelse med princip nr. 6 om anvendelse af offentlig infrastruktur.

Det er Ministeriet for Samfundssikkerhed og Beredskab vurdering, at de øvrige principper ikke er relevante for lovforslaget.

6. Økonomiske og administrative konsekvenser for erhvervslivet mv.

Lovforslaget medfører administrative omkostninger for erhvervslivet på over 4 mio. kr. De administrative omkostninger består særligt i § 5, hvor der stilles krav til teleudbydere om passende og forholdsmæssige tekniske, operationelle og organisatoriske foranstaltninger for at styre risiciene for sikkerheden i net- og informationssystemer. Teleudbydere skal bl.a. udarbejde politikker for risikoanalyse og informationssystemsikkerhed, jf. den foreslåede bestemmelse § 5, stk. 1, nr. 1, politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af sikkerhedsrisici, jf. den foreslåede § 5, stk. 1, nr. 6 samt politikker og procedurer vedrørende brug af kryptografi og, hvor det er relevant, kryptering, jf. den foreslåede § 5, stk. 1, nr. 8. Der er en række andre krav i § 5, stk. 1, som også forventes at medføre administrative omkostninger.

Derudover vil der også være administrative konsekvenser ved kravet i § 6, stk. 2 om, at ledelsen skal deltage i kurser om styring af informationssikkerhed, registreringspligten jf. § 7, underretningspligten ved væsentlige hændelser jf. §§ 8 og 9, pligt til at underrette modtagere af virksomhedernes tjenester om væsentlige hændelser jf. § 11, og krav om sikkerhedsgodkendelse af visse medarbejdere i virksomhederne jf. § 16, stk. 1. Desuden vil der blive ført tilsyn med teleudbydere jf. §§ 19 og 22, som også vil medføre administrative konsekvenser for erhvervslivet.

Lovforslaget giver hjemmel til udstedelse af bekendtgørelser, som indebærer administrative konsekvenser for erhvervslivet, jf. bl.a. lovforslagets § 5, stk. 3, som bemyndigeren ministeren til at fastsætte nærmere regler om krav til foranstaltninger efter § 5, stk. 1, samt krav om yderligere foranstaltninger for teleudbydere omfattet af loven § 7, stk. 4-5, som bemyndiger ministeren for samfundssikkerhed og beredskab til at fastsætte nærmere regler om yderligere oplysninger, teleudbydere skal afgive ved registrering, samt oplysnings- og underretningspligter for teleudbydere, § 8, stk. 3, som bemyndiger ministeren til at fastsætte nærmere regler om, hvornår en hændelse anses for at være væsentlig samt hvilke oplysninger, der skal gives i forbindelse med underretningen, § 13, stk. 4 og 5, som bemyndiger ministeren til at fastsætte nærmere regler i beredskabs- og andre ekstraordinære situationer og § 16, stk. 2, som bemyndiger ministeren til, efter forhandling med justitsministeren, at fastsætte regler om ansøgninger vedr. sikkerhedsgodkendelser af medarbejdere hos teleudbydere. Lovforslagets bemyndigelsesbestemmelser vurderes at medføre administrative konsekvenser over 4 mio. kr. og skal som udgangspunkt

kvantificeres forud for den offentlige høring af bekendtgørelserne.

Det vurderes, at omkring 175 teleudbydere helt eller delvis vil blive omfattet af nye krav som følge af lovforslaget.

Det vurderes på baggrund af ovenstående, at de samlede administrative omkostninger for erhvervslivet er over 4 mio. kr. Det har dog ikke været muligt at gennemføre en AM-VAB-måling af konsekvenserne inden udløbet af fristen for den offentlige høring, og det kan heller ikke nås inden fremsættelsen i Folketinget. Denne vil derfor blive foretaget ex post efter lovforslagets ikrafttræden.

Det har endvidere ikke været muligt at foretage en kvantificering af de erhvervsøkonomiske konsekvenser for erhvervslivet inden den offentlige høring. Det vurderes foreløbigt, at lovforslaget medfører øvrige efterlevelseskonsekvenser for erhvervslivet på mindre end 10 mio. kr. De økonomiske konsekvenser for erhvervslivet vil blive kvantificeret nærmere af Ministeriet for Samfundssikkerhed og Beredskab snarest muligt efter lovens ikrafttræden.

7. Administrative konsekvenser for borgerne

Lovforslaget vurderes ikke at have administrative konsekvenser for borgerne.

8. Klimamæssige konsekvenser

Lovforslaget vurderes ikke at have klimamæssige konsekvenser.

9. Miljø- og naturmæssige konsekvenser

Lovforslaget vurderes ikke at have miljø- og naturmæssige konsekvenser.

10. Forholdet til EU-retten

Loven og de bekendtgørelser, der vil blive udstedt i medfør af loven, gennemfører dele af Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen, om ændring af forordning (EU) nr. 910/2014 og direktiv (EU) 2018/1972 og om ophævelse af direktiv (EU) 2016/1148 (NIS 2-direktivet) i dansk ret. Derudover gennemfører loven og de bekendtgørelser, der vil udstedt i medfør af loven, dele af Europa-Parlamentets og Rådets direktiv (EU) 2018/1972 af 11. december 2018 om oprettelse af en europæisk kodeks for elektronisk kommunikation (omarbejdning).

Det følger af artikel 41, stk. 1, i NIS 2-direktivet, at direktivet skal være implementeret i dansk ret senest den 17. oktober 2024 og finde anvendelse senest den 18. oktober 2024. Med den foreslåede bestemmelse i § 32 vil loven dermed træde i kraft 1. juli 2025. Det bemærkes, at de dele af EU's telekodeks, der i dag henhører under Ministeriet for Samfundssikkerhed og Beredskabs ressortansvar, tidligere er implementeret i dansk ret ved lov nr. 1831 af 8. december 2020 om ændring af lov om net- og informationssikkerhed (Implementering af direktivet om oprettelse af en europæisk kodeks for elektronisk kommunikation, for så vidt angår sikkerhed i net og tjenester).

10.1. Principper for implementering af erhvervsrettet EU-regulering

For så vidt angår princip nr. 1 om, at den nationale regulering som udgangspunkt ikke bør gå videre end minimumskravene i EU-reguleringen, bemærkes det, at lovforslaget indebærer videreførelse af nationale særregler, der på visse områder går videre end de krav, der følger af NIS 2-direktivet. Det er Ministeriet for Samfundssikkerhed og Beredskabs vurdering, at der er væsentlige hensyn, der taler for, at der med lovforslaget sker en videreførelse af de eksisterende skærpede nationale særregler med henblik på at sikre en opretholdelse af det nuværende høje sikkerhedsniveau for telesektoren. Dette skal ses i lyset af det generelt høje trusselsbillede på cyberområdet og telesektorens samfundsmæssige kritikalitet. Ministeriet for Samfundssikkerhed og Beredskab vurderer således, at lovforslaget fraviger princip nr. 1, idet ministeriet i forbindelse med implementeringen af NIS 2-direktivet fastholder de allerede eksisterende skærpede nationale særregler.

For så vidt angår princip 2 om, at danske virksomheder ikke bør stilles dårligere i den internationale konkurrence, hvorfor implementeringen ikke bør være mere byrdefuld end den forventede implementering i sammenlignelige lande, er det Ministeriet for Samfundssikkerhed og Beredskabs vurdering, at implementeringen lever op til dette princip. Med lovforslaget foretages en minimumsimplementering af de nye cybersikkerhedskrav samt oplysnings- og underretningspligter, der følger af NIS 2-direktivet. Samtidig er det Ministeriet for Samfundssikkerhed og Beredskabs vurdering, at der er særlige hensyn, der taler for, at der med lovforslaget sker en videreførelse af de eksisterende skærpede nationale særregler med henblik på at sikre en opretholdelse af det nuværende høje sikkerhedsniveau for telesektoren. Dette skal ses i lyset af det generelt høje trusselsbillede på cyberområdet og telesektorens samfundsmæssige kritikalitet, jf. pkt. 2.1.3.

For så vidt angår princip 3 om, at fleksibilitet og undtagelsesmuligheder i EU-reguleringen bør udnyttes, skal det bemærkes, at Ministeriet for Samfundssikkerhed og Beredskab har afsøgt mulighederne herfor. NIS 2-direktivet indeholder imidlertid ikke sådanne muligheder i relation til telesektoren.

For så vidt angår princip 4 om, at EU-regulering – i det omfang det er muligt og hensigtsmæssigt, bør implementeres gennem alternativer til regulering, har Ministeriet for Samfundssikkerhed og Beredskab overvejet, om det er muligt og hensigtsmæssigt, at NIS 2-direktivet implementeres gennem alternativer til regulering. Ministeriet for Samfundssikkerhed og Beredskab vurderer imidlertid, at der er tale om et direktiv, der skal implementeres ved lovgivning.

For så vidt angår princip 5 om, at byrdefuld EU-regulering bør træde i kraft senest muligt og under hensyntagen til de fælles ikrafttrædelsesdatoer, er det Ministeriet for Samfundssikkerhed og Beredskabs vurdering, at den foreslåede ikrafttrædelsesdato i § 32 lever op til dette princip.

11. Hørte myndigheder og organisationer mv.

Et udkast til lovforslag har i perioden fra 12. december 2024 til den 9. januar 2025 (28 dage) været sendt i høring hos følgende myndigheder og organisationer mv.:

Advokatrådet, Amnesty International, Bauer Media, Borch Teknik, Cibicom A/S, Danmarks Radio, Dansk Beredskabskommunikation A/S, Dansk Energi, Dansk Erhverv, Dansk Industri (DI), DANSK IT, Dansk Kabel TV, Danske Advokater, Danske Regioner, Datatilsynet, DanPilot, Den Danske Dommerforening, DI Digital, Domstolsstyrelsen, Fibia A/S, Forenede Danske Antenneanlæg, GLOBALCONNECT A/S, Hi3G Denmark ApS, HORESTA, Institut for Menneskerettigheder, IT-Branchen, IT-Politisk Forening, Justitia, KL, Norlys, Præsidenten for Vestre Landsret, Præsidenten for Østre Landsret, Retspolitisk Forening, Rigsrevisionen, Rådet for Digital Sikkerhed, Samtlige byretspræsidenter, TDC A/S, TeleDCIS Teleindustrien (TI), Telenor A/S, Telia Company Danmark A/S, TT-Netværket P/S, TV 2 DTT A/S og Waoo A/S.

12. Sammenfattende skema

	Positive konsekvenser/mindreudgifter (hvis ja, angiv omfang/hvis nej, anfør »Ingen«)	Negative konsekvenser/merudgifter (hvis ja, angiv omfang/hvis nej, anfør »Ingen«)
Økonomiske konsekvenser for stat, kommuner og regioner	Ingen.	De statsfinansielle konsekvenser til øgede aktiviteter afstedkommet af lovforslaget vurderes at være beskedne og vil blive afholdt inden for egen ramme.
Implementeringskonsekvenser for stat, kommuner og regioner	Ingen.	Ingen.
Økonomiske konsekvenser for erhvervslivet mv.	Ingen.	Lovforslaget forventes at medføre negative erhvervsøkonomiske konsekvenser for erhvervslivet, som ikke er blevet yderligere kvantificeret, inden lovforslagets fremsættelse.
Administrative konsekvenser for erhvervslivet mv.	Ingen.	Lovforslaget forventes at medføre negative administrative konsekvenser for erhvervslivet, som forventes at være mere end 4 mio. kr. Disse er dog ikke blevet kvantificeret, jf. lovforslagets pkt. 6.
Administrative konsekvenser for borgerne	Ingen.	Ingen.
Klimamæssige konsekvenser	Ingen.	Ingen.
Miljø- og naturmæssige konsekvenser	Ingen.	Ingen.
Forholdet til EU-retten	Loven og de bekendtgørelser, der vil blive udstedt i medfør af loven, gennemfører dele af Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022 om foranstaltninger til sikring af et højt cybersikkerhedsniveau i hele Unionen, om ændring af forordning (EU) nr. 910/2014 og direktiv (EU) 2018/1972 og om ophævelse af direktiv (EU) 2016/1148 (NIS 2-direktivet). Der henvises til EU-tidende 2022, L nr. 333, side 80.	
Er i strid med de fem principper for implementering af erhvervsrettet EU-regulering (der i relevant omfang også gælder ved implementering af ikke-	Ja X	Nej

erhvervsrettet EU-regulering) (sæt X)	

Bemærkninger til lovforslagets enkelte bestemmelser

Til § 1

Lov om sikkerhed i net og tjenester, jf. lovbekendtgørelse nr. 153 af 1. februar 2021, som ændret ved § 18 i lov nr. 1156 af 8. juni 2021, regulerer i dag informationssikkerhed og beredskab i telesektoren, og finder anvendelse for udbydere af elektroniske kommunikationsnet eller -tjenester.

Det følger af NIS 2-direktivets artikel 2, stk. 1, at direktivet bl.a. finder anvendelse på udbydere af offentlige elektroniske kommunikationsnet og offentligt tilgængelige elektroniske kommunikationstjenester, jf. direktivets bilag I, pkt. 8. Det følger af derudover af NIS 2-direktivets artikel 26, stk. 1, litra a, at udbydere af offentlige elektroniske kommunikationsnet eller af offentligt tilgængelige elektroniske kommunikationstjenester anses for at henhøre under jurisdiktionen i den medlemsstat, hvor de leverer deres net eller tjenester.

Det følger af det foreslåede *stk. 1*, at loven finder anvendelse for teleudbydere, der med et kommercielt formål stiller offentlige elektroniske kommunikationsnet og offentligt tilgængelige elektroniske kommunikationstjenester til rådighed i Danmark, jf. dog stk. 2.

Den foreslåede bestemmelse gennemfører NIS 2-direktivets artikel 2, stk.1, og artikel 26.

Det foreslås med *stk. 2,* at loven ikke finder anvendelse for kommuner og regioner, der stiller offentlige elektroniske kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester til rådighed.

Baggrunden herfor er, at det følger af bemærkningerne til den foreslåede § 1, stk. 2, i det samtidig fremsatte forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau, at 'i telesektoren vil enheder i enhedskategorierne »udbydere af offentlige elektroniske kommunikationsnet« og »udbydere af offentligt tilgængelige elektroniske kommunikationstjenester«, i sektoren »Digital infrastruktur« i bilag I til NIS 2-direktivet, som udgangspunkt blive omfattet af lov om sikkerhed og beredskab i telesektoren. I det omfang kommuner og regioner måtte udbyde offentlige elektroniske kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester, vil de imidlertid være omfattet af nærværende lov. '

Til § 2

Lov om net og informationssikkerhed indeholder visse definitioner, som foreslås videreført i den foreslåede § 2, mens størstedelen af definitionerne i NIS 2-direktivet ikke findes i dansk ret.

Den foreslåede bestemmelse i *§ 2* indeholder definitioner af lovens centrale begreber.

Definitionerne bygger hovedsageligt på de tilsvarende definitioner i NIS 2-direktivet. Hertil kommer videreførelse af centrale definitioner i lov om sikkerhed i net og tjenester, som ophæves med nærværende lov.

Det foreslås at affatte definitionen i *nr. 1,* således »Beredskabssituationer og andre ekstraordinære situationer« defineres som situationer hvor der allerede er, eller hvor der kan opstå større ulykker, katastrofer eller hændelser, herunder krise eller krig og som kan påvirke udbuddet af net og tjenester.

Definitionen svarer i vidt omfang til den gældende definition af beredskabssituationer og andre ekstraordinære situationer i § 1, nr. 2 i bekendtgørelse nr. 259 af 22. februar 2021 om sikkerhed og beredskab i net og tjenester. Bekendtgørelsen definerer beredskabssituationer og andre ekstraordinære situationer som 'Større ulykker, katastrofer eller hændelser, hvor det kan være nødvendigt at indføre særlige foranstaltninger vedrørende net og tjenester med henblik på at kunne opretholde samfundets funktioner. Den nuværende definition omfatter alene tilfælde, hvor der er indtrådt en beredskabssituation eller anden ekstraordinær situation og ikke situationer, hvor der kan være risiko for dette. Det betyder i praksis, at der ikke kan gøres brug af de eksisterende handlemuligheder i forbindelse med planlagte begivenheder, herunder eksempelvis i forbindelse med opdatering af SINE-netværket.

Med den foreslåede ændring af definition vil handlemulighederne i beredskabssituationer og andre ekstraordinære situationer også kunne iværksættes, hvor der er risiko for påvirkning af udbuddet i net og tjenester.

Det foreslås, at affatte definitionen i *nr. 2,* således »cybertrussel« defineres som enhver potentiel omstændighed, begivenhed eller handling, som kan skade, forstyrre eller på anden måde have en negativ indvirkning på net- og informationssystemer, brugerne af sådanne systemer og andre personer.

Efter NIS 2-direktivets artikel 6, nr. 10, skal cybertrussel forstås på samme måde som definitionen i artikel 2, nr. 8, i Europa-Parlamentets og Rådets forordning (EU) 2019/881 af 17. april 2019 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed), om cybersikkerhedscertificering af informations- og kommunikationsteknologi og om ophævelse af forordning (EU) nr. 526/2013 (forordningen om cybersikkerhed).

Den foreslåede bestemmelse svarer til definitionen i den nævnte forordning. Det forudsættes, at bestemmelsen fortolkes i overensstemmelse med denne definition.

Det foreslås, at affatte definitionen i *nr. 3* således »elektronisk kommunikationsnet« defineres som et transmissionssystem, uanset om det bygger på en permanent infrastruktur eller en centraliseret administrationskapacitet, og, hvor det er relevant, koblings- og dirigeringsudstyr og andre ressourcer, herunder netelementer, der ikke er aktive, som gør det muligt at overføre signaler ved hjælp af trådforbindelse, radiobølger, lyslederteknik eller andre elektromagnetiske midler, herunder satellitnet, jordbaserede fastnet (kredsløbs- og pakkekoblede, herunder i internettet) og mobilnet, elkabelsystemer, i det omfang de anvendes til transmission af signaler, net, som anvendes til radio- og tv-spredning, og kabel-tv-net, uanset hvilken type information der overføres.

NIS 2-direktivets artikel 6, nr. 1, litra a) definerer et elektronisk kommunikationsnet ved en henvisning til artikel 2, nr. 1), i direktiv (EU) 2018/1972 (EU's telekodeks). Den foreslåede definition i nr. 3, svarer til definitionen af et elektronisk kommunikationsnet i artikel 2, nr. 1, i EU's telekodeks, og skal fortolkes i overensstemmelse hermed.

Det foreslås, at affatte definitionen i *nr. 3,* således »elektronisk kommunikationstjeneste« defineres som en tjeneste, som normalt ydes mod betaling via elektroniske kommunikationsnet, og som med undtagelse af tjenester, der består i tilrådighedsstillelse af eller udøvelse af redaktionel kontrol over indhold fremført via elektroniske kommunikationsnet og -tjenester omfatter følgende typer tjenester; internetadgangstjenester, interpersonelle kommunikationstjenester og tjenester, der udelukkende eller overvejende består i overføring af signaler, som f.eks. transmissionstjenester, der anvendes til levering af maskine-til-maskine-tjenester og til radio- og tv-spredning.

Med NIS 2-direktivets artikel 6, nr. 37, defineres en elektronisk kommunikationstjeneste ved en henvisning til artikel 2, nr. 4), i EU's telekodeks. Den foreslåede definition i nr. 3, svarer til definitionen af en elektronisk kommunikationstjeneste i artikel 2, nr. 4, i EU's telekodeks, og skal fortolkes i overensstemmelse hermed.

Det fremgår af artikel 2, nr. 4, i EU's telekodeks, at elektroniske kommunikationstjenester omfatter tre typer af tjenester, herunder navnlig internetadgangstjenester, interpersonelle kommunikationstjenester og tjenester, der udelukkende eller overvejende består i overføring af signaler, som f.eks. transmissionstjenester, der anvendes til levering af maskine-til-maskine-tjenester og til radio- og tv-spredning.

Det foreslås, at affatte definitionen i *nr. 5,* således »hændelse« defineres som en begivenhed, der bringer tilgængeligheden, autenticiteten, integriteten eller fortroligheden af lagrede, overførte eller behandlede data eller af de tjenester, der tilbydes af eller er tilgængelige via net- og informationssystemer, i fare.

Den foreslåede bestemmelse svarer til definitionen i NIS 2-direktivets artikel 6, nr. 6. Det forudsættes, at bestemmelsen fortolkes i overensstemmelse med direktivets definition.

Det foreslås, at affatte definitionen i *nr. 6,* således »håndtering af hændelser« defineres som enhver handling og procedure, der tager sigte på at forebygge, opdage, analysere og inddæmme eller at reagere på og reetablere sig efter en hændelse.

Den foreslåede bestemmelse svarer til definitionen i NIS 2-direktivets artikel 6, nr. 8. Det forudsættes, at bestemmelsen fortolkes i overensstemmelse med direktivets definition.

Det foreslås, at affatte definitionen i *nr. 7,* således »interpersonel kommunikationstjeneste« defineres som en tjeneste, som normalt ydes mod betaling, og som muliggør direkte interpersonel og interaktiv informationsudveksling via elektroniske kommunikationsnet mellem et afgrænset antal personer, hvor de personer, der indleder eller deltager i kommunikationen, bestemmer hvem modtageren eller modtagerne skal være, undtaget tjenester, der blot muliggør interpersonel og interaktiv kommunikation som en mindre støttefunktion, der er tæt knyttet til en anden tjeneste.

Definitionen svarer med enkelte sproglige justeringer til den tilsvarende definition i artikel 2, nr. 5, i EU's telekodeks, hvorefter der ved »interpersonel kommunikationstjeneste« forstås en tjeneste, som normalt ydes mod betaling, og som muliggør direkte interpersonel og interaktiv informationsudveksling via elektroniske kommunikationsnet mellem et afgrænset antal personer, hvor de personer, der indleder eller deltager i kommunikationen, bestemmer hvem modtageren eller modtagerne skal være, og omfatter ikke tjenester, der blot muliggør interpersonel og interaktiv kommunikation som en mindre støttefunktion, der er tæt knyttet til en anden tjeneste.

Ifølge EU's telekodeks omfatter interpersonelle kommunikationstjenester, to typer af tjenester, herunder både nummerbaserede- og nummeruafhængige kommunikationstjenester.

Det forudsættes, at definitionen af en interpersonel kommunikationstjeneste fortolkes i overensstemmelse med den tilsvarende definition i EU's telekodeks.

Det foreslås, at affatte definitionen i *nr. 8,* således »net- og informationssystem« defineres som a) et elektronisk kommunikationsnet, jf. den foreslåede nr. 3, b) enhver anordning eller gruppe af forbundne eller beslægtede anordninger, hvoraf en eller flere ved hjælp af et program udfører automatisk behandling af digitale data, og c) digitale data, som lagres, behandles, fremfindes eller overføres af elementer i litra a og b med henblik på deres drift, brug, beskyttelse og vedligeholdelse.

Den foreslåede bestemmelse svarer til definitionen i NIS 2-direktivets artikel 6, nr. 1, litra a. Det forudsættes, at definitionen forstås og fortolkes i overensstemmelse med definitionen i direktivet. Det bemærkes, at NIS 2-direktivets artikel 6, nr. 1, litra a, henviser til definitionen i EU's telekodeks artikel 2, nr. 1. Det forudsættes således desuden, at

definitionen forstås og fortolkes i overensstemmelse med definitionen i EU's telekodeks.

Det foreslås, at affatte definitionen i *nr. 9,* således »nærvedhændelse« defineres som en begivenhed, der kunne have bragt tilgængeligheden, autenticiteten, integriteten eller fortroligheden af lagrede, overførte eller behandlede data eller af de tjenester, der tilbydes af eller er tilgængelige via net- og informationssystemer, i fare, men som det lykkedes at forhindre, eller som ikke indtraf.

Den foreslåede bestemmelse svarer til definitionen i NIS 2-direktivets artikel 6, nr. 5. Det forudsættes, at bestemmelsen fortolkes i overensstemmelse med direktivets definition.

Det foreslås, at affatte definitionen i *nr. 10,* således »offentligt elektronisk kommunikationsnet« defineres som et elektronisk kommunikationsnet, som udelukkende eller overvejende bruges til udbud af elektroniske kommunikationstjenester, der er tilgængelige for offentligheden, og som danner grundlag for overførsel af information mellem netterminеringspunkter.

Den foreslåede bestemmelse svarer til definitionen i NIS 2-direktivets artikel 6, nr. 36, som henviser til definitionen i artikel 2, nr. 8, i EU's telekodeks.

Det foreslås, at affatte definitionen i *nr. 11,* således »offentligt tilgængelige elektroniske kommunikationstjenester« defineres som: en elektronisk kommunikationstjeneste, jf. det foreslåede nr. 4, der stilles til rådighed for en ikke på forhånd afgrænset kreds af slutbrugere eller teleudbydere.

Det foreslås, at affatte definitionen i *nr. 12,* således »radiobaseret lokalnet« defineres som et trådløst adgangssystem med lav effekt og lille rækkevidde, der har en lav risiko for at skabe interferens med andre sådanne systemer etableret i nærheden af andre brugere, og som på et ikkeeksklusivt grundlag anvender harmoniserede radiofrekvenser (RLAN).

Den foreslåede bestemmelse svarer til definitionen i artikel 2, nr. 24, i EU's telekodeks, og skal fortolkes i overensstemmelse hermed.

Det foreslås, at affatte definitionen i *nr. 13,* således »sikkerhed i net- og informationssystemer« defineres som net- og informationssystemers, jf. det foreslåede nr. 8, evne til, på et givet sikkerhedsniveau, at modstå enhver begivenhed, der kan være til skade for tilgængeligheden, autenticiteten, integriteten eller fortroligheden af lagrede, overførte eller behandlede data eller af de tjenester, der tilbydes af eller er tilgængelige via disse net- og informationssystemer.

Den foreslåede bestemmelse svarer til definitionen i NIS 2-direktivets artikel 6, nr. 2. Det forudsættes, at definitionen forstås og fortolkes i overensstemmelse med direktivets definition.

Det foreslås, at affatte definitionen i *nr. 14,* således »teleudbyder« defineres som den, der med et kommercielt formål stiller produkter af offentlige elektroniske kommunikationsnet og offentligt tilgængelige elektroniske kommunikationstjenester til rådighed for andre.

Definitionen viderefører definitionen af en erhvervsmæssig udbyder i § 2, nr. 5, i lov om sikkerhed i net og tjenester, og skal fortolkes i overensstemmelse hermed.

Det foreslås, at affatte definitionen i *nr. 15,* således »væsentlig cybertrussel« defineres som en cybertrussel, som på grundlag af sine tekniske karakteristika kan antages at have potentiale til at få alvorlig indvirkning på en udbyders net- og informationssystemer eller på brugerne af udbyderens tjenester ved at forårsage betydelig fysisk eller ikke fysisk skade.

Den foreslåede bestemmelse svarer til definitionen i NIS 2-direktivets artikel 6, nr. 11. Det forudsættes, at bestemmelsen forstås og fortolkes i overensstemmelse med direktivets definition.

Til § 3

Lov om sikkerhed i net og tjenester indeholder ikke en definition af væsentlige teleudbydere.

Efter NIS 2-direktivets artikel 3, stk. 1, litra a, anses enheder af en type, som er omhandlet i direktivets bilag I, og som overskrider tærsklerne for mellemstore virksomheder, der er fastsat i artikel 2, stk. 1, i bilaget til henstilling 2003/361/EF, for at være væsentlige enheder.

Det følger af den foreslåede *§ 3, stk. 1,* at teleudbydere, der med et kommercielt formål udbyder offentlige elektroniske kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester som deres hovedydelse, eller som en ikke-accessorisk del af virksomheden, anses for at være væsentlige, hvis de opfylder mindst én af følgende betingelser: 1) udbyderen beskæftiger mere end 50 ansatte, eller 2) udbyderen har en årlig omsætning på over 10 mio. EUR og en årlig balance på over 10 mio. EUR.

Den foreslåede bestemmelse vil gennemføre artikel 3, stk. 1, litra a, i NIS 2-direktivet.

Hvorvidt en enhed overskrider tærsklerne for mellemstore virksomheder efter den foreslåede bestemmelse, vil skulle vurderes ud fra de kriterier, der er fastsat i artikel 2, stk. 1, i bilaget til Europa-Kommissionens henstilling 2003/361/EF af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder. I artikel 2, stk. 1, i bilaget til henstilling 2003/361/EF af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder afgrænses kategorien af mikrovirksomheder, små og mellemstore virksomheder (SMV'er) som virksomheder, som beskæftiger under 250 personer, og har en årlig omsætning på ikke over 50 mio. EUR eller en årlig samlet balance på ikke over 43 mio. EUR.

Henstillingen må fortolkes således, at virksomheder falder

inden for definitionen af mellemstore virksomheder, når virksomheden har 50 ansatte eller derover eller en årlig omsætning på 10 mio. EUR eller derover og en årlig balance på 10 mio. EUR eller derover. Der henvises i øvrigt til gennemgangen heraf i pkt. 3.1.3.

For at sikre, at enheder, der har partnervirksomheder eller tilknyttede virksomheder, ikke betragtes som væsentlige enheder, hvor dette ville være uforholdsmæssigt, skal der i overensstemmelse med præambelbetragtning nr. 16 til NIS 2-direktivet tages hensyn til den grad af uafhængighed, som en enhed har i forhold til sine partnervirksomheder eller tilknyttede virksomheder. Der kan i denne forbindelse navnlig tages hensyn til, om en enhed er uafhængig af sine partnervirksomheder eller tilknyttede virksomheder med hensyn til de net- og informationssystemer, som enheden anvender i forbindelse med leveringen af sine tjenester og med hensyn til de tjenester, som enheden leverer.

På dette grundlag kan medlemsstaterne i overensstemmelse med præambelbetragtning nr. 16, hvor det er hensigtsmæssigt, anse en sådan enhed for ikke at udgøre en mellemstor virksomhed i henhold til artikel 2, i bilaget til henstilling 2003/361/EF, eller for ikke at overskride tærsklerne for en mellemstor virksomhed fastsat i nævnte artikels stk. 1, hvis den pågældende enhed i betragtning af dennes grad af uafhængighed ikke ville være blevet anset for at udgøre en mellemstor virksomhed eller at overskride disse tærskler, hvis kun dens egne data var blevet taget i betragtning.

Det foreslås, at alene teleudbydere, der opfylder størrelseskravet, og som med et kommercielt formål udbyder offentlige elektroniske kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester som deres hovedydelse, eller som en ikke-accessorisk del af virksomheden, anses for at være væsentlige.

Det afgørende for, om udbuddet sker med et kommercielt formål er, om udbuddet et nettet eller tjenesten sker på markedsmæssige vilkår, herunder som led i markedsføringen af virksomheden eller foreningen.

Som ikke-accessorisk del af virksomheden forstås, at udbuddet ikke kun er en accessorisk del af virksomheden. Et hotel, der for eksempel tilbyder sine kunder adgang til trådløst internet vil således som udgangspunkt ikke opfylde kravet, idet udbuddet i den forbindelse må anses for at være en integreret del af at leje et hotelværelse.

Formålet med tilføjelsen af kravet om kommercielt formål og at udbuddet skal være en ikke-accessorisk del af virksomheden er at sikre, at de nye skærpede regler efter NIS 2-direktivet ikke finder anvendelse for udbydere, der ikke meningsfuldt kan siges at falde ind under kategorien væsentlige teleudbydere efter NIS 2-direktivet.

Der henvises til den nærmere uddybning af lovens udbyderbegreb i pkt. 3.1.4.

Det foreslås i *stk. 2*, at uanset deres størrelse anses følgende teleudbydere for væsentlige teleudbydere: 1) teleudbydere, der er den eneste udbyder i Danmark af et net eller en tjeneste, der er væsentlig for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter, 2) en forstyrrelse af det net eller den tjeneste, teleudbyderen leverer, vil kunne have væsentlig indvirkning på den offentlige sikkerhed eller folkesundheden, 3) en forstyrrelse af det net eller den tjeneste, teleudbyderen leverer, vil kunne medføre en væsentlig systemisk risiko, herunder hvor en sådan forstyrrelse kan have en grænseoverskridende virkning, 4) teleudbyderen er kritisk på grund af sin specifikke betydning på nationalt eller regionalt plan for sektoren eller type af net eller tjeneste eller for andre indbyrdes afhængige sektorer i Danmark, eller 5) teleudbyderen er identificeret som en kritisk enhed i henhold til lov om kritiske enheders modstandsdygtighed.

Den foreslåede bestemmelse vil gennemføre artikel 3, stk. 1, litra c, litra e-f og artikel 2, stk. 2, litra b-e, i NIS 2-direktivet.

Den foreslåede bestemmelse svarer indholdsmæssigt til NIS 2-direktivets artikel 3, stk. 1, litra c, litra e-f og artikel 2, stk. 2, litra b-e, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Det bemærkes, at der inden lovforslagets ikrafttrædelse vil blive offentliggjort vejledningsmateriale, som vil hjælpe omfattede teleudbydere med at vurdere, om de er omfattet af den foreslåede bestemmelse, ligesom teleudbydere vil kunne få den fornødne vejledning herom fra Styrelsen for Samfundssikkerhed.

Det følger af det foreslåede *nr. 1,* at teleudbydere, der er den eneste udbyder i Danmark af et net eller en tjeneste, der er væsentlig for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter, anses for væsentlige teleudbydere.

Bestemmelsen skal forstås således, at teleudbyderen skal være den reelt eneste udbyder i Danmark.

Det følger af det foreslåede *nr. 2,* at en forstyrrelse af det net eller den tjeneste, teleudbyderen leverer, vil kunne have væsentlig indvirkning på den offentlige sikkerhed eller folkesundheden, anses for væsentlige teleudbydere.

Det følger af det foreslåede *nr. 3,* at en forstyrrelse af det net eller den tjeneste, teleudbyderen leverer, vil kunne medføre en væsentlig systemisk risiko, herunder hvor en sådan forstyrrelse kan have en grænseoverskridende virkning, anses for væsentlige teleudbydere.

Det følger af det foreslåede *nr. 4,* at teleudbydere, som er kritiske på grund af sin specifikke betydning på nationalt eller regionalt plan for sektoren eller type af net eller tjeneste eller for andre indbyrdes afhængige sektorer i Danmark, anses for væsentlige teleudbydere.

Det følger af det foreslåede *nr. 5,* at teleudbydere, der er

identificeret som en kritisk enhed i henhold til lov om kritiske enheders modstandsdygtighed, anses for væsentlige teleudbydere.

Det foreslås i *stk. 3*, at ministeren for samfundssikkerhed og beredskab kan fastsætte nærmere regler om kriterier for, hvornår enheder er omfattet af stk. 2.

Bemyndigelsesbestemmelsen giver Ministeriet for Samfundssikkerhed og Beredskab mulighed for at fastsætte nærmere kriterier for, hvornår enheder er omfattet af bestemmelsens stk. 2. Samtidig sikres gennem bemyndigelsesbestemmelsen, at kriterierne for, hvornår teleudbydere er omfattet at stk. 2, løbende og smidigt kan tilpasses og målrettes, således at det kan sikres, at kravene er i overensstemmelse med eventuelle delegerede retsakter, som Europa-Kommissionen måtte vedtage.

Den foreslåede bestemmelse skal endvidere sikre, at der kan tages højde for forskellige teknologier og typer af tjenesteudbud, hvor disse ikke entydigt kan eller bør vurderes efter samme væsentlighedskriterier. M2M og IoT-tjenester er konkrete eksempler, hvor den nuværende anvendelse af antal slutbrugere som kriterie for, hvornår en række bestemmelser bringes i anvendelse, i praksis har medført en skævvridning mellem ellers sammenlignelige teleudbydere i henhold til sikkerhed i net og tjenester eller i forhold til kritikaliteten af deres tjenesteudbud.

Til § 4

Det følger af det foreslåede *stk. 1,* at teleudbydere, der ikke opfylder kriterierne for at være væsentlige udbydere efter lovens § 3, anses som vigtige teleudbydere, såfremt de med et kommercielt formål udbyder offentlige elektroniske kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester som deres hovedydelse, eller som en ikke-accessorisk del af virksomheden.

Den foreslåede bestemmelse vil gennemføre NIS 2-direktivets artikel 3, stk. 2, 1. pkt., som fastsætter, at enheder af en type omhandlet af direktivets bilag I eller II, der ikke opfylder kriterierne for at være væsentlige enheder i henhold til artikel 3, stk. 1, anses for at være vigtige enheder.

Teleudbydere, som med et kommercielt formål udbyder offentlige elektroniske kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester som en accessorisk del af virksomheden, herunder RLAN-udbydere, anses således ikke som vigtige teleudbydere.

Det følger af det foreslåede *stk. 2,* at Styrelsen for Samfundssikkerhed kan træffe afgørelse om, at en teleudbyder, der er omfattet af § 3, stk. 2, nr. 1-4, skal anses som en vigtig teleudbyder. Der vil være tale om en forvaltningsretlig afgørelse, hvorfor forvaltningslovens regler herom vil finde anvendelse.

Den foreslåede bestemmelse vil delvist gennemføre NIS 2-direktivets artikel 3, stk. 2, jf. artikel 3, stk. 1, litra e og g. Det følger af artikel 3, stk. 2, at enheder af en type omhandlet i direktivets bilag I eller II, der ikke opfylder kriterierne for at være væsentlige enheder i henhold til artikel 3, stk. 1, anses for at være vigtige enheder. Dette indbefatter enheder, som medlemsstaterne har identificeret som vigtige enheder i medfør af artikel 2, stk. 2, litra b-e.

Den foreslåede bestemmelse indebærer, at Styrelsen for Samfundssikkerhed kan træffe afgørelse om, at en enhed, der er omfattet af loven på baggrund af de kvalitative kriterier i relation til deres samfundsmæssige betydning, jf. NIS 2-direktivets artikel 2, stk. 2, litra b-e, skal anses for at være en vigtig teleudbyder uanset udgangspunktet i det foreslåede § 3, stk. 2, nr. 1-4.

Såfremt en enhed i medfør af øvrige dele af lovforslagets § 3, herunder stk. 1, eller stk. 2, nr. 5, må anses for at være en væsentlig teleudbyder, vil der ikke kunne ske ændring af enhedens status fra væsentlig til vigtig efter den foreslåede bestemmelse.

Der henvises i øvrigt til lovforslagets pkt. 3.1.

Til § 5

Det følger af § 3, stk. 1, i lov om sikkerhed i net og tjenester, at Styrelsen for Samfundssikkerhed fastsætter regler om minimumskrav til sikkerhed i net og tjenester for udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester og udbydere af NUIK-tjenester, herunder krav om passende tekniske, processuelle og organisatoriske foranstaltninger med henblik på risikostyring i forhold til sikkerhed i net og tjenester og opretholdelse af et passende sikkerhedsniveau, herunder krav om, at sådanne foranstaltninger gennemføres på baggrund af dokumenterede og ledelsesforankrede processer.

Det følger af den foreslåede *stk. 1,* at væsentlige og vigtige teleudbydere skal træffe passende og forholdsmæssige tekniske, operationelle og organisatoriske foranstaltninger for at styre risiciene for sikkerheden i net- og informationssystemer, som disse enheder anvender til deres operationer eller til at levere deres tjenester, og for at forhindre hændelser eller minimere deres indvirkning på modtagere af deres tjenester og på andre tjenester. Foranstaltningerne skal som minimum omfatte de i bestemmelsens nr. 1-10 angivne foranstaltninger.

Den foreslåede bestemmelse vil gennemføre artikel 21, stk. 1-3, i NIS 2-direktivet.

Det fremgår af NIS 2-direktivets artikel 21, stk. 1, at medlemsstaterne skal sikre, at væsentlige og vigtige enheder træffer passende og forholdsmæssige tekniske, operationelle og organisatoriske foranstaltninger for at styre risiciene for sikkerheden i net- og informationssystemer, som disse enheder anvender til deres operationer eller til at levere deres tjenester, og for at forhindre hændelser eller minimere deres indvirkning på modtagere af deres tjenester og på andre tjenester. Foranstaltningerne skal under hensyntagen

til det aktuelle teknologiske stade og i givet fald til relevante europæiske og internationale standarder samt gennemførelsesomkostningerne tilvejebringe et sikkerhedsniveau i net- og informationssystemer, der står i forhold til risiciene. Ved vurderingen af proportionaliteten af disse foranstaltninger skal der tages behørigt hensyn til graden af enhedens eksponering for risici, enhedens størrelse og sandsynligheden for hændelser og deres alvor, herunder deres samfundsmæssige og økonomiske indvirkning.

Det fremgår af NIS 2-direktivets artikel 21, stk. 2, at de i stk. 1 omhandlede foranstaltninger skal baseres på en tilgang, der omfatter alle farer og sigter på at beskytte net- og informationssystemer og disse systemers fysiske miljø mod hændelser.

Efter NIS 2-direktivets artikel 21, stk. 3, skal medlemsstaterne sikre, at enhederne, når de overvejer hvilke foranstaltninger efter artikel 21, stk. 2, litra d, om forsyningssikkerhed der er passende, skal tage hensyn til de sårbarheder, der er specifikke for hver direkte leverandør og tjenesteudbyder, og den generelle kvalitet af deres leverandørers og tjenesteudbyderes produkter og cybersikkerhedspraksis, herunder deres sikre udviklingsprocedurer. Enhederne skal desuden tage hensyn til resultaterne af de koordinerede sikkerhedsrisikovurderinger af kritiske forsyningskæder, der kan foretages af Samarbejdsgruppen i samarbejde med Europa-Kommissionen og ENISA i overensstemmelse med NIS 2-direktivets artikel 22, stk. 1.

I overensstemmelse med direktivets forudsætninger, som udtrykt i præambelbetragtning nr. 83, 2. pkt., vil forpligtelsen til at indføre foranstaltninger til styring af cybersikkerhedsrisici finde anvendelse på væsentlige og vigtige enheder, uanset om de selv vedligeholder deres net- og informationssystemer eller outsourcer vedligeholdelsen deraf.

I overensstemmelse med præambelbetragtning nr. 79 skal foranstaltningerne omfatte alle farer og sigte på at beskytte net- og informationssystemer og de pågældende systemers fysiske miljø mod enhver begivenhed såsom tyveri, brand, oversvømmelse, telekommunikations- eller strømsvigt, eller uautoriseret fysisk adgang til, beskadigelse af eller indgreb i en væsentlig eller vigtig enheds informations- og informationsbehandlingsfaciliteter, som kan kompromittere tilgængeligheden, autenticiteten, integriteten eller fortroligheden af lagrede, overførte eller behandlede data eller de tjenester, der tilbydes af eller er tilgængelige via net- og informationssystemerne. Foranstaltningerne bør derfor også adressere den fysiske og miljømæssige sikkerhed i net- og informationssystemerne ved at inkludere foranstaltninger til beskyttelse af sådanne systemer mod systemsvigt, menneskelige fejl, ondsindede handlinger eller naturfænomener i overensstemmelse med europæiske og internationale standarder såsom dem, der indgår i ISO/IEC 27000-serien.

Det bemærkes, at væsentlige og vigtige teleudbydere i overensstemmelse med forvaltningslovens § 7 i fornødent omfang vil kunne få vejledning og bistand fra Styrelsen for Samfundssikkerhed.

Det foreslås i *nr. 1,* at foranstaltningerne skal omfatte eller tage højde for politikker for risikoanalyse og informationssystemsikkerhed.

Dette indebærer bl.a., at enheden skal udarbejde en politik for informationssikkerhed, der fastlægger den overordnede ramme for implementering af foranstaltninger, jf. § 6, stk. 1, nr. 1-10, som understøtter sikkerheden i enhedens omfattede net- og informationssystemer. Enheder skal endvidere udarbejde en politik for risikostyring, der identificerer og adresserer eventuelle risici i forhold til sikkerheden i net- og informationssystemer

Det følger af det foreslåede *nr. 2,* at foranstaltningerne skal omfatte eller tage højde for håndtering af hændelser.

Dette indebærer bl.a., at enheder skal udarbejde procedurer for håndtering af hændelser. Enheder skal således i fornødent omfang implementere logning og monitorering af uregelmæssigheder i enhedens net- og informationssystemer med henblik på at kunne identificere hændelser. Logdata skal derudover sikres mod manipulation og beskyttes mod uautoriseret adgang.

Det foreslås i *nr. 3*, at foranstaltningerne skal omfatte eller tage højde for driftskontinuitet.

Dette indebærer, at enheder skal udarbejde procedurer til sikring af driftskontinuitet i tilfælde af en hændelse. På grundlag af enhedernes risikostyring, jf. nr. 2, og driftskontinuitetsprocedure, skal enheder således udarbejde procedurer for backupstyring og gendannelse af data. Enheder skal foretage en vurdering af behovet for at udarbejde en beredskabsplan for krisestyring og reetablering efter en katastrofe. Enheder skal foretage en vurdering af, om der er behov for at etablere redundans, nødstrømsforsyning, understøttende forsyning eller anden sikring med tilsvarende virkning for enhedens net- og informationssystemer.

Det foreslås i *nr. 4,* at foranstaltninger skal omfatte eller tage højde for forsyningssikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem den enkelte enhed og dens direkte leverandører eller tjenesteudbydere.

Dette indebærer, at enheder skal udarbejde procedurer for leverandørstyring for at sikre passende forsyningskædesikkerhed. Der henvises i den forbindelse til NIS 2-direktivets artikel 21, stk. 3, hvoraf det følger, at enhederne, når de overvejer, hvilke foranstaltninger, der er passende, tager hensyn til de sårbarheder, der er specifikke for hver direkte leverandør og tjenesteudbyder, og den generelle kvalitet af deres leverandørers og tjenesteudbyderes produkter og cybersikkerhedspraksis, herunder deres sikre udviklingsprocedurer. Det fremgår i forlængelse heraf, at medlemsstaterne sikrer, at enhederne, når de overvejer, hvilke foranstaltninger omhandlet § 21, stk. 2, litra d, der er passende, er forpligtet til at tage hensyn til resultaterne af de koordinere-

de sikkerhedsrisikovurderinger af kritiske forsyningskæder, der foretages i overensstemmelse med artikel 22, stk. 1, hvoraf det fremgår, at samarbejdsgruppen i samarbejde med Kommissionen og ENISA kan foretage koordinerede sikkerhedsrisikovurderinger af specifikke kritiske IKT-tjenester, -systemer eller -produktforsyningskæder under hensyntagen til tekniske og, hvor det er relevant, ikketekniske risikofaktorer.

Der henvises endvidere til NIS 2-direktivets præambelbetragtning nr. 85, hvoraf det fremgår, at håndtering af risici, der stammer fra en enheds forsyningskæde og dens forhold til sine leverandører såsom udbydere af datalagrings- og databehandlingstjenester eller udbydere af administrerede sikkerhedstjenester og softwareudgivere, er særlig vigtig i betragtning af udbredelsen af hændelser, hvor enheder har været udsat for cyberangreb, og hvor ondsindede gerningspersoner har været i stand til at kompromittere sikkerheden af en enheds net- og informationssystemer ved at udnytte sårbarheder, der påvirker tredjepartsprodukter og -tjenester. Væsentlige og vigtige enheder bør derfor vurdere og tage hensyn til den generelle kvalitet og modstandsdygtighed af produkter og tjenester, de heri integrerede foranstaltninger til styring af cybersikkerhedsrisici og deres leverandørers og tjenesteudbyderes cybersikkerhedspraksis, herunder deres sikre udviklingsprocedurer. Væsentlige og vigtige enheder bør navnlig tilskyndes til at indarbejde foranstaltninger til styring af cybersikkerhedsrisici i kontraktlige arrangementer med deres direkte leverandører og tjenesteudbydere. Disse enheder kunne overveje risici hidrørende fra leverandører og tjenesteudbydere i andre led.

I overensstemmelse hermed bør procedurer efter det foreslåede nr. 4, tage højde for sikkerhedsrelaterede aspekter vedrørende forholdet mellem enheden og dens direkte leverandører og tjenesteudbydere relateret til enhedens net- og informationssystemer. Enheder skal i den forbindelse bl.a. udarbejde procedurer for aftaleindgåelse med direkte leverandører og tjenesteudbydere af produkter og tjenester, der kan påvirke sikkerheden i enhedens net-og informationssystemer.

Det foreslås i *nr. 5,* at foranstaltninger skal omfatte eller tage højde for sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer, herunder håndtering og offentliggørelse af sårbarheder.

Dette indebærer, at enheder skal udarbejde procedurer for sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af enhedens net- og informationssystemer, med udgangspunkt i politikken for informationssystemsikkerhed. Enheder skal endvidere udarbejde procedurer for håndtering af sårbarheder, der kan have indvirkning på enhedens net- og informationssystemer.

Det foreslås med *nr. 6,* at foranstaltninger skal omfatte eller tage højde for politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici.

Dette indebærer, at enheder skal udarbejde en politik og procedurer med henblik på at vurdere effektiviteten af de implementerede foranstaltninger samt for vurdering af behov for tekniske tests for potentielle sårbarheder, herunder f.eks. i form af sårbarheds-scanninger eller penetrationstests.

Det foreslås i *nr. 7,* at foranstaltninger skal omfatte eller tage højde for grundlæggende cyberhygiejnepraksisser og cybersikkerhedsuddannelse.

Dette indebærer bl.a., at enheder skal implementere relevante grundlæggende cyberhygiejnepraksisser med udgangspunkt i deres politik for informationssikkerhed, herunder f.eks. gennem brug af passwords og sikker brug af e-mails. Endvidere skal enheder udarbejde en politik for uddannelse af relevante medarbejdere for at sikre, at medarbejderne har relevant viden og færdigheder om informationssikkerhed.

Det foreslås med *nr. 8,* at foranstaltninger skal omfatte eller tage højde for politikker og procedurer vedrørende brug af kryptografi og, hvor det er relevant, kryptering.

Dette indebærer bl.a., at enheder skal udarbejde en politik og procedurer for brug af kryptografi og, hvor det er relevant, kryptering for at beskytte deres net- og informationssystemer. Politikken og procedurerne skal være passende i forhold til det aktuelle teknologiske stade.

Det foreslås i *nr. 9,* at foranstaltninger skal omfatte eller tage højde for personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver.

Dette indebærer bl.a., at teleudbyderne skal implementere foranstaltninger til personalesikkerhed, der skal sikre, at den enkelte medarbejder forstår, udviser og forpligter sig til at leve op til deres ansvar for informationssikkerhed.

Enheder skal derudover udarbejde en politik for adgangskontrol for at beskytte mod uautoriseret adgang til enhedens net- og informationssystemer. Politikken skal som minimum identificere og vurdere risici i forhold til logisk og fysisk adgangskontrol og indeholde procedurer for styring af adgangsrettigheder.

Enheder skal fastlægge hvordan den forvalter aktiver, der vil kunne påvirke sikkerheden i enhedens omfattede net- og informationssystemer.

Det foreslås med *nr. 10,* at foranstaltninger skal omfatte eller tage højde for brug af løsninger med multifaktorautentificering eller kontinuerlig autentificering, sikret tale-, video- og tekstkommunikation og sikrede nødkommunikationssystemer internt hos enheden, hvor det er relevant.

Dette indebærer bl.a., at enheder skal anvende multifaktorautentifikation eller kontinuerlig autentifikation ved adgang til net- og informationssystemer i overensstemmelse med enhedens politik for adgangskontrol. Enheder skal endvidere anvende sikret tale-, video- og tekstkommunikation i over-

ensstemmelse med politikken for brug af kryptografi og kryptering.

Det følger af det foreslåede *stk. 2,* at væsentlige eller vigtige teleudbyder, der ikke overholder ét eller flere af de krav, der er nævnt i stk. 1, eller regler om krav til foranstaltninger fastsat i medfør af stk. 3, uden unødigt ophold skal træffe alle nødvendige, passende og forholdsmæssige korrigerende foranstaltninger.

Den foreslåede bestemmelse vil gennemføre NIS 2-direktivets artikel 21, stk. 4. Efter NIS 2-direktivets artikel 21, stk. 4, skal medlemsstaterne sikre, at en enhed, der finder, at den ikke overholder foranstaltningerne i artikel 21, stk. 2, uden unødigt ophold træffer alle nødvendige, passende og forholdsmæssige korrigerende foranstaltninger.

Den foreslåede bestemmelse svarer indholdsmæssigt til NIS 2-direktivets artikel 21, stk. 4, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Den foreslåede bestemmelse i stk. 2, understreger, at enheder skal handle på eventuelle konstateringer af mangler i overholdelsen af de krav til foranstaltninger, der følger af det foreslåede stk. 1, og regler om krav til foranstaltninger udstedt i medfør af det foreslåede stk. 3. Dette skal ses i sammenhæng med den foreslåede § 6 om ledelsens ansvar.

Det følger af det foreslåede *stk. 3*, *1, pkt.,* at ministeren for samfundssikkerhed og beredskab fastsætter regler om krav til foranstaltninger efter stk. 1, og om yderligere foranstaltninger og krav hertil for teleudbydere omfattet af denne lov.

Den foreslåede bestemmelse indebærer, at ministeren for samfundssikkerhed og beredskab kan fastsættes nærmere regler om krav til de foranstaltninger til styring af sikkerhedsrisici, som væsentlige og vigtige teleudbydere skal træffe. Reglerne vil kunne stille mere konkretiserede krav til de foranstaltninger, som teleudbyderne skal træffe i medfør af den foreslåede bestemmelse i stk. 1, herunder fastsætte krav om yderligere foranstaltninger for telesektoren.

Dette omfatter bl.a. krav om foranstaltninger for i videst muligt omfang at sikre elektronisk kommunikation i beredskabssituationer og i andre ekstraordinære situationer. Bestemmelsen viderefører således § 5, stk. 1, i lov om sikkerhed i net og tjenester, og skal fortolkes i overensstemmelse hermed.

Bemyndigelsesbestemmelsen giver ministeren for samfundssikkerhed og beredskab mulighed for at fastsætte nærmere krav om foranstaltninger for samtlige teleudbydere, der er omfattet af lovens anvendelsesområde.

Det bemærkes i den forbindelse, at det følger af NIS 2-direktivets artikel 21, stk. 5, 2. led, at Europa-Kommissionen kan vedtage gennemførelsesretsakter, der fastsætter de tekniske og metodologiske, samt om nødvendigt sektorspecifikke, krav til de i direktivets artikel 21, stk. 2, omhandlede foranstaltninger. Det vides endnu ikke, om Europa-Kommissionen vil vælge at vedtage gennemførelsesretsakter i medfør af artikel 21, stk. 5, 2. led, samt i givet fald indholdet heraf.

Det vil til enhver tid skulle sikres, at bekendtgørelser i medfør af det foreslåede stk. 3, harmonerer med eventuelle gennemførelsesretsakter fra Europa-Kommissionen. Såfremt der måtte være udstedt bekendtgørelser på et tidspunkt, hvor Europa-Kommissionen vedtager gennemførelsesretsakter, vil disse bekendtgørelser i relevant omfang skulle tilpasses eller efter omstændighederne ophæves.

Det følger af det foreslåede *stk. 3, 2. pkt.,* at ministeren i den forbindelse kan fastsætte regler om, at væsentlige og vigtige teleudbydere skal anvende særlige IKT-produkter, -tjenester og -processer, som er certificeret i henhold til en europæisk cybersikkerhedscertificeringsordning for at påvise overensstemmelse med bestemte krav efter stk. 1, eller regler om krav til foranstaltninger fastsat i medfør af 1. pkt.

Bestemmelsen vil gennemføre artikel 24, stk. 1, i NIS 2-direktivet. Det følger af artikel 24, stk. 1, at for at påvise overensstemmelse med bestemte krav i direktivets artikel 21 (foranstaltninger til styring af cybersikkerhedsrisici), kan medlemsstaterne kræve, at væsentlige og vigtige enheder bruger særlige IKT-produkter, -tjenester og -processer, der er udviklet af den væsentlige eller vigtige enhed, eller indkøbt fra tredjeparter, og som er certificeret i henhold til europæiske cybersikkerhedscertificeringsordninger, der er vedtaget i henhold til artikel 49 i Europa-Parlamentets og Rådets forordning (EU) 2019/881 af 17. april 2019 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed), om cybersikkerhedscertificering af informations- og kommunikationsteknologi og om ophævelse af forordning (EU) nr. 526/2013 (forordningen om cybersikkerhed). Endvidere skal medlemsstaterne tilskynde væsentlige og vigtige enheder til at anvende kvalificerede tillidstjenester.

Artikel 49 i nævnte forordning fastsætter nærmere regler om udarbejdelse, vedtagelse og revision af en europæisk cybersikkerhedscertificeringsordning.

Den foreslåede bestemmelse svarer indholdsmæssigt til NIS 2-direktivets artikel 24, stk. 1, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger. De nærmere regler, der kan fastsættes i medfør af bestemmelsen, vil således skulle udarbejdes inden for denne ramme. Det indebærer bl.a., at reglerne vil skulle være i overensstemmelse med regeringens principper om minimumsimplementering.

Det er Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at bestemmelsen i NIS 2-direktivets artikel 24, stk. 1, hvorefter IKT-produkter, -tjenester og -processer skal være udviklet af enhederne eller »indkøbt fra tredjeparter«, ikke er til hinder for, at der kan fastsættes regler om, at enhederne skal bruge IKT-produkter, -tjenester og -processer, som stilles gratis til rådighed af tredjeparter.

Bestemmelsen skal i øvrigt ses i lyset af, at Europa-Kommissionen efter artikel 24, stk. 2, tillægges beføjelser til at

vedtage delegerede retsakter for at supplere direktivet ved at præcisere, hvilke kategorier af væsentlige og vigtige enheder, der skal anvende visse certificerede IKT-produkter, -tjenester og -processer eller indhente en attest i henhold til en europæisk cybersikkerhedscertificeringsordning. De delegerede retsakter vedtages, når der er identificeret utilstrækkelige cybersikkerhedsniveauer. I givet fald forudsættes det, at eventuelle allerede udstedte bekendtgørelser i relevant omfang tilpasses eller ophæves.

Til § 6

Det foreslås i *stk. 1,* at de foranstaltninger, som en væsentlig eller en vigtig teleudbyder træffer på baggrund af forpligtelserne i § 5, stk. 1 og 2, samt regler fastsat i medfør af § 5, stk. 3, skal være godkendt af teleudbyderens ledelsesorgan, samt at ledelsesorganet fører tilsyn med foranstaltningernes gennemførelse.

Den foreslåede bestemmelse i stk. 1, vil delvist gennemføre NIS 2-direktivets artikel 20, stk. 1. Det følger af NIS 2-direktivets artikel 20, stk. 1, at medlemsstaterne skal sikre, at de væsentlige og vigtige enheders ledelsesorganer godkender de foranstaltninger til styring af cybersikkerhedsrisici, som disse enheder har truffet med henblik på at overholde artikel 21, fører tilsyn med deres gennemførelse og kan gøres ansvarlige for enhedernes overtrædelser af forpligtelserne i den nævnte artikel. Dette berører dog ikke national ret for så vidt angår de ansvarsregler, der gælder for offentlige institutioner, samt ansvaret for embedsmænd og personer valgt eller udnævnt til offentlige hverv.

Den foreslåede bestemmelse i stk. 1 fastslår, at overholdelsen af forpligtelserne i den foreslåede § 5, stk. 1-3, er et ledelsesmæssigt ansvar.

Der findes i dansk ret ikke en entydig definition af et ledelsesorgan, idet visse virksomhedstyper ikke er omfattet af materielle regler om ledelsens organisering, hvorfor disse har en vis frihed til at organisere sig, efter egen vilje.

Lov om aktie- og anpartsselskaber, jf. lovbekendtgørelse nr. 1168 af 1. september 2023 (selskabsloven) definerer i § 5, nr. 4 dog bl.a. 'det centrale ledelsesorgan' som a) bestyrelsen i selskaber, der har en direktion og en bestyrelse, b) direktionen i selskaber, der alene har en direktion og c) direktionen i selskaber, der både har en direktion og et tilsynsråd. Selskabsloven finder dog alene anvendelse for aktie- og anpartsselskaber, jf. lovens § 1, stk. 1.

Lov om visse erhvervsdrivende virksomheder, jf. lovbekendtgørelse nr. 249 af 1. februar 2021 (LEV-loven), definerer i lovens § 4 a, nr. 2 en ledelse, som 'medlemmer af bestyrelse, direktion eller et tilsvarende ledelsesorgan'.

LEV-loven finder anvendelse for enkeltmandsvirksomheder, interessentskaber, kommanditselskaber, andelsselskaber (andelsforeninger) samt andre selskaber og foreninger med begrænset ansvar, som ikke er omfattet af selskabsloven, lov om erhvervsdrivende fonde eller §§ 133-154 i lov om forvaltere af alternative investeringsfonde m.v., jf. LEV-lovens § 1, stk. 2.

Det er på denne baggrund Ministeriet for Samfundssikkerhed og Beredskabs vurdering, at begrebet 'ledelsesorgan' i NIS 2-direktivet skal forstås i overensstemmelse med definitionerne af henholdsvis det centrale ledelsesorgan i selskabslovens § 5, nr. 4, og ledelsen i LEV-lovens § 4 a, nr. 2, afhængigt af enhedens selskabsform.

Det følger af det foreslåede *stk. 2,* at medlemmerne af ledelsesorganet i væsentlige eller vigtige teleudbyder skal deltage i relevante kurser om styring af informationssikkerhedsrisici og tilskynde til, at tilsvarende kurser tilbydes til ansatte i den væsentlige eller vigtige teleudbyder.

Den foreslåede bestemmelse i stk. 2 vil gennemføre NIS 2-direktivets artikel 20, stk. 2.

Det fremgår af NIS 2-direktivets artikel 20, stk. 2, at medlemsstaterne skal sikre, at medlemmerne af væsentlige og vigtige enheders ledelsesorganer er forpligtet til at følge kurser, og skal tilskynde væsentlige og vigtige enheder til løbende at tilbyde tilsvarende kurser til deres ansatte, således at de opnår tilstrækkelige kundskaber og færdigheder til at kunne identificere risici og vurdere metoderne til styring af cybersikkerhedsrisici og deres indvirkning på de tjenester, der leveres af enheden.

Henset til, at formålet med nærværende lov er at implementere NIS 2-direktivet gennem en integration med den eksisterende regulering på området, herunder navnlig lov om sikkerhed i net og tjenester, vurderes det, at kravet bør omfatte relevante kurser om styring af informationssikkerhedsrisici, og ikke kun cybersikkerhedsrisici, som forudsat i NIS 2-direktivet.

Til § 7

Det foreslås med *stk. 1,* at væsentlige- og vigtige teleudbydere skal registrere sig hos Styrelsen for Samfundssikkerhed og i den forbindelse oplyse 1) teleudbyderens navn, 2) teleudbyderens adresse og ajourførte kontaktoplysninger, herunder e-mailadresser, IP-intervaller og telefonnumre og 3) en liste over de øvrige medlemsstater i Den Europæiske Union, hvor teleudbyderen leverer tjenester, der er omfattet af anvendelsesområdet i artikel 2 i NIS 2-direktivet.

Den foreslåede bestemmelse vil gennemføre artikel 27, stk. 2, NIS 2-direktivet. Artikel 27, stk. 2, fastsætter bl.a., at medlemsstaterne pålægger DNS-tjenesteudbydere, topdomænenavneadministratorer, enheder, der leverer domænenavneregistreringstjenester og udbydere af cloudcomputingtjenester, af datacentertjenester, af indholdsleveringsnetværk, af administrerede tjenester, af administrerede sikkerhedstjenester, af onlinemarkedspladser, af onlinesøgemaskiner og af platforme for sociale netværkstjenester at indgive nærmere oplistede oplysninger til de kompetente myndigheder.

Den foreslåede bestemmelse svarer indholdsmæssigt til NIS 2-direktivets artikel 27, stk. 2, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Det er Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at der vil være tale om en oplysningspligt, der er omfattet af lov om retssikkerhed ved forvaltningens anvendelse af tvangsindgreb og oplysningspligter. Dette indebærer, at retten til ikke at inkriminere sig selv, jf. kapitel 4 i nævnte lov, skal overholdes. Det bemærkes dog, at det af bemærkningerne til § 10 i lov om retssikkerhed ved forvaltningens anvendelse af tvangsindgreb og oplysningspligter fremgår, at »[b]estemmelsen [om forbud mod selvinkriminering] er ikke til hinder for, at den mistænkte kan pålægges at give (faktuelle) oplysninger, som er uden betydning for bedømmelsen af, hvorvidt den pågældende har begået en lovovertrædelse, der kan medføre straf. Bestemmelsen vil således ikke være til hinder for at anvende en oplysningspligt til at kræve oplysninger om navn, adresse mv., jf. herved også retsplejelovens § 750, hvorefter enhver på forlangende er forpligtet til over for politiet at opgive navn, adresse og fødselsdato.« Der henvises til Folketingstidende 2003-04, tillæg A, side 3097. Der vil med den foreslåede bestemmelse være tale om en registreringspligt, hvorved enheder skal afgive en række helt overordnede oplysninger om bl.a. navn, adresse og enhedstype. Det er derfor Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at kapitel 4 i lov om retssikkerhed ved forvaltningens anvendelse af tvangsindgreb og oplysningspligter alene vil være relevant i praksis i yderst sjældne tilfælde.

Det foreslås i *stk. 2*, væsentlige og vigtige teleudbydere, der omfattes af lovens anvendelsesområde, skal indgive oplysningerne efter stk. 1, senest to uger efter, at teleudbyderen omfattes af loven.

Bestemmelsen vil gennemføre dele af NIS 2-direktivets artikel 3, stk. 3, hvorefter medlemsstaterne senest den 17. april 2025 skal udarbejde en liste over væsentlige og vigtige enheder samt enheder, der leverer domænenavnsregistreringstjenester. Det bemærkes, at NIS 2-direktivet skulle være implementeret i dansk ret senest den 17. oktober 2024. Idet denne lov træder i kraft den 1. juli 2025, er det Ministeriet for Samfundssikkerhed og Beredskabs vurdering, at nærværende frist bør fastsættes til den 1. oktober 2025.

Den foreslåede bestemmelse svarer indholdsmæssigt til dele af NIS 2-direktivets artikel 3, stk. 3, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Den foreslåede pligt for enhederne til at registrere sig vil ikke have indflydelse på, at teleudbyderen også før en registrering vil være omfattet af lovens anvendelsesområde. De rettigheder og forpligtelser, der følger af loven, vil derfor gælde uafhængigt af, om en teleudbyder har ladet sig registrere.

Det bemærkes, at den foreslåede bestemmelse alene finder anvendelse for enheder, der efter lovens ikrafttræden bliver omfattet af lovens anvendelsesområde. Enheder, der ved lovens ikrafttræden er omfattet af lovens anvendelsesområde vil ifølge den foreslåede bestemmelse i § 32, stk. 3, skulle indgive de nævnte oplysninger senest den 1. oktober 2025.

Det foreslås i *stk. 3,* at tilfælde af ændring i de oplysninger, der er afgivet i medfør af stk. 1, skal den væsentlige eller vigtige teleudbyder give Styrelsen for Samfundssikkerhed underretning herom senest to uger efter datoen for ændringen.

Bestemmelsen vil gennemføre NIS 2-direktivets artikel 27, stk. 3, som fastsætter en forpligtelse for medlemsstaterne til at sikre, at de nævnte enheder straks og under alle omstændigheder senest tre måneder efter den dato, hvor ændringen trådte i kraft, underretter den kompetente myndighed om enhver ændring af de oplysninger, de har indsendt i henhold til artikel 27, stk. 2.

Den foreslåede bestemmelse svarer indholdsmæssigt til dele af NIS 2-direktivets artikel 27, stk. 3, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Det foreslås i *stk. 4,* at ministeren for samfundssikkerhed og beredskab kan fastsætte regler om hvilke yderligere oplysninger væsentlige og vigtige teleudbydere skal afgive ved registrering.

Bestemmelsen har til formål at give ministeren for samfundssikkerhed og beredskab mulighed for at fastsætte nærmere regler om, at væsentlige og vigtige teleudbydere skal afgive yderligere oplysninger ved registrering.

Det foreslås i *stk. 5*, *nr. 1,* at ministeren for samfundssikkerhed og beredskab kan fastsætte nærmere regler om oplysnings- og underretningspligter for væsentlige og vigtige teleudbydere, herunder regler om afgivelse af oplysninger om væsentlige dele af teleudbyderens net eller tjenester eller driften heraf.

Bestemmelsen viderefører § 4, nr. 1 i lov om sikkerhed i net og tjenester, og skal fortolkes i overensstemmelse hermed.

Den foreslåede oplysningspligt vil indebære, at teleudbydere efter anmodning skal afgive oplysninger om de dele af deres net eller tjenester – eller driften heraf – der anses som væsentlige. Det kan f.eks. være oplysninger om, hvilke leverandører som teleudbyderen anvender. Dermed sikres det, at Styrelsen for Samfundssikkerhed kan få det nødvendige overblik over de centrale dele af teleinfrastrukturen.

Det foreslås i *stk. 5*, *nr. 2,* at ministeren for samfundssikkerhed og beredskab kan fastsætte nærmere regler om oplysnings- og underretningspligter for væsentlige og vigtige teleudbydere, herunder regler om underretning ved påtænkt indgåelse af aftaler om leverancer, der vedrører væsentlige dele af udbyderens net eller tjenester eller driften heraf, herunder regler om, at teleudbyderen skal indsende et endeligt aftaleudkast til Styrelsen for Samfundssikkerhed umiddelbart forud for indgåelse af aftalen, og at aftalen først kan

indgås op til 25 arbejdsdage efter centerets modtagelse af dette udkast.

Bestemmelsen viderefører § 4, nr. 2 i lov om sikkerhed i net og tjenester, og skal fortolkes i overensstemmelse hermed.

Oplysningspligten efter den foreslåede stk. 5, nr. 2, foreslås – ligesom tilfældet er i dag – suppleret af en underretningspligt, som indebærer, at teleudbydere skal underrette Styrelsen for Samfundssikkerhed i forbindelse med påtænkte indgåelser af visse større aftaler om leverancer af hardware, firmware eller software samt driften heraf.

Det foreslås med *stk. 5, nr. 3,* at ministeren for samfundssikkerhed og beredskab kan fastsætte nærmere regler om oplysnings- og underretningspligter for væsentlige og vigtige teleudbydere, herunder regler om, at teleudbyderen skal indsende et endeligt aftaleudkast til Styrelsen for Samfundssikkerhed umiddelbart forud for indgåelse af aftale, og at aftalen først kan indgås op til 25 arbejdsdage efter styrelsens modtagelse af pågældende udkast.

Bestemmelsen viderefører § 4, nr. 2 i lov om sikkerhed i net og tjenester, og skal fortolkes i overensstemmelse hermed.

Formålet med ordningen er at give Styrelsen for Samfundssikkerhed mulighed for at rådgive teleudbyderen om særlige trusler mod informationssikkerheden samt om mulighederne for at imødegå de trusler, som det pågældende aftaleudkast vurderes at indebære. Det vurderes, at dette vil bidrage til, at teleudbyderne får bedre forudsætninger for at vurdere mulige risici ved den påtænkte aftale, således at teleudbyderne kan tage højde herfor inden aftaleindgåelsen.

Til § 8

I *stk. 1* foreslås det, at § 17 i lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS 2-loven) finder tilsvarende anvendelse for teleudbydere omfattet af denne lov.

Det fremgår af den foreslåede § 1, stk. 2, 2. pkt., i forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau, at lovens § 17 finder anvendelse for enheder, der er omfattet af telesektoren.

Den foreslåede bestemmelse § 17 i lov om forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau, fastsætter CSIRT'ens opgaver over for væsentlige og vigtige enheder.

Det foreslås i *stk. 2,* at teleudbyderen skal underrette Styrelsen for Samfundssikkerhed og CSIRT'en om enhver væsentlig hændelse efter proceduren i den foreslåede § 9.

Den foreslåede bestemmelse vil gennemføre artikel 23, stk. 1, i NIS 2-direktivet.

Det følger bl.a. af NIS 2-direktivets artikel 23, stk. 1, at hver medlemsstat sikrer, at væsentlige og vigtige enheder uden unødigt ophold underretter dens CSIRT eller i givet fald dens kompetente myndighed om enhver hændelse, der har en væsentlig indvirkning på leveringen af deres tjenester. Hver medlemsstat sikrer, at enhederne indberetter alle oplysninger, der gør det muligt for CSIRT'en eller den kompetente myndighed at fastslå eventuelle grænseoverskridende virkninger af hændelsen.

Den foreslåede bestemmelse svarer indholdsmæssigt til NIS 2-direktivets artikel 23, stk. 1, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Den foreslåede bestemmelse indebærer, at samtlige teleudbydere, der er omfattet af lovens anvendelsesområde, skal underrette både Styrelsen for Samfundssikkerhed og CSIRT'en i tilfælde af hændelser, der har en væsentlig indvirkning på levering af deres tjenester. Dermed sikres det, at både Styrelsen for Samfundssikkerhed og CSIRT'en hurtigt og effektivt vil kunne varetage sine myndighedsopgaver.

Det bemærkes, at væsentlige og vigtige teleudbydere i overensstemmelse med forvaltningslovens § 7 i fornødent omfang vil kunne få vejledning og bistand fra Styrelsen for Samfundssikkerhed.

I overensstemmelse med præambelbetragtning nr. 83 vil den foreslåede forpligtelse til at foretage underretning ved hændelser finde anvendelse på de væsentlige og vigtige teleudbydere, uanset om disse teleudbydere selv vedligeholder deres net- og informationssystemer eller outsourcer vedligeholdelsen deraf. Såfremt der måtte ske en hændelse i et net- og informationssystem, som eksempelvis er outsourcet, vil det derfor fortsat være den væsentlige eller vigtige teleudbyders ansvar, at der sker underretning i fornødent omfang.

Det er Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at der vil være tale om en oplysningspligt omfattet af lov om retssikkerhed ved forvaltningens anvendelse af tvangsindgreb og oplysningspligter. Dette indebærer bl.a., at kapitel 4 (om retten til ikke at inkriminere sig selv mv.) vil gælde i tilfælde, hvor der måtte være en konkret mistanke om, at en enhed har begået en overtrædelse af lovgivningen, der kan medføre straf. Der henvises i øvrigt til kapitel 4 i lov om retssikkerhed ved forvaltningens anvendelse af tvangsindgreb og oplysningspligter og bemærkningerne hertil. Der henvises til Folketingstidende 2003-04, tillæg A, side 3075-3078 og side 3096-3099.

Såfremt en væsentlig hændelse, der underrettes om i medfør af bestemmelsen, måtte have grænseoverskridende virkning, vil CSIRT'en i overensstemmelse med forudsætningen i NIS 2-direktivets artikel 23, stk. 6, via det centrale kontaktpunkt uden unødigt ophold skulle underrette de øvrige berørte medlemsstater og ENISA om den væsentlige hændelse, navnlig hvor den væsentlige hændelse berører to eller flere medlemsstater. Efter samme bestemmelse vil en sådan information omfatte den type af oplysninger, der er modtaget i overensstemmelse med artikel 23, stk. 4, og CSIRT'en vil i den forbindelse – i overensstemmelse med EU-retten eller

national ret – sikre enhedens sikkerhed og kommercielle interesser samt fortrolig behandling af de afgivne oplysninger.

Det følger af det foreslåede *stk. 3, nr. 1,* at en hændelse anses for at være væsentlig, hvis den har forårsaget eller er i stand til at forårsage alvorlige driftsforstyrrelser af net eller tjenester eller økonomiske tab for den berørte udbyder.

Den foreslåede bestemmelse vil gennemføre NIS 2-direktivets artikel 23, stk. 3.

Med alvorlige driftsforstyrrelser forstås en hændelse, som kompromitterer tjenesterne fortroligled, integritet, autenticitet og/eller tilgængelighed.

Med økonomiske tab forstås betydelige tab og/eller omkostninger som følge af hændelse. Tab eller udbredelse af intellektuel ejendom, der kan bringe enhedens fremtidige indtægt eller omsætning i fare, medregnes ligeledes som økonomisk tab.

Det fremgår af præambelbetragtning nr. 101, at direktivet bør omfatte underretning om hændelser, som ud fra en indledende vurdering foretaget af den berørte enhed kunne forårsage alvorlige driftsmæssige forstyrrelser af tjenesterne.

Det følger af det foreslåede *stk. 3, nr. 2,* at en hændelse anses for at være væsentlig, hvis den har påvirket eller er i stand til at påvirke andre fysiske eller juridiske personer ved at forårsage betydelig fysisk eller ikke-fysisk skade.

Den foreslåede bestemmelse svarer med en enkelt sproglig justering uden indholdsmæssig betydning til NIS 2-direktivets artikel 23, stk. 3, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Det fremgår af præambelbetragtning nr. 101, at direktivet bør omfatte underretning om hændelser, som ud fra en indledende vurdering foretaget af den berørte enhed kunne forårsage alvorlige driftsmæssige forstyrrelser af tjenesterne eller økonomiske tab for denne enhed eller forvolde betydelig materiel eller immateriel skade for andre fysiske eller juridiske personer. En sådan indledende vurdering bør bl.a. tage i betragtning de berørte net- og informationssystemer, navnlig deres betydning for leveringen af enhedens tjenester, alvoren og de tekniske karakteristika af en cybertrussel, eventuelle underliggende sårbarheder, der udnyttes, samt enhedens erfaring med tilsvarende hændelser. Indikatorer såsom graden af påvirkning af tjenestens funktionsdygtighed, varigheden af en hændelse eller antallet af berørte tjenestemodtagere vil kunne spille en vigtig rolle med hensyn til at fastslå, om den driftsmæssige forstyrrelse af tjenesten er alvorlig.

En hændelse anses altid for væsentlig, hvis den forårsager hel eller delvis ødelæggelse af kritiske tredje parts fysiske eller digitale aktiver. Ligeledes anses en hændelse altid for at være væsentlig, hvis den forårsager død, eller skader der kræver hospitalsindlæggelse eller behandling.

Det følger af det foreslåede *stk. 4,* at ministeren for samfundssikkerhed og beredskab kan fastsættes nærmere regler om, hvornår en hændelse kan anses for at være væsentlig og hvilke oplysninger, der skal gives i forbindelse med underretningen.

Henset til at kriterierne for, hvornår en hændelse anses for at være væsentlig efter det foreslåede stk. 3, har en kvalitativ og skønspræget karakter, vurderes det hensigtsmæssigt, at ministeren for samfundssikkerhed og beredskab kan fastsættes nærmere regler, som præciserer, hvornår en hændelse anses for at være væsentlig i telesektoren.

Til § 9

Det foreslås i *stk. 1*, at underretningen efter § 8, stk. 2, skal ske på følgende måde: 1) en tidlig varsling, som skal angive, om den væsentlige hændelse mistænkes at være forårsaget af ulovlige eller ondsindede handlinger eller kunne have en grænseoverskridende virkning, sendes uden unødigt ophold og senest inden for 24 timer efter, at teleudbyderen har fået kendskab til den væsentlige hændelse, 2) en hændelsesunderretning, som skal ajourføre oplysningerne fra den tidlige varsling, jf. nr. 1, og give en indledende vurdering af den væsentlige hændelse, herunder dens alvor og indvirkning samt kompromitteringsindikatorerne, hvor sådanne foreligger, sendes uden unødigt ophold og senest inden for 72 timer efter, at teleudbyderen har fået kendskab til den væsentlige hændelse, jf. dog stk. 2, 3) en foreløbig rapport med relevante statusopdateringer sendes til enten Styrelsen for Samfundssikkerhed eller CSIRT'en efter myndighedens anmodning herom, 4) en endelig rapport sendes til Styrelsen for Samfundssikkerhed og CSIRT'en senest en måned efter fremsendelsen af den hændelsesunderretning, der er omhandlet i nr. 2. Rapporten skal indeholde følgende: a) en detaljeret beskrivelse af hændelsen, herunder dens alvor og indvirkning, b) den type trussel eller grundlæggende årsag, der sandsynligvis har udløst hændelsen, c) anvendte og igangværende afbødende foranstaltninger og d) de eventuelle grænseoverskridende virkninger af hændelsen og 5) pågår hændelsens fortsat på tidspunktet for fremsendelsen af den endelige rapport, jf. nr. 4, skal den berørte teleudbyder indsende en statusrapport på det pågældende tidspunkt og en endelig rapport senest en måned efter, at hændelsen er håndteret.

Med den foreslåede bestemmelse fastlægges der en flertrinstilgang for underretninger om væsentlige hændelser.

Det bemærkes, at det er Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at der vil være tale om oplysningspligter omfattet af lov om retssikkerhed ved forvaltningens anvendelse af tvangsindgreb og oplysningspligter. Dette indebærer bl.a., at kapitel 4 (om retten til ikke at inkriminere sig selv mv.) vil gælde i tilfælde, hvor der måtte være en konkret mistanke om, at en enhed har begået en overtrædelse af lovgivningen, der kan medføre straf. Der henvises i øvrigt til kapitel 4 i lov om retssikkerhed ved forvaltningens anvendelse af tvangsindgreb og oplysningspligter og

bemærkningerne hertil. Der henvises til Folketingstidende 2003-04, tillæg A, side 3075-3078 og side 3096-3099.

I overensstemmelse med NIS 2-direktivets præambelbetragtning nr. 102 vil det skulle sikres, at forpligtelsen til at indgive den tidlige varsling eller den efterfølgende hændelsesunderretning ikke medfører, at den underrettende enhed skal bruge færre ressourcer på aktiviteter vedrørende håndtering af hændelsen. Enhedens ressourcer bør således prioriteres, så det forhindres, at forpligtelser vedrørende hændelsesrapportering enten omdirigerer ressourcer fra håndtering af væsentlige hændelser eller på anden måde kompromitterer enhedens indsats i denne henseende.

Det forudsættes på denne baggrund, at det sikres, at underretningen kan ske på en så ressourcebesparende måde som muligt, eksempelvis ved at anvende én fælles digital løsning.

Det følger af det forslåede *nr. 1*, at en tidlig varsling skal angive, om den væsentlige hændelse mistænkes at være forårsaget af ulovlige eller ondsindede handlinger eller kunne have en grænseoverskridende virkning, sendes uden unødigt ophold og senest inden for 24 timer efter, at enheden har fået kendskab til den væsentlige hændelse.

Den foreslåede bestemmelse indebærer, at væsentlige og vigtige teleudbydere indledningsvist vil være forpligtet til at indgive en tidlig varsling uden unødigt ophold og under alle omstændigheder inden for 24 timer efter, at de bliver opmærksomme på en væsentlig hændelse.

I overensstemmelse med NIS 2-direktivets præambelbetragtning nr. 102 vil den tidlige varsling alene skulle indeholde de oplysninger, der er nødvendige for at gøre CSIRT'en og den relevante kompetente myndighed opmærksom på den væsentlige hændelse og give enheden mulighed for om nødvendigt at anmode om assistance. En sådan tidlig varsling bør endvidere, hvis det er relevant, angive om den væsentlige hændelse mistænkes for at være forårsaget af ulovlige eller ondsindede handlinger, og om den sandsynligvis vil have grænseoverskridende virkninger.

Det følger af det foreslåede *nr. 2,* at en hændelsesunderretning skal ajourføre oplysningerne fra den tidlige varsling, jf. nr. 1, og give en indledende vurdering af den væsentlige hændelse, herunder dens alvor og indvirkning samt kompromitteringsindikatorerne, hvor sådanne foreligger, sendes uden unødigt ophold og senest inden for 72 timer efter, at enheden har fået kendskab til den væsentlige hændelse.

Den tidlige varsling efter det foreslåede nr. 1 vil således skulle efterfølges af en hændelsesunderretning, som bl.a. skal ajourføre oplysningerne fra den tidlige varsling. Denne hændelsesunderretning skal sendes uden unødigt ophold og senest inden for 72 timer efter, at en enhed har fået kendskab til den væsentlige hændelse.

Det følger af den foreslåede *nr. 3,* at en foreløbig rapport med relevante statusoplysninger sendes efter anmodning fra CSIRT'en.

Den foreslåede bestemmelse indebærer, at CSIRT'en på baggrund af hændelsesunderretningen kan anmode om den underrettende enhed om en foreløbig rapport med relevante statusopdateringer. Indholdet i den foreløbige rapport vil afhænge af hændelsens nærmere omstændigheder.

Den berørte teleudbyder vil skulle sende en endelig rapport senest en måned efter forelæggelsen af hændelsesunderretningen efter den foreslåede § 9, stk. 1, nr. 2. I tilfælde af at hændelsen fortsat er igangværende på tidspunktet for indgivelsen af den endelige rapport, skal den berørte enhed forelægge en statusrapport for CSIRT'en og den relevante kompetente myndighed. Den endelige rapport vil i så fald skulle indgives senest en måned efter, at enheden har håndteret den væsentlige hændelse.

Det følger af det foreslåede *nr. 4,* at en endelig rapport sendes senest én måned efter fremsendelsen af den hændelsesunderretning, der er omhandlet i nr. 2.

Den foreslåede bestemmelse vil medføre, at en endelig rapport skal sendes til CSIRT'en senest én måned efter fremsendelsen af hændelsesunderretningen efter det foreslåede nr. 2.

Rapporten vil skulle indeholde en a) detaljeret beskrivelse af hændelsen, herunder dens alvor og indvirkning, b) den type trussel eller grundlæggende årsag, der sandsynligvis har udløst hændelsen, c) anvendte og igangværende afbødende foranstaltninger, og d) oplysninger om de eventuelle grænseoverskridende virkninger af hændelsen.

Det følger af det foreslåede *nr. 5,* at pågår hændelsen fortsat på tidspunktet for fremsendelsen af den endelige rapport, skal den underrettende teleudbyder indsende en statusrapport på det pågældende tidspunkt og en endelig rapport senest én måned efter, at hændelsen er håndteret.

Den foreslåede bestemmelse vil indebære, at i tilfælde hvor en hændelse fortsat pågår på tidspunktet, hvor den endelige rapport efter det foreslåede nr. 4 skal foreligge, vil den underrettende enhed være forpligtet til at indsende en statusrapport på tidspunktet. Enheden vil endvidere være forpligtet til at sende en endelig rapport senest én måned efter, at hændelsen er håndteret.

Det følger af det foreslåede *stk. 2, 1. pkt.,* at Styrelsen for Samfundssikkerhed og CSIRT'en sikrer, at den underrettende teleudbyder uden unødigt ophold og senest inden for 24 timer efter modtagelsen af den tidlige varsling, gives et svar, herunder indledende tilbagemeldinger om den væsentlige hændelse.

Den foreslåede bestemmelse vil gennemføre NIS 2-direktivets artikel 23, stk. 5, som bl.a. fastsætter, at CSIRT'en eller den relevante kompetente myndighed uden unødigt ophold, og hvor det er muligt, inden for 24 timer efter

modtagelsen af den i stk. 4, litra a, omhandlede tidlige varsling giver den underrettende enhed et svar, herunder indledende tilbagemeldinger om den væsentlige hændelse og, efter anmodning fra enheden, vejledning eller operativ rådgivning om gennemførelsen af mulige afbødende foranstaltninger. CSIRT'en yder supplerende teknisk bistand, hvis den berørte teleudbyder anmoder herom. Hvor den væsentlige hændelse mistænkes for at være af strafferetlig karakter, giver CSIRT'en eller Styrelsen for Samfundssikkerhed også vejledning om underretning om den væsentlige hændelse til retshåndhævende myndigheder.

Den foreslåede bestemmelse svarer med enkelte sproglige tilpasninger uden indholdsmæssig betydning til NIS 2-direktivets artikel 23, stk. 5, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Den foreslåede bestemmelse indeholder en forpligtelse for CSIRT'en til at sikre, at der hurtigt gives svar på de tidlige varslinger, som den modtager fra teleudbydere, og i denne forbindelse give indledende tilbagemeldinger om den væsentlige hændelse.

Svar og tilbagemeldinger vil kunne gives af CSIRT'en selv eller Styrelsen for Samfundssikkerhed. Svar og tilbagemeldinger vil bl.a. kunne bestå i, at der gives vejledning om mulige afværgeforanstaltninger, om anden relevant viden, som CSIRT'en eller Styrelsen for Samfundssikkerhed er i besiddelse af, eller om anmeldelse til politiet, såfremt den væsentlige hændelse mistænkes for at udgøre en strafbar handling. Derimod er det ikke hensigten, at CSIRT'en eller Styrelsen for Samfundssikkerhed, som afgiver svaret, skal tilvejebringe oplysninger fra tredjemand.

Det følger af det foreslåede *stk. 2, 2. pkt.,* at efter anmodning fra teleudbyderen skal CSIRT'en desuden yde vejledning, operativ rådgivning om gennemførelsen af mulige afbødende foranstaltninger og supplerende teknisk bistand.

Den foreslåede bestemmelse svarer med enkelte sproglige tilpasninger uden indholdsmæssig betydning til NIS 2-direktivets artikel 23, stk. 5, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Det bemærkes i den forbindelse, at hvis en hændelse efterforskes som et strafbart forhold, vil der skulle tages højde for, at de opfølgende oplysninger ikke må vanskeliggøre eller forhindre efterforskningen.

Til § 10

Det følger af den foreslåede bestemmelse i *stk. 1*, at teleudbydere kan underrette Styrelsen for Samfundssikkerhed og CSIRT'en om hændelser, nærvedhændelser og cybertrusler.

Bestemmelsen vil gennemføre artikel 30, stk. 1, i NIS 2-direktivet, som fastsætter en forpligtelse for medlemsstaterne til at sikre, at der ud over underretningsforpligtelsen i artikel 23 kan indgives underretninger til CSIRT'en eller i givet fald de kompetente myndigheder på frivillig basis af: a) væsentlige og vigtige enheder for så vidt angår hændelser, cybertrusler og nærvedhændelser og 2) enheder, udover dem der er omhandlet i litra a), uanset om de er omfattet af dette direktivs anvendelsesområde, for så vidt angår væsentlige hændelser, cybertrusler og nærvedhændelser.

Den foreslåede bestemmelse svarer indholdsmæssigt til bestemmelsen i NIS 2-direktivets artikel 30, stk. 1, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Den foreslåede bestemmelse indebærer, at alle teleudbydere kan underrette Styrelsen for Samfundssikkerhed og CSIRT'en om hændelser, nærvedhændelser og cybertrusler.

Det følger af den foreslåede *stk. 2,* at Styrelsen for Samfundssikkerhed og CSIRT'en behandler underretninger efter stk. 1 på samme måde som underretninger modtaget i medfør af § 8. CSIRT'en kan prioritere håndteringen af underretninger, der er modtaget i medfør af § 8 frem for underretninger efter det foreslåede stk. 1.

Bestemmelsen vil gennemføre artikel 30, stk. 2, i NIS 2-direktivet. Det følger af NIS 2-direktivets artikel 30, stk. 2, at medlemsstaterne behandler de i artiklens stk. 1 omhandlede underretninger i overensstemmelse med proceduren, der er fastsat i artikel 23. Medlemsstaterne kan prioritere behandling af obligatoriske underretninger frem for frivillige underretninger. Hvor det er nødvendigt, giver CSIRT'erne og i givet fald de kompetente myndigheder det centrale kontaktpunkt de oplysninger om underretninger, de har modtaget i medfør af denne artikel, samtidig med at de sikrer fortroligheden og passende beskyttelse af de oplysninger, der er afgivet af den underrettende enhed. Uden at det berører forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger, må frivillig rapportering ikke medføre, at den underrettende enhed pålægges nogen yderligere forpligtelser, som den ikke ville være omfattet af, hvis den ikke havde foretaget underretningen.

Den foreslåede bestemmelse svarer med sproglige tilpasninger uden indholdsmæssig betydning til bestemmelsen i NIS 2-direktivets artikel 30, stk. 2, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Den foreslåede bestemmelse indebærer, at CSIRT'en og Styrelsen for Samfundssikkerhed vil skulle behandle frivillige underretninger, der er indgivet i medfør af den foreslåede bestemmelse i § 10, stk. 1, efter procedurebestemmelsen i den foreslåede § 9. De forpligtelser for myndigheder, der er angivet i § 9 og bemærkningerne hertil, vil således også gælde for underretninger, der indgives i medfør af den foreslåede bestemmelse i § 10, stk. 1.

Det bemærkes, at den foreslåede bestemmelse ikke indebærer, at teleudbyderen er forpligtet til at følge proceduren efter den foreslåede bestemmelse i § 9, når der indgives underretning efter den foreslåede § 10, stk. 1.

Den foreslåede bestemmelse indebærer desuden, at

CSIRT'en kan prioritere at håndtere de underretninger, der er modtaget i medfør af § 8, før CSIRT'en og Styrelsen for Samfundssikkerhed behandler de underretninger, der er modtaget i medfør af § 10, stk. 1.

I *stk. 3* foreslås det, at teleudbydere, uanset om de er omfattet af lovens anvendelsesområde, kan give frivillig underretning til Styrelsen for Samfundssikkerhed og CSIRT'en efter stk. 1.

Efter den foreslåede bestemmelse i § 10, stk. 3, kan alle teleudbydere underrette CSIRT'en om hændelser, der negativt påvirker eller vurderes at kunne påvirke tilgængeligheden, integriteten eller fortroligheden af data, informationssystemer, digitale netværk eller digitale servicer.

Den foreslåede bestemmelse indebærer, at enheder, der ellers ikke ville være omfattet af lovens anvendelsesområde, har mulighed for at give frivillig underretning til CSIRT'en om hændelser.

Den foreslåede bestemmelse vil delvist gennemføre NIS 2-direktivets artikel 29, stk. 2.

Til § 11

Det følger af det foreslåede *stk. 1,* at er det sandsynligt, at en væsentlige hændelse, jf. § 8, stk. 3, vil påvirke teleudbyderens levering af deres tjenester til modtagerne heraf negativt, underretter teleudbyderen i relevant omfang modtagerne herom uden unødigt ophold.

Bestemmelsen vil gennemføre artikel 23, stk. 1, 2. pkt., i NIS 2-direktivet, som fastsætter en forpligtelse for medlemsstaterne til at sikre, at væsentlige og vigtige enheder i relevant omfang underretter modtagerne af deres tjenester om væsentlige hændelser, der sandsynligvis vil påvirke leveringen af disse tjenester negativt.

Den foreslåede bestemmelse svarer indholdsmæssigt til bestemmelsen i NIS 2-direktivets artikel 23, stk. 1, 2. pkt., og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger, dog med den ændring, at kravet om underretning ikke alene gælder for væsentlige og vigtige teleudbydere, men for samtlige teleudbydere, der er omfattet af nærværende lov.

Dette skal navnlig ses i lyset af, at den gældende lov om sikkerhed i net og tjenester finder anvendelse for samtlige teleudbydere. Henset til det aktuelle trusselsbillede, vurderer Ministeriet for Samfundssikkerhed og Beredskab, at det nuværende sikkerhedsniveau bør opretholdes.

Den foreslåede bestemmelse indebærer en forpligtelse for teleudbydere til at underrette modtagerne af deres tjenester om en væsentlig hændelse. Underretning af modtagerne vil alene skulle ske i relevant omfang. Det indebærer, at teleudbyderne vil kunne undlade at foretage underretning af modtagerne ud fra en konkret vurdering af, at underretningen ikke vil være i modtagernes interesse.

Om en hændelse er at anse for væsentlig vurderes ud fra den foreslåede bestemmelse i § 8, stk. 2, og ud fra regler, der måtte være udstedt i en given sektor i medfør af § 8, stk. 4.

Der stilles ingen formkrav til underretningen, og de pågældende teleudbydere vil derfor have metodefrihed i forhold til, hvordan underretningen af modtagerne vil skulle ske, idet det dog forudsættes, at underretningen skal være umiddelbart tilgængelig for de relevante modtagere og kommunikeres på et letforståeligt sprog.

Det følger af det foreslåede *stk. 2, 1. pkt.,* at teleudbydere oplyser uden unødigt ophold modtagerne af deres tjenester, som potentielt er berørt af en væsentlig cybertrussel, om eventuelle foranstaltninger eller modforholdsregler, som modtagerne kan træffe som reaktion på den pågældende trussel. Hvor det er relevant, skal udbyderne også informere de pågældende modtagere om selve den væsentlige cybertrussel.

Bestemmelsen vil gennemføre NIS 2-direktivets artikel 23, stk. 2, der fastsætter en forpligtelse for medlemsstaterne til at sikre, at væsentlige og vigtige enheder i givet fald uden unødigt ophold meddeler modtagerne af deres tjenester, som potentielt kan være berørt af en væsentlig cybertrussel, eventuelle foranstaltninger eller modforholdsregler, som disse modtagere kan træffe som reaktion på den pågældende trussel. Hvor det er relevant, skal enhederne også informere de pågældende modtagere om selve den væsentlige trussel.

Den foreslåede bestemmelse svarer indholdsmæssigt til bestemmelsen i NIS 2-direktivets artikel 23, stk. 2, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger, dog med den ændring, at kravet om underretning ikke alene gælder for væsentlige og vigtige teleudbydere, men for samtlige teleudbydere, der er omfattet af nærværende lov.

Dette skal navnlig ses i lyset af, at den gældende lov om sikkerhed i net og informationer finder anvendelse for samtlige teleudbydere. Henset til det aktuelle trusselsbillede, vurderer Ministeriet for Samfundssikkerhed og Beredskab, at det nuværende sikkerhedsniveau bør opretholdes.

Den foreslåede bestemmelse indebærer i overensstemmelse med NIS 2-direktivets præambelbetragtning nr. 103, bl.a. at væsentlige og vigtige enheder uden unødigt ophold vil skulle underrette modtagerne af deres tjenester om enhver foranstaltning eller modforholdsregel, som modtagerne kan træffe for at afbøde risici fra en væsentlig hændelse.

Det foreslås med *stk. 2, 2. pkt.,* at hvor det er relevant, skal udbyderne også informere de pågældende modtagere om selve den væsentlige cybertrussel.

Bestemmelsen vil gennemføre NIS 2-direktivets artikel 23, stk. 2.

Den foreslåede bestemmelse indebærer i overensstemmelse med NIS 2-direktivets præambelbetragtning nr. 103, at te-

leudbydere, hvor det er hensigtsmæssigt, vil skulle informere deres tjenestemodtagere om selve den væsentlige cybertrussel. Kravet om at informere modtagerne bør opfyldes efter bedste evne, men vil ikke fritage teleudbyderne for forpligtelsen til at træffe passende og øjeblikkelige foranstaltninger til at forebygge eller afhjælpe enhver hændelse og genoprette tjenestens normale sikkerhedsniveau.

I overensstemmelse med præambelbetragtning nr. 103 indebærer bestemmelsen endvidere, at oplysninger om væsentlige cybertrusler skal stilles gratis til rådighed for modtagerne i et let forståeligt sprog

Der stilles i øvrigt ingen formkrav til oplysningen, og de pågældende teleudbyderne vil derfor have metodefrihed i forhold til, hvordan underretningen af modtagerne vil skulle ske.

Til § 12

Det foreslås i *stk. 1,* at Styrelsen for Samfundssikkerhed efter høring af en teleudbyder, der er ramt af en væsentlig hændelse, jf. § 8, stk. 3, kan informere offentligheden om den væsentlige hændelse, hvis offentliggørelsen er nødvendig for at forebygge eller håndtere hændelsen, eller hvis offentliggørelse af hændelsen på anden vis er i offentlighedens interesse.

Bestemmelsen vil delvist gennemføre artikel 23, stk. 7, i NIS 2-direktivet.

Det fremgår af NIS 2-direktivets artikel 23, stk. 7, at hvor offentlighedens kendskab er nødvendig for at forebygge en væsentlig hændelse eller for at håndtere en igangværende hændelse, eller hvor offentliggørelse af den væsentlige hændelse på anden vis er i offentlighedens interesse, kan en medlemsstats CSIRT eller i givet fald dens kompetente myndighed, og hvor det er relevant CSIRT'erne eller de kompetente myndigheder i andre berørte medlemsstater efter høring af den berørte enhed informere offentligheden om den væsentlige hændelse eller kræve, at enheden gør det.

Den foreslåede bestemmelse svarer – med visse sproglige tilpasninger uden indholdsmæssig betydning – til NIS 2-direktivets artikel 23, stk. 7, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger, dog således, at bestemmelsen ikke alene gælder for væsentlige og vigtige teleudbydere, men for samtlige teleudbydere, der er omfattet af nærværende lov.

Dette skal navnlig ses i lyset af, at den gældende lov om sikkerhed i net og informationer finder anvendelse for samtlige teleudbydere. Henset til det aktuelle trusselsbillede, vurderer Ministeriet for Samfundssikkerhed og Beredskab, at det nuværende sikkerhedsniveau bør opretholdes.

Den foreslåede bestemmelse indebærer, at Styrelsen for Samfundssikkerhed kan informere offentligheden om en væsentlig hændelse, hvis offentliggørelsen er nødvendig for at forebygge eller håndtere hændelsen, eller hvor offentliggørelsen af hændelsen på anden vis er i offentlighedens interesse.

Styrelsen for Samfundssikkerhed vil i medfør af bestemmelsen skulle høre den berørte teleudbyder, før der sker offentliggørelse af hændelsen.

Formålet med høringen vil være at sikre, at Styrelsen for Samfundssikkerhed kan træffe afgørelse om offentliggørelse på et oplyst grundlag, herunder foretage en afvejning af hensynet til den konkrete enhed over for hensynet til orientering af offentligheden.

Det vil være op til Styrelsen for Samfundssikkerhed at tage stilling til formen for orienteringen. Orientering af offentligheden kan således ske på den måde, som Styrelsen for Samfundssikkerhed finder bedst egnet under hensyn til den berørte enhed, hændelsens karakter, den geografiske udstrækning, den forventede betydning for bestemte dele af offentligheden mv.

Det vil i den forbindelse skulle sikres, at offentligheden informeres på en ansvarlig måde, som ikke kompromitterer fortrolige oplysninger. Det bemærkes, at den kompetente myndighed vil skulle sikre, at de hensyn til fortrolighed, der fremgår af i forvaltningslovens § 27 om offentligt ansattes tavshedspligt, iagttages. Dette omfatter bl.a. hensynet til enkeltpersoners private forhold, forretningshemmeligheder samt hensynet til forebyggelse, efterforskning og forfølgning af lovovertrædelser.

Det foreslås, at det som udgangspunkt er Styrelsen for Samfundssikkerhed, og ikke CSIRT'en, der foretager offentliggørelsen af en væsentlig hændelse, jf. dog det foreslåede stk. 3, idet Styrelsen for Samfundssikkerhed vil være nærmest til at foretage afvejningen af teleudbyderens eventuelle interesse i, at der ikke sker offentliggørelse, over for hensynet til offentligheden.

Det følger af den foreslåede bestemmelse i *stk. 2*, at Styrelsen for Samfundssikkerhed i de situationer, der er nævnt i stk. 1, kan træffe afgørelse om, at den relevante teleudbyder informerer offentligheden om en væsentlig hændelse og bestemme, hvordan denne information skal gives.

Bestemmelsen vil delvist gennemføre NIS 2-direktivets artikel 23, stk. 7.

Det fremgår af NIS 2-direktivets artikel 23, stk. 7, at hvor offentlighedens kendskab er nødvendig for at forebygge en væsentlig hændelse eller for at håndtere en igangværende hændelse, eller hvor offentliggørelse af den væsentlige hændelse på anden vis er i offentlighedens interesse, kan en medlemsstats CSIRT eller i givet fald dens kompetente myndighed, og hvor det er relevant CSIRT'erne eller de kompetente myndigheder i andre berørte medlemsstater efter høring af den berørte enhed informere offentligheden om den væsentlige hændelse eller kræve, at enheden gør det.

Den foreslåede bestemmelse svarer med sproglige tilpasnin-

ger uden indholdsmæssig betydning til NIS 2-direktivets artikel 23, stk. 7, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger, dog med den ændring, at bestemmelsen ikke alene gælder for væsentlige og vigtige teleudbydere, men for samtlige teleudbydere, der er omfattet af nærværende lov.

Dette skal navnlig ses i lyset af, at den gældende lov om sikkerhed i net og tjenester finder anvendelse for samtlige teleudbydere. Henset til det aktuelle trusselsbillede, vurderer Ministeriet for Samfundssikkerhed og Beredskab, at det nuværende sikkerhedsniveau bør opretholdes.

Styrelsen for Samfundssikkerhed vil skulle foretage høring af den berørte teleudbyder, før der træffes afgørelse om, at teleudbyderen skal offentliggøre hændelsen, i overensstemmelse med proceduren beskrevet i bemærkningerne til det foreslåede stk. 1. I forbindelse med en afgørelse om offentliggørelse vil den kompetente myndighed endvidere skulle varetage de fortrolighedshensyn, der ligeledes er beskrevet i bemærkningerne til det foreslåede stk. 1.

Det følger af det foreslåede *stk. 3,* at CSIRT'en efter samme kriterier som i stk. 1, kan informere offentligheden om væsentlige hændelser, der kan påvirke mere end én sektor.

Bestemmelsen vil delvist gennemføre NIS 2-direktivets artikel 23, stk. 7.

Det fremgår af NIS 2-direktivets artikel 23, stk. 7, at hvor offentlighedens kendskab er nødvendig for at forebygge en væsentlig hændelse eller for at håndtere en igangværende hændelse, eller hvor offentliggørelse af den væsentlige hændelse på anden vis er i offentlighedens interesse, kan en medlemsstats CSIRT eller i givet fald dens kompetente myndighed, og hvor det er relevant CSIRT'erne eller de kompetente myndigheder i andre berørte medlemsstater efter høring af den berørte enhed informere offentligheden om den væsentlige hændelse eller kræve, at enheden gør det.

Den foreslåede bestemmelse svarer med sproglige tilpasninger uden indholdsmæssig betydning til NIS 2-direktivets artikel 23, stk. 7, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Bestemmelsen indebærer, at det vil være CSIRT'en, der informerer offentligheden om væsentlige hændelser, når disse kan påvirke flere sektorer, idet det typisk vil være CSIRT'en, der har viden om, at en hændelse rammer flere sektorer eller har potentialet til at ramme flere sektorer.

CSIRT'en vil skulle foretage høring af den berørte teleudbyder, før der træffes afgørelse om, at teleudbyderen skal offentliggøre hændelsen, i overensstemmelse med proceduren beskrevet i bemærkningerne til det foreslåede stk. 1. I forbindelse med en afgørelse om offentliggørelse vil CSIRT'en endvidere skulle varetage de fortrolighedshensyn, og forvaltningslovens regler om tavshedspligt der ligeledes er beskrevet i bemærkningerne til det foreslåede stk. 1. Det forudsættes, at høringen vil ske inden for rammerne af forvaltningslovens regler om tavshedspligt og partshøring.

Herudover forudsættes det, at der sker en tæt koordination mellem CSIRT'en og Styrelsen for Samfundssikkerhed forud for eventuel offentliggørelse af en væsentlig hændelse.

Det følger af det foreslåede *stk. 4,* at CSIRT'en efter samme kriterier som i stk. 1, kan informere offentligheden om væsentlige hændelser i andre medlemsstater.

Bestemmelsen vil delvist gennemføre NIS 2-direktivets artikel 23, stk. 7.

Det fremgår af NIS 2-direktivets artikel 23, stk. 7, at hvor offentlighedens kendskab er nødvendig for at forebygge en væsentlig hændelse eller for at håndtere en igangværende hændelse, eller hvor offentliggørelse af den væsentlige hændelse på anden vis er i offentlighedens interesse, kan en medlemsstats CSIRT eller i givet fald dens kompetente myndighed, og hvor det er relevant CSIRT'erne eller de kompetente myndigheder i andre berørte medlemsstater, efter høring af den berørte enhed informere offentligheden om den væsentlige hændelse eller kræve, at enheden gør det.

Den foreslåede bestemmelse svarer med sproglige tilpasninger uden indholdsmæssig betydning til NIS 2-direktivets artikel 23, stk. 7, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Den foreslåede bestemmelse indebærer, at CSIRT'en efter høring af en enhed i en anden medlemsstat, hvor teleudbyderen er ramt af en væsentlig hændelse, kan informere offentligheden i Danmark om den væsentlige hændelse.

Det er et krav, at offentliggørelsen er nødvendig for at forebygge eller håndtere en lignende hændelse i Danmark, eller at offentliggørelsen på anden vis er i den danske offentligheds interesse. En sådan situation vil eksempelvis foreligge, hvis CSIRT'en vurderer, at den konkrete væsentlige hændelse kan have grænseoverskridende virkning, og at det derfor er nødvendigt at orientere offentligheden, således at der i Danmark kan træffes de fornødne forebyggende foranstaltninger eller modforholdsregler.

Før der træffes afgørelse om, at teleudbyderen skal offentliggøre hændelsen, vil CSIRT'en skulle foretage høring af den berørte teleudbyder i overensstemmelse med proceduren beskrevet i bemærkningerne til det foreslåedes stk. 1. Det forudsættes dog, at høringen af teleudbyderen vil ske via det centrale kontaktpunkt i den pågældende medlemsstat. I forbindelse med en afgørelse om offentliggørelse vil CSIRT'en endvidere skulle varetage de fortrolighedshensyn og forvaltningslovens regler om tavshedspligt, der er beskrevet i bemærkningerne til det foreslåede stk. 1.

Til § 13

Det følger af § 5, stk. 3, i lov om sikkerhed i net og tjenester, at Styrelsen for Samfundssikkerhed koordinerer og

prioriterer beredskabsaktørernes behov for samfundsvigtig elektronisk kommunikation i beredskabssituationer og i andre ekstraordinære situationer. Der følger af bestemmelsens 2. pkt. at Styrelsen for Samfundssikkerhed kan fastsætte regler om, at erhvervsmæssige udbydere skal sikre, at de foretagne prioriteringer gennemføres i net og tjenester.

Bemyndigelsen i § 5, stk. 3, er udmøntet i bekendtgørelse nr. 261 af 22. februar 2021 om beredskabsaktørers adgang til elektronisk kommunikation i beredskabssituationer mv.

Bestemmelsen i § 5, stk. 3, gennemfører i øvrigt delvist artikel 108 i EU's telekodeks. Artikel 108 berøres ikke af NIS 2-direktivet.

Ordningen er en del af den samlede beredskabsplanlægning inden for den civile sektor. Det følger således af § 24, stk. 1, i beredskabsloven, jf. lovbekendtgørelse nr. 314 af 3. april 2017 med senere ændringer, at hver enkelt minister inden for sit område skal planlægge for opretholdelse og videreførelse af samfundets funktioner i tilfælde af større ulykker og katastrofer, herunder udarbejde beredskabsplaner.

Bestemmelsens anvendelsesområde omfatter beredskabssituationer samt andre ekstraordinære situationer. Dette omfatter såvel situationer med krigshandlinger som situationer, hvor det som følge af en større ulykke, katastrofe eller anden ekstraordinær hændelse eller krise er nødvendigt at indføre særlige foranstaltninger vedrørende net og tjenester med henblik på at opretholde samfundets funktioner. Bestemmelsens anvendelsesområde omfatter således både naturskabte og menneskeskabte ulykker og katastrofer, herunder eksempelvis orkan- og stormflodssituationer og alvorlige cyberangreb.

Det foreslås i *stk. 1,* at Styrelsen for Samfundssikkerhed koordinerer og prioriterer beredskabsaktørernes behov for samfundsvigtig elektronisk kommunikation i beredskabssituationer og i andre ekstraordinære situationer.

Ministeriet for Samfundssikkerhed og Beredskab finder det således henset til vurderingen af det aktuelle trusselsniveau mod telesektoren væsentligt at opretholde det nuværende sikkerhedsniveau for sektoren. Der er med videreførelsen af bestemmelsen ikke tilsigtet materielle ændringer af bestemmelsens indhold.

Den foreslåede bestemmelse vedrører koordinering og prioritering af de forskellige beredskabsaktørers behov for elektronisk kommunikation i beredskabssituationer og i andre ekstraordinære situationer. En sådan koordinering og prioritering vil ofte være nødvendigt i beredskabssituationer og i andre ekstraordinære situationer, hvor der kan opstå kapacitetsproblemer eller beskadigelse af teleinfrastrukturen.

Ved beredskabsaktører forstås myndigheder, virksomheder og institutioner som skal bidrage til opretholdelse af samfundets funktioner i en beredskabssituation eller i en anden ekstraordinær situation.

Bestemmelsen indebærer, at Styrelsen for Samfundssikkerhed fortsat varetager den overordnede krisestyring i forhold til telesektoren. Styrelsen for Samfundssikkerhed skal i den forbindelse i beredskabssituationer eller i andre ekstraordinære situationer være bindeled mellem beredskabsaktører samt vigtige og væsentlige teleudbydere og søge at tilgodese eller prioritere mellem beredskabsaktørernes behov for elektronisk kommunikation. Styrelsen for Samfundssikkerhed skal i den forbindelse koordinere teleberedskabet med beredskabsindsatsen i de øvrige samfundssektorer.

Det foreslås med *stk. 2,* at væsentlige og vigtige teleudbydere skal sikre, at de foretagne prioriteringer gennemføres i net og tjenester.

Bestemmelsen viderefører § 5, stk. 3, 2. pkt. i lov om sikker i net og tjenester.

Det foreslås i *stk. 3, 1. pkt.,* at væsentlige og vigtige teleudbydere skal underrette Styrelsen for Samfundssikkerhed i tilfælde, hvor udbyderen aktiverer sit beredskab, eller hvor udbyderen bliver bekendt med en hændelse, som vurderes at kunne føre til en beredskabssituation eller en anden ekstraordinær situation for teleudbyderen selv eller for en anden udbyder.

Den foreslåede bestemmelse viderefører delvist indholdet af § 5, stk. 2, i lov om sikkerhed i net og tjenester.

Det foreslås i *stk. 3, 2. pkt.,* at ministeren for samfundssikkerhed og beredskab kan fastsætte nærmere regler om underretningspligten efter 1. pkt.

Den foreslåede bestemmelse viderefører delvist indholdet af § 5, stk. 2, i lov om sikkerhed i net og tjenester.

De regler, som Styrelsen for Samfundssikkerhed med hjemmel i bestemmelsen kan fastsætte nærmere regler om omfatter regler om underretningspligten efter 1. pkt., herunder regler om hvorledes underretnings skal foretages.

Det foreslås i *stk. 4, 1. pkt.*at teleudbydere, som i medfør af lov om elektroniske kommunikationsnet og -tjenester skal udsende offentlige advarsler om overhængende eller truende alvorlige nødsituationer og katastrofer, skal træffe alle nødvendige foranstaltninger til at sikre uafbrudt transmission af advarslerne.

Den foreslåede bestemmelse viderefører § 5 a i lov om sikkerhed i net og tjenester.

Det foreslås i *stk. 4, 2. pkt.,* at ministeren for samfundssikkerhed og beredskab kan fastsætte nærmere regler om foranstaltninger efter 1. pkt.

Den foreslåede bestemmelse viderefører § 5 a i lov om sikkerhed i net og tjenester, jf. lovbekendtgørelse nr. 153 af 1. februar 2021, som ændret ved § 18 i lov nr. 1156 af 8. juni 2021. Bemyndigelsen til at fastsætte regler er ikke udmøntet i dag.

Der vil med hjemmel i den foreslåede bestemmelse kunne fastsættes regler om, at udbydere, som i medfør af teleloven skal udsende offentlige advarsler om overhængende eller truende alvorlige nødsituationer og katastrofer, skal træffe alle nødvendige foranstaltninger til at sikre uafbrudt transmission af advarslerne.

Den foreslåede bestemmelse gennemfører den del af artikel 108, 2. pkt., i EU's telekodeks, hvorefter medlemsstaterne sikrer, at udbydere af talekommunikationstjenester træffer alle nødvendige foranstaltninger til at sikre uafbrudt transmission af offentlige advarsler. Artikel 108, 2 pkt. berøres ikke af NIS 2-direktivet.

Den pågældende del af bestemmelsen i artikel 108, 2. pkt., i EU's telekodeks skal ses i sammenhæng med artikel 110, der pålægger medlemsstater, der allerede har etableret offentlige varslingssystemer, at sørge for, at udbydere af mobile nummerbaserede interpersonelle kommunikationstjenester udsender offentlige advarsler til berørte slutbrugere (mobilbaseret varsling).

Forpligtelsen i artikel 110 er implementeret ved telelovens § 62, stk. 1 da forpligtelsen har nær sammenhæng med eksisterende forpligtelser i teleloven i relation til bl.a. alarm- og beredskabsforhold. Det mobilbaserede varslingssystem, der er etableret i medfør af artikel 110 i EU's telekodeks og implementeret i dansk ret ved telelovens § 62, blev taget i brug i foråret 2023.

Forpligtelsen til at udsende offentlige advarsler, der følger af telelovens § 62, stk. 1, påhviler de såkaldte mobiloperatører, som omfatter udbydere af elektroniske kommunikationstjenester i mobilnet og udbydere af mobilnet.

Den foreslåede bestemmelse har til formål at sikre, at mobiloperatørerne træffer alle nødvendige foranstaltninger for at undgå, at udstyr og systemer, der anvendes i forbindelse med transmission af offentlige advarsler, afbrydes. Mobiloperatørerne vil i forlængelse af eksisterende forpligtelser til at sikre en robust teleinfrastruktur skulle planlægge og sørge for opretholdelsen af uafbrudt transmission af offentlige advarsler, herunder i relation til udstyr og systemer, der anvendes til transmission af offentlige advarsler, bl.a. tage stilling til fremskaffelse af det nødvendige reserveudstyr, og sikring af redundans og nødstrømsforsyning.

Det foreslås i *stk. 5, 1. pkt.,* at i beredskabssituationer og i andre ekstraordinære situationer kan Styrelsen for Samfundssikkerhed påbyde væsentlige og vigtige teleudbydere uden unødigt ophold at iværksætte nærmere angivne sikkerhedsforanstaltninger.

Den foreslåede bestemmelse viderefører indholdet af § 5, stk. 4, i lov om sikkerhed i net og tjenester, jf. lovbekendtgørelse nr. 153 af 1. februar 2021, som ændret ved § 18 i lov nr. 1156 af 8. juni 2021.

Ministeriet for Samfundssikkerhed og Beredskab finder det henset til vurderingen af det aktuelle trusselsniveau mod telesektoren væsentligt at opretholde det nuværende sikkerhedsniveau for sektoren. Der er med videreførelsen af bestemmelsen ikke tilsigtet materielle ændringer af bestemmelsens indhold.

Den gældende bestemmelse i § 5, stk. 4, i lov om sikkerhed i net og tjenester gennemfører i øvrigt delvist artikel 108 i EU's telekodeks. Artikel 108 berøres ikke af NIS 2-direktivet.

Ordningen er en del af den samlede beredskabsplanlægning inden for den civile sektor. Det følger således af § 24, stk. 1, i beredskabsloven, jf. lovbekendtgørelse nr. 314 af 3. april 2017 med senere ændringer, at hver enkelt minister inden for sit område skal planlægge for opretholdelse og videreførelse af samfundets funktioner i tilfælde af større ulykker og katastrofer, herunder udarbejde beredskabsplaner.

Bestemmelsens anvendelsesområde omfatter beredskabssituationer samt andre ekstraordinære situationer. Dette omfatter såvel situationer med krigshandlinger som situationer, hvor det som følge af en større ulykke, katastrofe eller anden ekstraordinær hændelse eller krise er nødvendigt at indføre særlige foranstaltninger vedrørende net og tjenester med henblik på at opretholde samfundets funktioner. Bestemmelsens anvendelsesområde omfatter således både naturskabte og menneskeskabte ulykker og katastrofer, herunder eksempelvis orkan- og stormflodssituationer og alvorlige cyberangreb.

Styrelsen for Samfundssikkerhed vil efter den foreslåede bestemmelse kunne påbyde væsentlige og vigtige teleudbydere at iværksætte akutte sikkerhedsforanstaltninger, forudsat at der er en hændelse eller trussel, der i betydeligt omfang påvirker, eller kan påvirke, udbuddet af net og tjenester negativt. En hændelse, der i betydeligt omfang påvirker udbuddet af net og informationssystemer, kan eksempelvis være et alvorligt cyberangreb eller et terrorangreb, som medfører, at net eller informationssystemer i en periode ikke er tilgængelige for slutbrugerne. Sådanne hændelser kan endvidere være kraftige vejrfænomener såsom orkaner eller skybrud, der medfører, at større dele af teleinfrastrukturen beskadiges. En trussel, der vurderes i betydeligt omfang at kunne påvirke udbuddet af net eller tjenester, vil eksempelvis være, hvis der foreligger oplysninger om et nært forestående sabotageforsøg eller terrorangreb mod kritiske dele af teleinfrastrukturen.

For at anvende bestemmelsen skal der foreligge en beredskabssituation eller en anden ekstraordinær situation, eller en risiko for påvirkning af udbuddet af net og tjenester. Det bemærkes i den forbindelse, at en hændelse eller trussel, der i betydeligt omfang påvirker, eller kan påvirke, udbuddet af net eller informationssystemer negativt, i sig selv kan udgøre en beredskabssituation.

Det foreslås i *stk. 5, 2. pkt.,* at ministeren for samfundssikkerhed og beredskab kan fastsætte regler om de sikkerhedsforanstaltninger, der er nævnt i 1. pkt.

Der vil bl.a. kunne fastsættes regler om, at Styrelsen for Samfundssikkerhed kan i påbyde væsentlige og vigtige teleudbydere at iværksætte akutte sikkerhedsforanstaltninger såsom indførelse af særlige adgangskontroller til udbyderens lokaliteter, begrænsning af adgangsveje til og parkeringsrestriktioner på udbyderens arealer samt eftersyn med udbyderens arealer og bygninger. Der kan endvidere fastsættes regler om, at Styrelsen for Samfundssikkerhed kan påbyde de væsentlige og de vigtige teleudbydere foranstaltninger ved håndteringen af postforsendelser, f.eks. gennemlysning af breve og pakker. Desuden kan der fastsættes regler om, at Styrelsen for Samfundssikkerhed kan påbyde udbyderne at udpege særligt kritiske eller aktuelt truede dele af deres teleinfrastruktur og sørge for vagtrundering, kontrol med sikringsforanstaltninger og eventuelt bevogtning af de pågældende dele af teleinfrastrukturen i samarbejde med relevante beredskabsaktører. Der kan tillige fastsættes regler om, at Styrelsen for Samfundssikkerhed kan påbyde de væsentlige og de vigtige teleudbydere at foranstalte akutte sikkerhedsforanstaltninger til begrænsning af skadevirkningen af eksempelvis naturskabte hændelser. Der kan endvidere fastsættes regler om, at Styrelsen for Samfundssikkerhed i forhold til cyberangreb eksempelvis kan påbyde logning eller blokering af IP-adresser, der anvendes som led i et angreb. Derudover kan der fastsættes regler om, at styrelsen kan påbyde udbyderne at gennemgå deres beredskabsplaner med henblik på at kunne iværksatte de forberedte tiltag til sikring af teleinfrastrukturen.

Det forudsættes, at udbyderne skal foretage de pågældende foranstaltninger uden omkostninger for staten, hvilket svarer til, at der heller ikke på andre områder udtrykkeligt er angivet, at de påkrævede foranstaltninger skal foretages uden omkostninger for staten.

Det foreslås i *stk. 6,* at i beredskabssituationer og i andre ekstraordinære situationer skal væsentlige teleudbydere efter påbud fra Styrelsen for Samfundssikkerhed prioritere retablering af nærmere angivne dele af udbyderens beskadigede infrastruktur.

Den foreslåede ordning er en videreførelse af § 17 i bekendtgørelse nr. 261 om beredskabsaktørers adgang til elektronisk kommunikation i beredskabssituationer mv.

Henset til det aktuelle trusselsbillede finder Ministeriet for Samfundssikkerhed og Beredskab, at der skal ske en videreførelse af den nævnte bestemmelse.

Der forudsættes ikke en ændring af gældende ret, og bestemmelsen skal således fortolkes i overensstemmelse med den gældende fortolkning og praksis på området.

Det foreslås i *stk. 7,* at i beredskabssituationer og i andre ekstraordinære situationer, hvor der opstår kapacitetsproblemer, skal væsentlige teleudbydere efter påbud fra Styrelsen for Samfundssikkerhed prioritere fremførsel i net af nærmere angivne forbindelser og tjenester, herunder om nødvendigt afbryde andre forbindelser eller tjenester helt eller delvist.

Den foreslåede ordning er en videreførelse af § 18 i bekendtgørelse nr. 261 om beredskabsaktørers adgang til elektronisk kommunikation i beredskabssituationer mv.

Henset til det aktuelle trusselsbillede finder Ministeriet for Samfundssikkerhed og Beredskab, at der skal ske en videreførelse af den nævnte bestemmelse.

Der forudsættes ikke en ændring af gældende ret, og bestemmelsen skal således fortolkes i overensstemmelse med den gældende fortolkning og praksis på området.

Til § 14

Det følger af § 7, stk. 1, i lov om sikkerhed i net og tjenester, at det i regler udstedt i medfør af lovens § 4, kan fastsættes, at underretninger og afgivelse af oplysninger efter § 4, nr. 1-3, er undtaget fra aktindsigt efter lov om offentlighed i forvaltningen og partsaktindsigt efter forvaltningsloven.

Der følger endvidere at § 8, stk. 1, i lov om sikkerhed i net og tjenester, at myndigheder og virksomheder kan underrette Styrelsen for Samfundssikkerhed om hændelser, der negativt påvirker eller vurderes at ville kunne påvirke tilgængelighed, integritet eller fortrolighed af data, informationssystemer, digitale netværk eller digitale servicer. Sådanne underretninger er efter bestemmelsens stk. 2, undtaget fra aktindsigt efter lov om offentlighed i forvaltningen og partsaktindsigt efter forvaltningsloven.

Det foreslås i *stk. 1,* at underretninger modtaget i medfør af § 8, stk. 2 og § 10 er undtaget fra aktindsigt efter lov om offentlighed i forvaltningen og partsaktindsigt efter forvaltningsloven.

Bestemmelsen viderefører indholdet af § 8, stk. 1 og 2 i lov om sikkerhed i net og tjenester.

Bemyndigelsen til at fastsætte regler om aktindsigt er i dag udmøntet i bekendtgørelse nr. 258 af 22. februar 2021 om oplysnings- og underretningspligter vedrørende sikkerhed i net og tjenester.

Det følger af den foreslåede § 8, stk. 2, at teleudbydere skal underrette Styrelsen for Samfundssikkerhed og CSIRT'en om enhver væsentlig hændelse.

Det følger af den foreslåede § 10, stk. 1, at teleudbydere kan underrette Styrelsen for Samfundssikkerhed og CSIRT'en om hændelser, nærvedhændelser og cybertrusler.

Undtagelserne fra aktindsigt skal navnlig ses i lyset af, at en velfungerende underretningsordning forudsætter, at der ikke er risiko for, at de ofte særligt kommercielt følsomme oplysninger, som vil blive modtaget fra teleudbyderne, kan tilgå teleudbydernes konkurrenter eller potentielle angribere.

Undtagelsen skal navnlig ses i lyset af, at underretning af Styrelsen for Samfundssikkerhed skaber de bedst mulige forudsætninger for, at styrelsen kan udnytte erfaringer med cybertrusler og sikkerhedsrisici på tværs af samfundet – og dermed skabe et samlet overblik over den aktuelle sikkerhedstilstand på den danske del af internettet. Underretningerne sætter således Styrelsen for Samfundssikkerhed i stand til at varsle hurtigere om trusler og styrke grundlaget for styrelsens rådgivning om risici og passende sikkerhedstiltag.

Oplysninger om, at der f.eks. er gennemført et vellykket hackerangreb, hvor en virksomhed har mistet data, kan imidlertid i høj grad skade virksomhedens omdømme, og risikoen for, at oplysningerne via aktindsigt bliver offentligt tilgængelige, kan i praksis afholde mange virksomheder fra at underrette Styrelsen for Samfundssikkerhed om et sådant hackerangreb. Derfor bør også disse særlige underretninger være undtaget fra aktindsigt.

Undtagelsen fra aktindsigt omfatter ikke teleudbydernes adgang til at gøre sig bekendt med oplysninger, der vedrører deres egne forhold.

Til § 15

Det foreslås i *§ 15,* at det i regler udstedt i medfør af § 7, stk. 5 kan fastsættes, at underretninger og afgivelse af oplysninger efter denne bestemmelse er undtaget fra aktindsigt efter lov om offentlighed i forvaltningen og partsaktindsigt efter forvaltningsloven.

Det følger af den foreslåede § 7, stk. 5, at ministeren for samfundssikkerhed og beredskab kan fastsætte nærmere regler om oplysnings- og underretningspligter for væsentlige- og vigtige teleudbydere, herunder krav om: 1) afgivelse af oplysninger om væsentlige dele teleudbyderens net eller tjenester eller driften heraf, 2) krav om underretning ved påtænkt indgåelse af aftaler om leverancer, der vedrører væsentlige dele af udbyderens net eller tjenester eller driften heraf, og 3) krav om, at teleudbyderen skal indsende et endeligt aftaleudkast til Styrelsen for Samfundssikkerhed umiddelbart forud for indgåelse af aftalen, og at aftalen først kan indgås op til 25 arbejdsdage efter styrelsens modtagelse af pågældende udkast.

Det foreslås, at der ikke skal være mulighed for aktindsigt i teleudbyderes afgivelse af oplysninger om væsentlige dele af teleudbyderens net eller tjenester eller driften heraf.

De oplysninger, som Styrelsen for Samfundssikkerhed som led i den foreslåede § 7, stk. 5, nr. 1, modtager fra og sender til teleudbydere vedrørende væsentlige dele af udbyderens net og tjenester eller varetagelsen af driften heraf, vil ofte indeholde oplysninger om fejl eller sårbarheder i net eller tjenester, som kan misbruges af potentielle angribere, hvis de kommer til uvedkommendes kendskab. Det foreslås derfor, at oplysningerne i deres helhed undtages fra aktindsigt, herunder partsaktindsigt efter forvaltningsloven, således at aktindsigtsanmodninger ikke – som det ellers ville være tilfældet – behandles efter principperne i offentlighedsloven.

Det forudsættes endvidere, at der i medfør af den foreslåede bestemmelse kan fastsættes regler om, at der ikke er adgang til aktindsigt i de udkast til aftaler, som væsentlige og vigtige teleudbydere indsender til Styrelsen for Samfundssikkerhed i medfør af regler fastsat efter den foreslåede § 7, stk. 5, nr. 2. Aftalerne vil ofte indeholde en lang række oplysninger om udbydernes net og tjenester samt aftaleforhold, som dels er kommercielt fortrolige, dels kan misbruges af potentielle angribere. Reglerne svarer til den gældende § 7, stk. 1, i lov om sikkerhed i net og tjenester. Der tilsigtes ikke en ændring af denne praksis.

Til § 16

Cirkulære nr. 10338 af 17. december 2014 om sikkerhedsbeskyttelse af informationer af fælles interesse for landene i NATO eller EU, andre klassificerede informationer samt informationer af sikkerhedsmæssig beskyttelsesinteresse i øvrigt (sikkerhedscirkulæret) indeholder de almindelige regler for bl.a. sikkerhedsundersøgelser og sikkerhedsgodkendelser af ansatte i offentlige myndigheder og ansatte i private firmaer, der arbejder for en offentlig myndighed.

Lov om sikkerhed i net og tjenester indeholder i lovens kapitel 4 regler om sikkerhedsgodkendelser af medarbejdere og repræsentanter for teleudbydere i tilfælde, hvor de pågældende som led i deres konkrete opgaveløsning for udbyderen skal behandle klassificerede informationer eller andre informationer, der er særligt beskyttelsesværdige i relation til sikkerhed i net og tjenester eller beredskab.

Den foreslås i *stk. 1,* at medarbejdere hos væsentlige og vigtige teleudbydere og repræsentanter for disse udbydere skal sikkerhedsgodkendes af Styrelsen for Samfundssikkerhed, når 1) det er nødvendigt i forhold til den pågældendes adgang til klassificeret information eller til de funktioner, som den pågældende skal varetage eller 2) den pågældende varetager kontakten til Styrelsen for Samfundssikkerhed i relation til beredskabet i henhold til regler, der er udstedt i medfør af § 13, stk. 3.

Bestemmelsens viderefører delvist indholdet af den gældende § 6, stk. 1, i lov om sikkerhed i net og tjenester, jf. lovbekendtgørelse nr. 153 af 1. februar 2021, som ændret ved § 18 i lov nr. 1156 af 8. juni 2021.

Bestemmelsen indebærer, at personkredsen nævnt i bestemmelsens stk. 1, skal sikkerhedsgodkendes af Styrelsen for Samfundssikkerhed.

Afgørelsen baseres på en sikkerhedsundersøgelse foretaget af Politiets Efterretningstjeneste og træffes ud fra en konkret vurdering af alle foreliggende oplysninger om den pågældende person. I overensstemmelse med ordningen efter sikkerhedscirkulærets § 14 vil der ved afgørelsen om sikker-

hedsgodkendelse blive lagt vægt på, om vedkommende har udvist ubestridt loyalitet og har en sådan adfærd og karakter, herunder vaner, forbindelser og diskretion, at der ikke kan være tvivl om den pågældendes pålidelighed i forbindelse med håndtering af klassificerede informationer eller andre beskyttelsesværdige informationer. Der kan ved afgørelsen tilsvarende lægges vægt på oplysninger om en ægtefælles, samlevers, registreret partners eller samboendes adfærd, karakter og forhold i øvrigt.

Det foreslås i *stk. 2,* at ministeren for samfundssikkerhed og beredskab efter forhandling med justitsministeren kan fastsætte regler om ansøgninger vedrørende sikkerhedsgodkendelser, herunder betingelser for indgivelse af sådanne ansøgninger samt meddelelse og tilbagekaldelse af sikkerhedsgodkendelser.

Med den foreslåede bestemmelse vil der således i loven være en særskilt hjemmel til fastsættelse af regler om sikkerhedsgodkendelse af medarbejdere hos væsentlige og vigtige teleudbydere og repræsentanter for disse.

Det forventes, at der fastsættes nærmere regler om ansøgning og afgørelser om sikkerhedsgodkendelser, samt meddelelse om og tilbagekaldelse af afgørelser om sikkerhedsgodkendelser. Dette omfatter bl.a. administrative krav i forbindelse med indgivelse af en ansøgning, krav om afmelding, hvis en person ikke længere har en funktion, som forudsætter en sikkerhedsgodkendelse, og bestemmelser om, at afgørelsen tilbagekaldes, hvis en person ikke længere opfylder kravene til godkendelsen.

Til § 17

Det foreslås med *§ 17,* at Styrelsen for Samfundssikkerhed fører tilsyn med overholdelsen af denne lov og regler, der er udstedt i medfør af loven.

Der er således ikke forudsat en ændring af tilsynsmyndigheden på området for sikkerhed og beredskab i telesektoren.

De nærmere regler om Styrelsen for Samfundssikkerheds kompetencer og regler for håndhævelse af fastsat i forslagets §§ 18-25.

Til § 18

Det foreslås i *stk. 1*, at Styrelsen for Samfundssikkerhed kan påbyde væsentlige og vigtige teleudbydere at inddrage nærmere angivne områder af deres virksomhed og nærmere angivne trusler mod sikkerheden i net og informationssystemer i deres risikostyringsprocesser efter § 5, stk. 1.

Bestemmelsen viderefører indholdet af § 3, stk. 2, i lov om sikkerhed i net og tjenester.

Ministeriet for Samfundssikkerhed og Beredskab finder det således henset til vurderingen af det aktuelle trusselsniveau mod telesektoren væsentligt at opretholde det nuværende sikkerhedsniveau for sektoren. Der er med videreførelsen af bestemmelsen ikke tilsigtet materielle ændringer af bestemmelsens indhold.

Det foreslås derfor med bestemmelsen, at Styrelsen for Samfundssikkerhed kan påbyde væsentlige og vigtige teleudbydere at inddrage nærmere angivne områder af deres virksomhed og nærmere angivne trusler mod sikkerheden i net og informationssystemer i deres risikostyringsprocesser efter § 5, stk. 1.

Der kan efter den foreslåede bestemmelse stilles krav om, at udbyderne i risikostyringsprocesserne skal tage højde for bestemte, herunder både konkrete og generelle trusler mod sikkerheden i net og informationssystemer efter påbud fra Styrelsen for Samfundssikkerhed. Det kan eksempelvis ske på baggrund af de trusselsvurderinger, som løbende udarbejdes af Styrelsen for Samfundssikkerhed eller Forsvarets Efterretningstjeneste.

Endvidere kan Styrelsen for Samfundssikkerhed ved påbud bestemme, at visse områder af en udbyders virksomhed, der er nærmere specificeret i påbuddet, skal være omfattet af risikostyringsprocesserne, hvis dette ikke i forvejen er tilfældet.

Det foreslås i *stk. 2*, 1. pkt., at er det af væsentlig samfundsmæssig betydning kan Styrelsen for Samfundssikkerhed påbyde væsentlige og vigtige teleudbydere at træffe konkrete foranstaltninger med henblik på at sikre sikkerheden i net- og informationssystemer, herunder påbud om, at udstyr, der skal anvendes i forbindelse med indgreb i meddelelseshemmeligheden skal opsættes i og drives fra Danmark.

Den foreslåede bestemmelse viderefører indholdet af § 3, stk. 4, i lov om sikkerhed i net og tjenester.

Ministeriet for Samfundssikkerhed og Beredskab finder det således henset til vurderingen af det aktuelle trusselsniveau mod telesektoren væsentligt at opretholde det nuværende sikkerhedsniveau for sektoren. Der er med videreførelsen af bestemmelsen ikke tilsigtet materielle ændringer af bestemmelsens indhold.

Det foreslås derfor med bestemmelsen, at Styrelsen for Samfundssikkerhed skal kunne påbyde væsentlige og vigtige teleudbydere at træffe andre og konkrete foranstaltninger end de i stk. 1 nævnte med henblik på at sikre sikkerheden i net og informationssystemer, hvis sådanne foranstaltninger er af væsentlig samfundsmæssig betydning.

Foranstaltninger af væsentlig samfundsmæssig betydning kan i denne sammenhæng eksempelvis være tiltag, der skal reducere risikoen for, at uvedkommende får adgang til myndigheders elektroniske kommunikation. Det kan endvidere være foranstaltninger, der skal hindre uvedkommendes adgang via net og tjenester til infrastruktur, som er nødvendige, for at samfundsvigtige funktioner opretholdes. Dette kan være funktioner, som er særligt vigtige for samfundets og demokratiets opretholdelse og sikkerhed samt borgernes tryghed, herunder funktioner inden for sundhed, energi,

transport, forsyning, finans, forskning, medier og kommunikation samt funktioner, som har stor økonomisk betydning for samfundet.

Styrelsen for Samfundssikkerhed vil desuden med hjemmel i bestemmelsen kunne påbyde væsentlige teleudbydere og vigtige erhvervsmæssige teleudbydere at sikre, at udstyr og systemer, som skal anvendes i forbindelse med indgreb i meddelelseshemmeligheden – de såkaldte »lawful interception-funktionaliteter« – skal opsættes i og drives fra Danmark. Påbudsmuligheden forudsættes imidlertid ikke benyttet, såfremt en teleudbyder kan godtgøre, at der er et tilstrækkeligt sikkerhedsniveau på trods af, at lawful interception-funktionaliteterne opsættes og drives uden for Danmark. »Lawful interception-funktionaliteterne« vil i tilfælde af utilstrækkelige sikkerhedsforanstaltninger kunne benyttes af uvedkommende til at overvåge telekunders kommunikation, ligesom uvedkommende vil kunne få kendskab til politiets igangværende aflytninger. En tilstrækkelig sikkerhed i forhold til »lawful interception-funktionaliteterne« er derfor særligt vigtig for samfundets og demokratiets opretholdelse og sikkerhed samt borgernes tryghed.

Det bemærkes i den forbindelse, at Styrelsen for Samfundssikkerhed alene vil kunne foretage tilsynsbesøg, såfremt »lawful interception-funktionaliteten« er placeret i Danmark. Opsættes udstyr og systemer, som skal anvendes i forbindelse med indgreb i meddelelseshemmeligheden i udlandet, vil Styrelsen for Samfundssikkerhed således ikke have mulighed for at konstatere, om udbyderne i praksis har gennemført de nødvendige foranstaltninger med henblik på at sikre et passende sikkerhedsniveau i net og informationssystemer. Det bemærkes desuden, at Styrelsen for Samfundssikkerheds tilsyn alene vil omfatte de systemtekniske sikkerhedsforanstaltninger, og at styrelsen ikke i forbindelse med tilsyn vil få adgang til oplysninger om igangværende eller historiske aflytninger.

Et påbud efter den foreslåede bestemmelses stk. 2, vil i almindelighed have karakter af erstatningsfri regulering. Det kan imidlertid ikke udelukkes, at påbud udstedt i medfør af den foreslåede bestemmelse vil kunne ramme væsentlige og vigtige teleudbydere så økonomisk intensivt og atypisk hårdt, at der vil kunne være tale om et ekspropriativt indgreb mod den pågældende udbyder. Det vil bero på en konkret vurdering, om der i det enkelte tilfælde foreligger ekspropriation efter grundlovens § 73. Spørgsmålet om adgang til erstatning efter grundlovens § 73 henhører under domstolene.

De foreslåede bestemmelser indebærer ikke, at der ændres ved det grundlæggende princip om aftalefrihed. Der kan således ikke med hjemmel i bestemmelserne ske regulering af ejerforhold, fastsættes forbud mod at indgå aftale med bestemte leverandører eller forbud mod ejerskab af bestemte netværk eller produkter.

Det foreslås i *stk. 2, 2. pkt.,* at ministeren for samfundssikkerhed og beredskab kan fastsætte nærmere regler om påbud om foranstaltninger efter 1. pkt.

Den foreslåede bestemmelse har til formål at bemyndige ministeren for samfundssikkerhed og beredskab til at fastsætte nærmere regler om påbud om foranstaltninger efter stk. 1. Den nærmere udmøntning af den foreslåede 1. pkt., vil således ske i en bekendtgørelse.

Til § 19

Det følger af § 9, stk. 6, i lov om sikkerhed i net og tjenester, at såfremt det er nødvendigt af hensyn til sikkerheden i net og tjenester, har Styrelsen for Samfundssikkerhed efter et skriftligt varsel på mindst 7 arbejdsdage uden retskendelse mod behørig legitimation adgang til udbyderes forretningslokaler med henblik på at påse overholdelsen af loven og regler, der er udstedt i medfør af loven. Styrelsen for Samfundssikkerhed kan ikke i forbindelse med adgang til forretningslokaler tilgå kommunikation til, fra eller mellem udbyderens kunder.

Der følger endvidere af § 9, stk. 7 i lov om sikkerhed i net og tjenester, at såfremt det er nødvendigt af hensyn til sikkerheden i net og tjenester, har Styrelsen for Samfundssikkerhed efter et skriftligt varsel på mindst 7 arbejdsdage uden retskendelse mod behørig legitimation adgang til forretningslokaler hos udbyderes samarbejdspartnere, leverandører eller underleverandører med henblik på at påse overholdelsen af loven og regler, der er udstedt i medfør af loven, i relation til outsourcet aktivitet.

Det foreslås i *stk. 1,* at Styrelsen for Samfundssikkerhed som led i sit tilsyn ud fra en konkret vurdering af omstændighederne i hver enkelt sag kan anvende nærmere angivne tilsynsforanstaltninger over for en væsentlig teleudbyder.

Det foreslås med *nr. 1,* at Styrelsen for Samfundssikkerhed uden retskendelse of mod behørig legitimation kan foretage kontrol hos teleudbydere samt deres samarbejdspartnere, leverandører eller underleverandører i relation til outsourcet aktivitet og eksternt tilsyn, herunder foretage stikprøvekontroller.

Den foreslåede bestemmelse vil gennemføre artikel 32, stk. 1 og 2, i NIS 2-direktivet.

Det følger af NIS 2-direktivets artikel 32, stk. 1, at medlemsstaterne skal sikre, at de tilsyns- eller håndhævelsesforanstaltninger, der pålægges væsentlige enheder, for så vidt angår forpligtelserne fastsat i direktivet, er effektive, står i rimeligt forhold til overtrædelsen og har afskrækkende virkning under hensyntagen til omstændighederne i hver enkelt sag.

Den foreslåede bestemmelse i stk. 1, nr. 1, vil endvidere videreføre § 9, stk. 6 og 7 i lov om sikkerhed i net og tjenester.

Ministeriet for Samfundssikkerhed og Beredskab finder det således henset til vurderingen af det aktuelle trusselsniveau mod telesektoren, jf. lovforslagets pkt. 1 ovenfor, væsentligt at opretholde det nuværende sikkerhedsniveau for sekto-

ren. Der er med videreførelsen af bestemmelsen ikke tilsigtet materielle ændringer af bestemmelsens indhold.

For effektivt at kunne konstatere, om væsentlige teleudbydere i praksis har gennemført de nødvendige foranstaltninger til at sikre deres net- og informationssystemer, er det nødvendigt, at Styrelsen for Samfundssikkerhed som led i et tilsyn har adgang til forretningslokaler hos væsentlige teleudbydere. Det foreslås derfor, at der skal være adgang til kontrol på stedet uden retskendelse og mod behørig legitimation.

Den foreslåede bestemmelse vil betyde, at Styrelsen for Samfundssikkerhed som led i et tilsyn kan foretage kontrol på stedet til enhver tid. Det forudsættes dog almindeligvis, at Styrelsen for Samfundssikkerhed forinden et kontrolbesøg vil varsle den væsentlige enhed herom.

Det bemærkes, at Styrelsen for Samfundssikkerhed ikke i forbindelse med adgang til forretningslokaler efter stk. 1, kan tilgå kommunikation til, fra eller mellem udbyderens kunder.

Styrelsen for Samfundssikkerhed vil ikke i forbindelse med tilsynsbesøgene kunne få adgang til elektronisk kommunikation til, fra og mellem udbydernes kunder, ligesom centeret alene vil kunne foretage tilsynsbesøg i det omfang, udbyderens forretningslokaler er placeret i Danmark.

Det foreslås i *nr. 2,* at Styrelsen for Samfundssikkerhed kan foretage regelmæssige og målrettede sikkerhedsaudits eller stille krav om, at udbyderen får et kvalificeret uafhængigt organ til at foretage disse audits, og at resultaterne heraf stilles til rådighed for Styrelsen for Samfundssikkerhed,

Den foreslåede bestemmelse vil gennemføre artikel 32, stk. 1 og 2, i NIS 2-direktivet. Den foreslåede bestemmelse svarer med sproglige tilpasninger uden indholdsmæssig betydning til NIS 2-direktivets artikel 32, stk. 1 og 2, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Det følger af NIS 2-direktivets artikel 32, stk. 1, at medlemsstaterne skal sikre, at de tilsyns- eller håndhævelsesforanstaltninger, der pålægges væsentlige enheder, for så vidt angår forpligtelserne fastsat i direktivet, er effektive, står i rimeligt forhold til overtrædelsen og har afskrækkende virkning under hensyntagen til omstændighederne i hver enkelt sag.

Efter direktivets artikel 32, stk. 2, 2. led, baseres de målrettede sikkerhedsaudits, der er omhandlet i første led, litra b, på risikovurderinger foretaget af den kompetente myndighed eller den reviderede enhed eller på andre tilgængelige risikorelaterede oplysninger. Resultaterne af enhver målrettet sikkerhedsaudit stilles til rådighed for den kompetente myndighed. Omkostningerne ved en sådan målrettet sikkerhedsaudit, der udføres af et uafhængigt organ, afholdes af den reviderede enhed, undtagen i behørigt begrundede tilfælde når den kompetente myndighed bestemmer andet.

Det foreslås i *nr. 3,* at Styrelsen for Samfundssikkerhed kan foretage sikkerhedsaudits ad hoc.

Den foreslåede bestemmelse vil gennemføre artikel 32, stk. 1 og 2, i NIS 2-direktivet. Den foreslåede bestemmelse svarer med sproglige tilpasninger uden indholdsmæssig betydning til NIS 2-direktivets artikel 32, stk. 1 og 2, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Det følger af NIS 2-direktivets artikel 32, stk. 1, at medlemsstaterne skal sikre, at de tilsyns- eller håndhævelsesforanstaltninger, der pålægges væsentlige enheder, for så vidt angår forpligtelserne fastsat i direktivet, er effektive, står i rimeligt forhold til overtrædelsen og har afskrækkende virkning under hensyntagen til omstændighederne i hver enkelt sag.

Det foreslås i *nr. 4,* at Styrelsen for Samfundssikkerhed kan foretage sikkerhedsscanninger.

Den foreslåede bestemmelse vil gennemføre artikel 32, stk. 1 og 2, i NIS 2-direktivet. Den foreslåede bestemmelse svarer med sproglige tilpasninger uden indholdsmæssig betydning til NIS 2-direktivets artikel 32, stk. 1 og 2, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Det følger af NIS 2-direktivets artikel 32, stk. 1, at medlemsstaterne skal sikre, at de tilsyns- eller håndhævelsesforanstaltninger, der pålægges væsentlige enheder, for så vidt angår forpligtelserne fastsat i direktivet, er effektive, står i rimeligt forhold til overtrædelsen og har afskrækkende virkning under hensyntagen til omstændighederne i hver enkelt sag.

Det foreslås i *nr. 5,* at Styrelsen for Samfundssikkerhed kan kræve at få udleveret oplysninger, der er nødvendige for at vurdere de foranstaltninger til styring af sikkerhedsrisici, som den berørte udbyder har indført.

Den foreslåede bestemmelse vil gennemføre artikel 32, stk. 1 og 2, i NIS 2-direktivet. Den foreslåede bestemmelse svarer med sproglige tilpasninger uden indholdsmæssig betydning til NIS 2-direktivets artikel 32, stk. 1 og 2, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Det følger af NIS 2-direktivets artikel 32, stk. 1, at medlemsstaterne skal sikre, at de tilsyns- eller håndhævelsesforanstaltninger, der pålægges væsentlige enheder, for så vidt angår forpligtelserne fastsat i direktivet, er effektive, står i rimeligt forhold til overtrædelsen og har afskrækkende virkning under hensyntagen til omstændighederne i hver enkelt sag.

Det foreslås i *nr. 6,* at Styrelsen for Samfundssikkerhed kan kræve at få adgang til data, dokumenter og oplysninger, der er nødvendige for udførelsen af tilsynsopgaven, herunder til

afgørelse af om et forhold er omfattet af denne lov eller regler udstedt i medfør af loven.

Den foreslåede bestemmelse vil gennemføre artikel 32, stk. 1 og 2, i NIS 2-direktivet. Den foreslåede bestemmelse svarer med sproglige tilpasninger uden indholdsmæssig betydning til NIS 2-direktivets artikel 32, stk. 1 og 2, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Det følger af NIS 2-direktivets artikel 32, stk. 1, at medlemsstaterne skal sikre, at de tilsyns- eller håndhævelsesforanstaltninger, der pålægges væsentlige enheder, for så vidt angår forpligtelserne fastsat i direktivet, er effektive, står i rimeligt forhold til overtrædelsen og har afskrækkende virkning under hensyntagen til omstændighederne i hver enkelt sag.

Det foreslås i *nr. 7,* at Styrelsen for Samfundssikkerhed kan kræve at få udleveret dokumentation for gennemførelsen af sikkerhedspolitikker.

Den foreslåede bestemmelse vil gennemføre artikel 32, stk. 1 og 2, i NIS 2-direktivet. Den foreslåede bestemmelse svarer med sproglige tilpasninger uden indholdsmæssig betydning til NIS 2-direktivets artikel 32, stk. 1 og 2, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Det følger af NIS 2-direktivets artikel 32, stk. 1, at medlemsstaterne skal sikre, at de tilsyns- eller håndhævelsesforanstaltninger, der pålægges væsentlige enheder, for så vidt angår forpligtelserne fastsat i direktivet, er effektive, står i rimeligt forhold til overtrædelsen og har afskrækkende virkning under hensyntagen til omstændighederne i hver enkelt sag.

Det foreslås i *nr. 8,* at Styrelsen for Samfundssikkerhed kan kræve at få skriftlige udtalelser og redegørelser om faktiske forhold af betydning for Styrelsen for Samfundssikkerheds tilsynsvirksomhed.

Den foreslåede bestemmelse vil gennemføre artikel 32, stk. 1 og 2, i NIS 2-direktivet.

Det følger af NIS 2-direktivets artikel 32, stk. 1, at medlemsstaterne skal sikre, at de tilsyns- eller håndhævelsesforanstaltninger, der pålægges væsentlige enheder, for så vidt angår forpligtelserne fastsat i direktivet, er effektive, står i rimeligt forhold til overtrædelsen og har afskrækkende virkning under hensyntagen til omstændighederne i hver enkelt sag.

Den foreslåede bestemmelse svarer med sproglige tilpasninger uden indholdsmæssig betydning til NIS 2-direktivets artikel 32, stk. 1 og 2, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Det er Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at der for de foreslåede tilsynsforanstaltninger vil være tale om et indgreb, der er omfattet af lov om retssikkerhed ved forvaltningens anvendelse af tvangsindgreb og oplysningspligter. Dette indebærer, at retten til ikke at inkriminere sig selv, jf. kapitel 4 i nævnte lov, skal overholdes. Det bemærkes dog, at det af bemærkningerne til § 10 i lov om retssikkerhed ved forvaltningens anvendelse af tvangsindgreb og oplysningspligter fremgår, at »[b]estemmelsen [om forbud mod selvinkriminering] er ikke til hinder for, at den mistænkte kan pålægges at give (faktuelle) oplysninger, som er uden betydning for bedømmelsen af, hvorvidt den pågældende har begået en lovovertrædelse, der kan medføre straf.«

Det foreslås i *stk. 2*, at ved anvendelsen af tiltagene i stk. 1, nr. 5-8, skal Styrelsen for Samfundssikkerhed angive formålet med tiltaget og præcisere, hvilke oplysninger der kræves udleveret og hvordan og i hvilken form oplysningerne og materialet nævnt i stk. 1, nr. 5-8, skal udleveres.

Den foreslåede bestemmelse vil gennemføre NIS 2-direktivets artikel 32, stk. 3, hvorefter de kompetente myndigheder ved udøvelsen af deres beføjelser i henhold til artikel 32, stk. 2, litra e, f eller g, skal angive formålet med anmodningen og præcisere, hvilke oplysninger der anmodes om.

Den foreslåede bestemmelse svarer indholdsmæssigt til NIS 2-direktivets artikel 32, stk. 3, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Den foreslåede bestemmelse indebærer endvidere, at Styrelsen for Samfundssikkerhed i forbindelse med, at der stilles krav om udlevering af oplysninger eller materiale efter de foreslåede bestemmelser i stk. 1, nr. 5-8, samtidig kan kræve, at oplysningerne eller materialet udleveres på en bestemt måde, på et bestemt sprog og i en bestemt form.

Der vil eksempelvis kunne stilles krav om anvendelse af bestemte skemaer, eller at der skal foretages indtastninger på en hjemmeside.

Til § 20

Det foreslås i *stk. 1,* at Styrelsen for Samfundssikkerhed kan anvende nærmere angivne håndhævelsesforanstaltninger over for en væsentlig teleudbyder.

Den foreslåede bestemmelse vil gennemføre artikel 32, stk. 4, litra a-h, i NIS 2-direktivet, for så vidt angår telesektoren.

Den foreslåede bestemmelse svarer med sproglige tilpasninger uden indholdsmæssig betydning til NIS 2-direktivets artikel 32, stk. 4, litra a-h, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Efter bestemmelsen får Styrelsen for Samfundssikkerhed mulighed for at udstede advarsler, bindende instrukser, påbud og forbud.

Det bemærkes i den forbindelse, at det følger af NIS 2-direktivets artikel 32, stk. 1, at de håndhævelsesforanstaltninger, der anvendes overfor væsentlige teleudbydere i medfør

af den foreslåede bestemmelse, skal være effektive, stå i et rimeligt forhold til overtrædelsen og have en afskrækkende virkning under hensyntagen til omstændighederne i hver enkelt sag.

Det følger af den foreslåede bestemmelse, at Styrelsen for Samfundssikkerhed skal foretage en konkret vurdering af omstændighederne i hver enkelt sag, når styrelsen anvender håndhævelsesforanstaltningerne over for væsentlige teleudbydere, således at proportionalitetsprincippet overholdes ved valg mellem de oplistede håndhævelsesmuligheder.

Styrelsen for Samfundssikkerhed skal derfor i overensstemmelse med NIS 2-direktivets artikel 32, stk. 7, litra a, tage hensyn til 1) overtrædelsens grovhed og vigtigheden af de overtrådte bestemmelser, idet bl.a. følgende under alle omstændigheder skal betragtes som alvorlige overtrædelser: a) Gentagne overtrædelser, b) manglende underretning om eller afhjælpning af væsentlige hændelser, c) manglende afhjælpning af mangler efter bindende instrukser fra Styrelsen for Samfundssikkerhed, d) hindringer for audits eller overvågningsaktiviteter beordret af Styrelsen for Samfundssikkerhed efter konstatering af en overtrædelse, og e) afgivelse af urigtige eller klart unøjagtige oplysninger vedrørende cybersikkerhedsrisikostyringsforanstaltninger eller rapporteringsforpligtelser, 2) overtrædelsens varighed, 3) den pågældende udbyders relevante tidligere overtrædelser, 4) enhver fysisk eller ikke fysisk skade, der er forårsaget, herunder ethvert finansielt eller økonomisk tab, virkninger for andre tjenester og antallet af brugere, der er berørt, 5) hvorvidt der ved overtrædelsen er handlet forsætligt eller uagtsomt, 6) enhver foranstaltning truffet af udbyderen for at forebygge eller afbøde den fysisk eller ikke fysisk skade, 7) hvorvidt godkendte adfærdskodekser eller godkendte certificeringsmekanismer er overholdt, og 8) i hvilken udstrækning de fysiske eller juridiske personer, der holdes ansvarlige for overtrædelsen, samarbejder med Styrelsen for Samfundssikkerhed.

Det følger endvidere af NIS 2-direktivets artikel 32, stk. 7, at den kompetente myndighed ved anvendelsen af håndhævelsesforanstaltninger skal overholde retten til forsvar. Dette sikres ved, at et påbud eller forbud efter den foreslåede § 22 vil være omfattet af forvaltningslovens almindelige regler, herunder bestemmelserne i kapitel 3 (om vejledning og repræsentation mv.), kapitel 5 (om partshøring), kapitel 6 (om begrundelse mv.) og kapitel 7 (om klagevejledning).

Derudover vil der være mulighed for at indbringe afgørelserne for domstolene.

Der vil i forbindelse med en afgørelse om påbud eller forbud efter den foreslåede § 20, nr. 3-6 og 8 blive fastsat en frist, inden for hvilken udbyderen skal efterkomme indholdet i afgørelsen.

En væsentlig teleudbyder, der modtager en afgørelse om påbud eller forbud efter den foreslåede § 20, nr. 3-6 og 8, vil også kunne ifalde straf for en eventuel overtrædelse af denne lov eller regler udstedt i medfør af loven, jf. stk. 1, nr. 3.

Det følger af det foreslåede *nr. 1,* at Styrelsen for Samfundssikkerhed kan udstede advarsler om teleudbyderens overtrædelse af kapitel 2-4, og regler udstedt i medfør af bestemmelser i disse kapitler.

Den foreslåede bestemmelse vil give Styrelsen for Samfundssikkerhed mulighed for at udstede advarsler om enhedens overtrædelse af loven. Der er tale om den mildeste form for håndhævelsesforanstaltning, som kan tages i brug af Styrelsen for Samfundssikkerhed.

Det følger af den foreslåede *nr. 2,* at Styrelsen for Samfundssikkerhed kan udstede bindende instrukser, herunder vedrørende foranstaltninger, der er nødvendige for at forhindre eller afhjælpe en hændelse, samt frister for gennemførelse af sådanne foranstaltninger og for rapportering om deres gennemførelse eller pålægge de pågældende enheder at afhjælpe de konstaterede mangler eller overtrædelserne af denne lov.

Den foreslåede bestemmelse vil indebære, at Styrelsen for Samfundssikkerhed vil kunne udstede bindende instrukser, herunder vedrørende foranstaltninger, der er nødvendige for at forhindre eller afhjælpe en hændelse. Det forudsættes, at den kompetente myndighed vil meddele enheden en frist for gennemførelse af nødvendige foranstaltninger, og for rapportering om foranstaltningernes gennemførelse.

Det bemærkes, at der vil være tale om en forvaltningsretlig afgørelse, hvorfor forvaltningslovens regler herom vil finde anvendelse.

Det følger af den foreslåede *nr. 3,* at Styrelsen for Samfundssikkerhed vil kunne påbyde udbyderen at træffe foranstaltninger, der er nødvendige for at forhindre eller afhjælpe en hændelse.

Den foreslåede bestemmelse vil medføre, at Styrelsen for Samfundssikkerhed vil kunne påbyde en enhed at træffe foranstaltninger, der er nødvendige for at forhindre eller afhjælpe en hændelse. Det bemærkes, at denne håndhævelsesforanstaltning vil anses for mere indgribende end en bindende instruks.

Det bemærkes, at der vil være tale om en forvaltningsretlig afgørelse, hvorfor forvaltningslovens regler herom vil finde anvendelse.

Det følger af det foreslåede *nr. 4,* at Styrelsen for Samfundssikkerhed kan meddele udbyderen påbud og forbud for at sikre overholdelsen af de krav, der er fastsat i lovens kapitel 2-4, og regler udstedt i medfør af bestemmelser i disse kapitler

Det bemærkes, at en advarsel efter nr. 1, vil være mildere tilsynsforanstaltning end et påbud.

I tilfælde af, at en udbyder eksempelvis ikke lever op til de

krav, der er fastsat i loven, vil Styrelsen for Samfundssikkerhed kunne angive, hvilke nærmere foranstaltninger udbyderen skal træffe. Det kan eksempelvis være organisatoriske foranstaltninger vedrørende passende rolle- og ansvarsfordeling, herunder forbud mod ansvarssammenfald, samt procedurer i relation til erhvervelse og udvikling af net- og informationssystemer, tekniske foranstaltninger vedrørende sikkerhedskopiering af data eller om udbyderens anvendelse af bestemte logningsmetoder.

Det følger af det foreslåede *nr. 5,* at Styrelsen for Samfundssikkerhed kan påbyde udbyderen at underrette de fysiske eller juridiske personer, til hvilke udbyderen leverer tjenester eller udfører aktiviteter, som potentielt kan være berørt af en væsentlig hændelse, om denne trussels karakter samt om eventuelle beskyttelsesforanstaltninger eller afhjælpende foranstaltninger, som de fysiske eller juridiske personer kan træffe som reaktion på denne trussel.

Bestemmelsen skal ses i sammenhæng med den foreslåede bestemmelse i § 11, stk. 2, som indeholder en forpligtelse for væsentlige teleudbydere og vigtige teleudbydere til i relevant omfang at underrette modtagerne af deres tjenester, som potentielt er berørt af en væsentlig cybertrussel, om eventuelle foranstaltninger eller modforholdsregler, som modtagerne kan træffe som reaktion på den pågældende trussel. Hvor det er relevant, skal udbyderne også informere de pågældende modtagere om den væsentlige cybertrussel.

Med den foreslåede bestemmelse vil Styrelsen for Samfundssikkerhed kunne påbyde, at der skal foretages underretning af modtagerne af udbyderens tjenester, uanset om udbyderen selv vurderer, at det er relevant.

Det følger af det foreslåede *nr. 6,* at Styrelsen for Samfundssikkerhed kan påbyde udbyderen at gennemføre de anbefalinger, der er fremsat i forbindelse med en gennemført sikkerhedsaudit.

Bestemmelsen skal ses i sammenhæng med den foreslåede § 19, stk. 1, nr. 2, hvorefter Styrelsen for Samfundssikkerhed kan foretage regelmæssige og målrettede sikkerhedsaudits eller stille krav om, at den væsentlige teleudbyder får et kvalificeret uafhængigt organ til at foretage disse audits, samt den foreslåede § 19, stk. 1, nr. 3, hvorefter Styrelsen for Samfundssikkerhed kan foretage sikkerhedsaudits ad hoc.

Det følger af det foreslåede *nr. 7,* at Styrelsen for Samfundssikkerhed kan udpege en person med ansvar for i en nærmere fastsat periode at føre tilsyn med udbyderens overholdelse af lovens kapitel 2 og 3 samt regler udstedt i medfør heraf.

Styrelsen for Samfundssikkerhed vil enten kunne udpege en ansat eller en ekstern person. Det forudsættes, at den pågældende person har de nødvendige kvalifikationer til at udføre opgaven. Den pågældende person vil skulle monitorere udbyderens overholdelse af krav til foranstaltninger til styring af cybersikkerhedsrisici i medfør af den foreslåede § 5 og udbyderens overholdelse af oplysnings- og underretningspligterne i de foreslåede § 8, § 9, § 11 og § 12, samt regler udstedt i medfør af de nævnte bestemmelser.

Det følger af det foreslåede *nr. 8,* at Styrelsen for Samfundssikkerhed kan påbyde udbyderen i ikke-anonymiseret form og på en nærmere angiven måde at offentliggøre afgørelser om håndhævelsesforanstaltninger efter nr. 1-5 samt resumeer af domme eller bødevedtagelser, hvor der idømmes eller vedtages en bøde.

I overensstemmelse med principperne i betænkning nr. 1516 om offentlige myndigheders offentliggørelse af kontrolresultater, afgørelser mv. forudsættes det, at Styrelsen for Samfundssikkerhed ved beslutningen om, hvilke oplysninger en udbyder pålægges at offentliggøre, i fornødent omfang bl.a. iagttager de hensyn til fortrolighed, der fremgår af forvaltningslovens § 27 om offentlig ansattes tavshedspligt, herunder bl.a. hensynene til enkeltpersoners private forhold, forretningshemmeligheder samt forebyggelse, efterforskning og forfølgning af lovovertrædelser.

Til § 21

Det foreslås i *stk. 1*, *1. pkt.,* at hvis én eller flere af de håndhævelsesforanstaltninger, der er pålagt i medfør af § 20 nr. 1-8, har vist sig at være utilstrækkelige, kan Styrelsen for Samfundssikkerhed fastsætte en frist, inden for hvilken den væsentlige teleudbyder skal foretage de nødvendige tiltag for at afhjælpe manglerne eller opfylde Styrelsen for Samfundssikkerheds krav.

Det foreslås i *stk. 1, 2. pkt. ,* at er manglerne ikke afhjulpet eller Styrelsen for Samfundssikkerheds krav ikke opfyldt inden for den fastsatte frist, kan Styrelsen for Samfundssikkerhed træffe afgørelse om 1) midlertidigt at suspendere en certificering eller godkendelse vedrørende dele af eller alle de relevante tjenester, udbyderen leverer, eller aktiviteter, der udføres af udbyderen og 2) midlertidigt at forbyde enhver fysisk person med ledelsesansvar på niveau med administrerende direktør eller den juridiske repræsentant hos udbyderen at udøve ledelsesfunktioner ved den pågældende udbyder.

Bestemmelsen vil gennemføre artikel 32, stk. 5, 1. led, i NIS 2-direktivet, for så vidt angår telesektoren. Det følger af bestemmelsen, at medlemsstaterne skal sikre, at de kompetente myndigheder i en situation, hvor håndhævelsesforanstaltninger anvendt i medfør af direktivets artikel 32, stk. 4, litra a-d og f, er virkningsløse, skal have beføjelse til at fastsætte en frist, inden for hvilken den væsentlige enhed skal tage de nødvendige tiltag for at afhjælpe manglerne eller opfylde myndighedernes krav. Hvis de ønskede tiltag ikke tages inden for den fastsatte frist, skal de kompetente myndigheder have beføjelse til a) midlertidigt at suspendere, eller anmode et certificerings- eller godkendelsesorgan eller en domstol om i overensstemmelse med national ret midlertidigt at suspendere en certificering eller godkendelse vedrørende dele af eller alle de relevante tjenester, der leveres, eller aktiviteter, der udføres af en væsentlig enhed og b) at anmode

de relevante organer eller domstole om i overensstemmelse med national ret midlertidigt at forbyde enhver fysisk person med ledelsesansvar på direktionsniveau eller som juridisk repræsentant i den pågældende væsentlige enhed at udøve ledelsesfunktioner i den pågældende enhed.

Det bemærkes, at de eksisterende muligheder for rettighedsfrakendelse i straffeloven ikke vurderes tilstrækkelige til at sikre korrekt og tilstrækkelig gennemførelse af bestemmelsen i direktivet. Det skyldes navnlig, at rettighedsfrakendelse i medfør af straffelovens § 79 alene kan ske i forbindelse med dom for strafbart forhold, og hvis det udviste forhold begrunder en nærliggende fare for misbrug af stillingen.

Det vil være en forudsætning for at anvende bestemmelsen, at håndhævelsesforanstaltninger pålagt i medfør af den foreslåede § 20, nr. 1-8, har vist sig at være utilstrækkelige. Det er dermed en forudsætning, at mindre indgribende midler har været forsøgt og vist sig utilstrækkelige til at sikre, at udbyderen foretager de nødvendige tiltag for at afhjælpe mangler, som Styrelsen for Samfundssikkerhed har konstateret, eller opfylder styrelsens krav.

Bestemmelsen vil skulle anvendes i overensstemmelse med direktivets forudsætninger som udtrykt i præambelbetragtning nr. 133, hvorefter bestemmelsen kun bør anvendes som en sidste udvej, dvs. først efter at de øvrige, relevante håndhævelsesforanstaltninger er udtømt. Det fremgår videre af samme præambelbetragtning, at i betragtning af deres alvor og indvirkning på enhedernes aktiviteter og i sidste ende brugerne, bør sådanne midlertidige suspensioner eller forbud kun anvendes proportionalt med overtrædelsens alvor og under hensyntagen til omstændighederne i hvert enkelt tilfælde, herunder i lyset af om overtrædelsen var forsætlig eller uagtsom, og ethvert tiltag der er iværksat for at forebygge eller afbøde den fysisk eller ikke fysisk skade.

Styrelsen for Samfundssikkerhed vil efter omstændighederne og i relevant omfang kunne træffe afgørelse om anvendelse af flere håndhævelsesforanstaltninger på én gang. Der er således ikke i medfør af den foreslåede § 21 et krav om, at relevante håndhævelsesforanstaltninger anvendes tidsmæssigt forskudt af hinanden, såfremt det vurderes, at flere foranstaltninger i kombination er nødvendige for at sikre, at reglerne efterleves.

Der vil efter bestemmelsen skulle fastsættes en nærmere angivet frist, inden for hvilken den væsentlige teleudbyder skal have truffet de nødvendige tiltag for at afhjælpe manglerne eller opfylde Styrelsen for Samfundssikkerheds krav. Varigheden af fristen vil afhænge af en konkret vurdering, som foretages af Styrelsen for Samfundssikkerhed.

Det foreslås, at afgørelse om suspension eller forbud træffes af Styrelsen for Samfundssikkerhed i første instans. Det skal ses i lyset af, at muligheden for suspension og forbud ligger i forlængelse af Styrelsen for Samfundssikkerheds øvrige håndhævelsesmuligheder, og at der i en afgørelse om suspension eller forbud forudsættes at skulle indgå en begrundelse for, hvorfor allerede pålagte håndhævelsesforanstaltninger er utilstrækkelige.

Det følger af NIS 2-direktivets artikel 32, stk. 7, at den kompetente myndighed ved anvendelsen af håndhævelsesforanstaltninger såsom suspension eller forbud efter den foreslåede bestemmelse skal tage hensyn til en række nærmere angivne forhold.

I direktivets artikel 32, stk. 7, er følgende hensyn oplistet: 1) overtrædelsens grovhed og vigtigheden af de overtrådte bestemmelser, idet bl.a. følgende under alle omstændigheder skal betragtes som alvorlige overtrædelser: a) gentagne overtrædelser, b) manglende underretning om eller afhjælpning af væsentlige hændelser, c) manglende afhjælpning af mangler efter bindende instrukser fra kompetente myndigheder, d) hindringer for audits eller overvågningsaktiviteter beordret af den kompetente myndighed efter konstatering af en overtrædelse og e) afgivelse af urigtige eller klart unøjagtige oplysninger vedrørende cybersikkerhedsrisikostyringsforanstaltninger eller rapporteringsforpligtelser, 2) overtrædelsens varighed, 3) den pågældende enheds relevante tidligere overtrædelser, 4) enhver materiel eller immateriel skade, der er forårsaget, herunder ethvert finansielt eller økonomisk tab, virkninger for andre tjenester og antallet af brugere, der er berørt, 5) hvorvidt der ved overtrædelsen er handlet forsætligt eller uagtsomt, 6) enhver foranstaltning truffet af enheden for at forebygge eller afbøde den materielle eller immaterielle skade, 7) hvorvidt godkendte adfærdskodekser eller godkendte certificeringsmekanismer er overholdt, og 8) i hvilken udstrækning de fysiske eller juridiske personer, der holdes ansvarlige for overtrædelsen, samarbejder med de kompetente myndigheder.

Den foreslåede bestemmelse i stk. 1*, nr. 1,* indebærer, at såfremt den væsentlige teleudbyder ikke har iværksat tiltag for at afhjælpe manglerne eller efterkomme Styrelsen for Samfundssikkerheds krav inden for den fastsatte frist, kan Styrelsen for Samfundssikkerhed træffe afgørelse om midlertidigt at suspendere en certificering eller godkendelse vedrørende dele af eller alle de relevante tjenester, udbyderen leverer, eller aktiviteter, der udføres af udbyderen.

Den foreslåede bestemmelse skal læses i sammenhæng med den foreslåede bestemmelse i stk. 4, hvorefter Styrelsen for Samfundssikkerhed vil kunne fastsætte nærmere regler for, hvilke certificeringer og godkendelser, som bestemmelsen i stk. 1, nr. 1, finder anvendelse på. Det forudsættes, at den foreslåede bestemmelse i stk. 1, nr. 1, ikke anvendes, før bemyndigelsen i den foreslåede stk. 4, er anvendt.

En afgørelse efter nr. 1 vil være af midlertidig karakter, jf. også det foreslåede stk. 2, hvorefter afgørelsen kun kan anvendes, så længe den væsentlige teleudbyder ikke har truffet de nødvendige tiltag for at afhjælpe de mangler eller efterleve de krav fra Styrelsen for Samfundssikkerhed, som gav anledning til, at foranstaltningerne blev anvendt.

Den foreslåede bestemmelse i stk. 1*, nr. 2,* indebærer, at så-

fremt den væsentlige teleudbyder ikke har iværksat tiltag for at afhjælpe manglerne eller efterkomme Styrelsen for Samfundssikkerheds krav inden for den fastsatte frist, kan styrelsen træffe afgørelse om midlertidigt at forbyde enhver fysisk person med ledelsesansvar på niveau med administrerende direktør eller den juridiske repræsentant hos udbyderen at udøve ledelsesfunktioner ved den pågældende udbyder.

Det bemærkes hertil, at det af den danske oversættelse af NIS 2-direktivets artikel 32, stk. 5, litra b, bl.a. fremgår, at de personer med ledelsesansvar, der midlertidigt kan suspenderes, omfatter »enhver fysisk person med ledelsesansvar på direktionsniveau«. Denne oversættelse er efter Ministeriet for Samfundssikkerhed og Beredskabs opfattelse imidlertid ikke forenelig med den engelske udgave af direktivet, hvori »any natural person who is responsible for discharging managerial responsibilities at chief executive officer […] level« er anvendt. Den franske sprogversion anvender en tilsvarende formulering som den engelske. I den foreslåede bestemmelse anvendes på den baggrund betegnelsen »enhver fysisk person med ledelsesansvar på niveau med administrerende direktør«.

I det omfang en virksomhed eller organisation ikke har en administrerende direktør, vil bestemmelsen omfatte den øverste leder af den pågældende væsentlige teleudbyder, f.eks. en generalsekretær, direktør, koncernchef eller managing partner.

En afgørelse efter nr. 2 vil være af midlertidig karakter, jf. også det foreslåede stk. 2, hvorefter afgørelsen kun kan anvendes, så længe den væsentlige teleudbyder ikke har truffet de nødvendige tiltag for at afhjælpe de mangler eller opfylde de krav fra Styrelsen for Samfundssikkerhed, som gav anledning til, at foranstaltningerne blev anvendt.

Det følger af det foreslåede *stk. 2,* at suspensioner eller forbud, som er pålagt i medfør af stk. 1, kun kan anvendes, indtil den væsentlige teleudbyder træffer de nødvendige tiltag for at afhjælpe de mangler eller opfylde de krav, som gav anledning til, at foranstaltningerne i medfør af stk. 1 blev anvendt.

Den foreslåede bestemmelse vil gennemføre NIS 2-direktivets artikel 32, stk. 5, 1. led, for så vidt angår telesektoren. Det følger af 32, stk. 5, 1. led, at midlertidige suspensioner eller forbud, som er pålagt i henhold til dette stykke, kun anvendes, indtil den pågældende enhed træffer de nødvendige foranstaltninger til at afhjælpe manglerne eller opfylde den kompetente myndigheds krav, som gav anledning til, at disse håndhævelsesforanstaltninger blev anvendt.

Den foreslåede bestemmelse svarer med sproglige tilpasninger uden indholdsmæssig betydning til NIS 2-direktivets artikel 32, stk. 5, 1. led, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Bestemmelsen indebærer, at når Styrelsen for Samfundssikkerhed har truffet afgørelse om midlertidigt at suspendere en certificering eller midlertidigt har forbudt en fysisk person med ledelsesansvar på niveau med administrerende direktør eller den juridiske repræsentant ved udbyderen at udøve ledelsesfunktioner ved den pågældende udbyder, skal styrelsen træffe afgørelse om at ophæve foranstaltningen, når udbyderen har truffet de nødvendige tiltag for at afhjælpe de mangler eller opfylde de krav, som gav anledning til, at foranstaltningen blev anvendt.

Det følger af det foreslåede *stk. 3,* at en afgørelse efter stk. 1 kan forlanges indbragt for domstolene af den væsentlige teleudbyder eller den fysiske person, afgørelsen vedrører. Styrelsen for Samfundssikkerhed anlægger i givet fald sag inden for rammerne af den civile retspleje mod den udbyder eller person, som har forlangt sagen indbragt.

Den foreslåede bestemmelse vil gennemføre NIS 2-direktivets artikel 32, stk. 5, 2. led, hvoraf det følger, at pålæggelse af midlertidige suspensioner eller forbud skal være underlagt passende proceduremæssige garantier i overensstemmelse med de generelle principper i EU-retten og chartret, herunder retten til effektive retsmidler og til en retfærdig rettergang, uskyldsformodningen og retten til et forsvar.

Det vil efter den foreslåede bestemmelse være muligt for den væsentlige teleudbyder eller den fysiske person, som afgørelsen om suspension eller forbud vedrører, at forlange afgørelsen indbragt for retten. Når en sådan sag indbringes for retten, vil bestemmelserne i retsplejeloven finde anvendelse, hvilket vil sikre de nødvendige retssikkerhedsgarantier.

Det følger af det foreslåede *stk. 4,* at ministeren for samfundssikkerhed kan fastsætte regler om, hvilke certificeringer og godkendelser der er omfattet af stk. 1, nr. 1.

Den foreslåede bestemmelse i stk. 4 indebærer, at Styrelsen for Samfundssikkerhed kan fastsætte nærmere regler om, hvilke certificeringer og godkendelser der er omfattet af den midlertidige suspensionsordning i § 21, stk. 1, nr. 1.

Ved at fastsætte nærmere regler i bekendtgørelsesform sikres det, at det vil være klart og forudsigeligt for de væsentlige teleudbydere, hvilke certificerings- og godkendelsesordninger, der vil kunne medføre suspension. Det sikres endvidere, at reglerne løbende kan tilpasses den udvikling, der er på området, f.eks. i tilfælde af, at der indføres en ny cybersikkerhedscertificering i EU-regi.

De nærmere regler vil skulle udarbejdes inden for den ramme, som det foreslåede stk. 1 udgør. Det indebærer bl.a., at reglerne vil skulle være i overensstemmelse med regeringens principper om minimumsimplementering. Det forudsættes, at den foreslåede bestemmelse i stk. 1, nr. 1, ikke anvendes, før bemyndigelsen i den foreslåede stk. 4, er anvendt.

Til § 22

Det foreslås i *stk. 1,* at Styrelsen for Samfundssikkerhed som led i sit tilsyn kan anvende nærmere angivne tilsynsforanstaltninger over for en vigtig teleudbyder.

I overensstemmelse med direktivets forudsætninger, som udtrykt i præambelbetragtning nr. 122, vil vigtige teleudbydere – i modsætning til væsentlige teleudbydere – ikke blive underlagt løbende tilsyn, men i stedet et lettere, reaktivt tilsyn. Det betyder, at tilsyn iværksættes på baggrund af oplysninger, der tyder på, at den pågældende enhed potentielt ikke efterlever sine forpligtelser efter loven og regler udstedt i medfør af loven, herunder eventuelt efter en væsentlig hændelse.

Vigtige teleudbydere vil således som udgangspunkt ikke være forpligtet til systematisk at dokumentere overholdelsen af foranstaltninger til styring af cybersikkerhedsrisici over for myndighederne, og de kompetente myndigheder vil ikke have en generel forpligtelse til at føre tilsyn med vigtige enheder.

Som forudsat i samme præambelbetragtning vil det reaktive tilsyn kunne iværksættes på baggrund af oplysninger, som Styrelsen for Samfundssikkerhed modtager fra andre myndigheder, enheder, borgere, medier eller andre kilder eller offentligt tilgængelige oplysninger. Det kan desuden eksempelvis være oplysninger, der hidrører fra andre aktiviteter, der indgår i de kompetente myndigheders udførelse af deres arbejdsopgaver.

Den foreslåede bestemmelse vil endvidere skulle forstås og anvendes i lyset af NIS 2-direktivets artikel 31, stk. 1, hvorefter medlemsstaterne sikrer, at deres kompetente myndigheder effektivt overvåger og træffer de nødvendige foranstaltninger til at sikre, at direktivet overholdes. Det følger endvidere af artikel 31, stk. 2, at medlemsstaterne kan tillade deres kompetente myndigheder at prioritere tilsynsopgaver. En sådan prioritering baseres på en risikobaseret tilgang. Med henblik herpå kan de kompetente myndigheder, når de udfører deres tilsynsopgaver i henhold til artikel 32 og 33, fastlægge tilsynsmetoder, der gør det muligt at prioritere sådanne opgaver efter en risikobaseret tilgang. De kompetente myndigheder vil således ved tilrettelæggelsen af et risikobaseret reaktivt tilsyn med vigtige enheder kunne lægge vægt på eksempelvis enhedernes samfundsmæssige betydning.

Anvendelsen af de forskellige tilsynsforanstaltninger, som opregnes i den foreslåede § 22, stk. 1, vil skulle ske efter en konkret vurdering af omstændighederne i hver enkelt sag. Valget af tilsynsforanstaltninger vil endvidere skulle ske i overensstemmelse med det forvaltningsretlige proportionalitetsprincip.

Det er Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at der for så vidt angår de foreslåede bestemmelser i nr. 4-7 og den del af bestemmelsen i nr. 2, der vedrører, at der kan stilles krav om, at udbyderen får et kvalificeret uafhængigt organ til at foretage sikkerhedsaudits, og at resultaterne herfor skal stilles til rådighed for Styrelsen for Samfundssikkerhed, vil være tale om oplysningspligter omfattet af lov om retssikkerhed ved forvaltningens anvendelse af tvangsindgreb og oplysningspligter. Dette indebærer bl.a., at kapitel 4 (om retten til ikke at inkriminere sig selv mv.) vil gælde i tilfælde, hvor der måtte være en konkret mistanke om, at en enhed har begået en overtrædelse af lovgivningen, der kan medføre straf. Der henvises i øvrigt til kapitel 4 i lov om retssikkerhed ved forvaltningens anvendelse af tvangsindgreb og oplysningspligter og bemærkningerne hertil. Der henvises til Folketingstidende 2003-04, tillæg A, side 3075-3078 og side 3096-3099.

I overensstemmelse med forudsætningerne i direktivets præambelbetragtning nr. 123 bør de kompetente myndigheders udførelse af tilsynsopgaver ikke unødigt hæmme den berørte enheds forretningsaktiviteter.

Det foreslås med *nr. 1,* at Styrelsen for Samfundssikkerhed uden retskendelse og behørig legitimation kan foretage kontrol hos teleudbydere samt deres samarbejdspartnere, leverandører eller underleverandører i relation til outsourcet aktivitet og eksternt efterfølgende tilsyn.

Den foreslåede bestemmelse vil gennemføre artikel 33, stk. 1 og 2, i NIS 2-direktivet.

Den foreslåede bestemmelse i stk. 1, nr. 1, vil endvidere videreføre § 9, stk. 6 og 7 i lov om sikkerhed i net og tjenester.

Ministeriet for Samfundssikkerhed og Beredskab finder det således henset til vurderingen af det aktuelle trusselsniveau mod telesektoren, jf. lovforslagets pkt. 1 ovenfor, væsentligt at opretholde det nuværende sikkerhedsniveau for sektoren. Der er med videreførelsen af bestemmelsen ikke tilsigtet materielle ændringer af bestemmelsens indhold.

For effektivt at kunne konstatere, om vigtige teleudbydere i praksis har gennemført de nødvendige foranstaltninger til at sikre deres net- og informationssystemer, er det nødvendigt, at Styrelsen for Samfundssikkerhed som led i et tilsyn har adgang til forretningssteder hos vigtige teleudbydere samt deres samarbejdspartnere, leverandører eller underleverandører i relation til outsourcet aktivitet og eksternt tilsyn. Det foreslås derfor, at der skal være adgang til kontrol på stedet uden retskendelse og mod behørig legitimation.

Den foreslåede bestemmelse vil betyde, at Styrelsen for Samfundssikkerhed som led i et tilsyn kan foretage kontrol på stedet til enhver tid. Det forudsættes dog almindeligvis, at Styrelsen for Samfundssikkerhed forinden et kontrolbesøg vil varsle den vigtige enhed herom.

Det bemærkes, at Styrelsen for Samfundssikkerhed ikke i forbindelse med adgang til forretningslokaler efter stk. 1, kan tilgå kommunikation til, fra eller mellem udbyderens kunder.

Styrelsen for Samfundssikkerhed vil ikke i forbindelse med tilsynsbesøgene kunne få adgang til elektronisk kommunikation til, fra og mellem udbydernes kunder, ligesom styrelsen alene vil kunne foretage tilsynsbesøg i det omfang, udbyderens forretningslokaler er placeret i Danmark.

Det fremgår desuden af NIS 2-direktivets artikel 33, stk. 2, litra a, at der kan foretages »eksternt efterfølgende tilsyn«, hvilket er en formulering, der efter Ministeriet for Samfundssikkerhed og Beredskabs opfattelse kan give anledning til fortolkningstvivl i dansk sammenhæng. I den engelske sprogversion af NIS 2-direktivet anvendes formuleringen »off-site *ex post* supervision«. Efter Ministeriet for Samfundssikkerhed og Beredskabs opfattelse udgør eksternt efterfølgende tilsyn forstået som off-site ex post supervision et reaktivt tilsyn fra en kompetent myndighed uden fysisk tilstedeværelse *på stedet*, men eksempelvis udført på skriftligt grundlag. Det bemærkes, at de kompetente myndigheder i medfør af den foreslåede bestemmelse kan kræve relevante oplysninger fra enhederne. Det indebærer også, at de kompetente myndigheder kan kræve at få udleveret nødvendige oplysninger til afgørelse af, om et forhold er omfattet af loven eller regler udstedt i medfør af loven.

Det foreslås i *nr. 2,* at Styrelsen for Samfundssikkerhed kan foretage regelmæssige og målrettede sikkerhedsaudits eller stille krav om, at udbyderen får et kvalificeret uafhængigt organ til at foretage disse audits, og at resultaterne heraf stilles til rådighed for Styrelsen for Samfundssikkerhed,

Den foreslåede bestemmelse vil gennemføre artikel 33, stk. 1 og 2, i NIS 2-direktivet. Den foreslåede bestemmelse svarer med sproglige tilpasninger uden indholdsmæssig betydning til NIS 2-direktivets artikel 33, stk. 1 og 2, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Efter direktivets artikel 33, stk. 2, 2. led, baseres de målrettede sikkerhedsaudits, der er omhandlet i første led, litra b, på risikovurderinger foretaget af den kompetente myndighed eller den reviderede enhed eller på andre tilgængelige risikorelaterede oplysninger. Resultaterne af enhver målrettet sikkerhedsaudit stilles til rådighed for den kompetente myndighed. Omkostningerne ved en sådan målrettet sikkerhedsaudit, der udføres af et uafhængigt organ, afholdes af den reviderede enhed, undtagen i behørigt begrundede tilfælde, når den kompetente myndighed bestemmer andet.

Det foreslås i *nr. 3,* at Styrelsen for Samfundssikkerhed kan foretage sikkerhedsscanninger.

Den foreslåede bestemmelse vil gennemføre artikel 33, stk. 1 og 2, i NIS 2-direktivet. Den foreslåede bestemmelse svarer med sproglige tilpasninger uden indholdsmæssig betydning til NIS 2-direktivets artikel 33, stk. 1 og 2, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Det foreslås i *nr. 4,* at Styrelsen for Samfundssikkerhed kan kræve at få udleveret oplysninger, der er nødvendige for efterfølgende at vurdere de foranstaltninger til styring af sikkerhedsrisici, som den berørte udbyder har indført.

Den foreslåede bestemmelse vil gennemføre artikel 33, stk. 1 og 2, i NIS 2-direktivet. Den foreslåede bestemmelse svarer med sproglige tilpasninger uden indholdsmæssig betydning til NIS 2-direktivets artikel 33, stk. 1 og 2, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Det foreslås i *nr. 5,* at Styrelsen for Samfundssikkerhed kan kræve at få adgang til data, dokumenter og oplysninger, der er nødvendige for udførelsen af tilsynsopgaven, herunder til afgørelse af, om et forhold er omfattet af denne lov eller regler udstedt i medfør af loven.

Den foreslåede bestemmelse vil gennemføre artikel 33, stk. 1 og 2, i NIS 2-direktivet. Den foreslåede bestemmelse svarer med sproglige tilpasninger uden indholdsmæssig betydning til NIS 2-direktivets artikel 33, stk. 1 og 2, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Det foreslås i *nr. 6,* at Styrelsen for Samfundssikkerhed kan kræve at få udleveret dokumentation for gennemførelsen af sikkerhedspolitikker.

Den foreslåede bestemmelse vil gennemføre artikel 33, stk. 1 og 2, i NIS 2-direktivet. Den foreslåede bestemmelse svarer med sproglige tilpasninger uden indholdsmæssig betydning til NIS 2-direktivets artikel 33, stk. 1 og 2, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Det foreslås i *nr. 7,* at Styrelsen for Samfundssikkerhed kan kræve at få skriftlige udtalelser og redegørelser om faktisk forhold af betydning for Styrelsen for Samfundssikkerheds tilsynsvirksomhed.

Den foreslåede bestemmelse vil gennemføre artikel 33, stk. 1 og 2, i NIS 2-direktivet. Den foreslåede bestemmelse svarer med sproglige tilpasninger uden indholdsmæssig betydning til NIS 2-direktivets artikel 33, stk. 1 og 2, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Det er Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at der for de foreslåede tilsynsforanstaltninger vil være tale om et indgreb, der er omfattet af lov om retssikkerhed ved forvaltningens anvendelse af tvangsindgreb og oplysningspligter. Dette indebærer, at retten til ikke at inkriminere sig selv, jf. kapitel 4 i nævnte lov, skal overholdes. Det bemærkes dog, at det af bemærkningerne til § 10 i lov om retssikkerhed ved forvaltningens anvendelse af tvangsindgreb og oplysningspligter fremgår, at »[b]estemmelsen [om forbud mod selvinkriminering] er ikke til hinder for, at den mistænkte kan pålægges at give (faktuelle) oplysninger, som er uden betydning for bedømmelsen af, hvorvidt den pågældende har begået en lovovertrædelse, der kan medføre straf.«

Det følger af det foreslåede *stk. 2,* at de Styrelsen for Samfundssikkerhed ved anvendelsen af tiltagene i stk. 1, nr. 4-7, skal Styrelsen for Samfundssikkerhed angive formålet med tiltaget og præcisere, hvilke oplysninger der kræves

udleveret og hvordan og i hvilken form oplysningerne og materialet nævnt i stk. 1, nr. 4-7, skal udleveres.

Den foreslåede bestemmelse indebærer, at Styrelsen for Samfundssikkerhed i forbindelse med, at der stilles krav om udlevering af oplysninger eller materiale efter de foreslåede bestemmelser i stk. 1, nr. 4-7 samtidig kan kræve, at oplysningerne eller materialet udleveres på en bestemt måde, på et bestemt sprog og i en bestemt form.

Der vil eksempelvis kunne stilles krav om anvendelse af bestemte skemaer, eller at der skal foretages indtastninger på en hjemmeside.

Den foreslåede bestemmelse vil gennemføre NIS 2-direktivets artikel 33, stk. 3, hvorefter de kompetente myndigheder ved udøvelsen af deres beføjelser i henhold til artikel 33, stk. 2, litra d, e, og f, skal angive formålet med anmodningen og præcisere, hvilke oplysninger der anmodes om.

Til § 23

Det foreslås i *stk. 1*, at Styrelsen for Samfundssikkerhed kan anvende følgende håndhævelsesforanstaltninger over for en vigtig teleudbyder: 1) udstede advarsler om teleudbyderens overtrædelse af kapitel 2-4 og regler udstedt i medfør heraf, 2) udstede bindende instrukser, herunder vedrørende foranstaltninger, der er nødvendige for at forhindre eller afhjælpe en hændelse, samt frister for gennemførelse af sådanne foranstaltninger og for rapportering om deres gennemførelse eller pålægge de pågældende enheder at afhjælpe de konstaterede mangler eller overtrædelserne af denne lov, 3) meddele udbyderen påbud og forbud for at sikre overholdelsen af de krav, der er fastsat i loven eller regler udstedt i medfør af loven, 4) påbyde udbyderen at underrette de fysiske eller juridiske personer, til hvilke udbyderen leverer tjenester eller udfører aktiviteter, som potentielt kan være berørt af en væsentlig cybertrussel, om denne trussels karakter samt om eventuelle beskyttelsesforanstaltninger eller afhjælpende foranstaltninger, som de fysiske eller juridiske personer kan træffe som reaktion på denne trussel, 5) påbyde udbyderen at gennemføre de anbefalinger, der er fremsat i forbindelse med en gennemført sikkerhedsaudit, og 6) påbyde udbyderen i ikke-anonymiseret form og på en nærmere angiven måde at offentliggøre afgørelser om håndhævelsesforanstaltninger efter nr. 1-3 samt resumeer af domme eller bødevedtagelser, hvor der idømmes eller vedtages en bøde.

Den foreslåede bestemmelse vil gennemføre artikel 33, stk. 1 og 2, i NIS 2-direktivet.

Den foreslåede bestemmelse vil gennemføre artikel 33, stk. 4, litra a-g, i NIS 2-direktivet for så vidt angår telesektoren.

Den foreslåede bestemmelse svarer med sproglige tilpasninger uden indholdsmæssig betydning til NIS 2-direktivets artikel 33, stk. 4, litra a-g, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Det bemærkes i den forbindelse, at det følger af NIS 2-direktivets artikel 32, stk. 1, at de håndhævelsesforanstaltninger, der anvendes overfor væsentlige teleudbydere i medfør af den foreslåede bestemmelse, skal være effektive, stå i et rimeligt forhold til overtrædelsen og have en afskrækkende virkning under hensyntagen til omstændighederne i hver enkelt sag.

Det følger af den foreslåede bestemmelse, at Styrelsen for Samfundssikkerhed skal foretage en konkret vurdering af omstændighederne i hver enkelt sag, når centret anvender håndhævelsesforanstaltningerne over for væsentlige teleudbydere, således at proportionalitetsprincippet overholdes ved valg mellem de oplistede håndhævelsesmuligheder.

De foranstaltninger, der anvendes i forhold til vigtige teleudbydere skal i overensstemmelse med NIS 2-direktivets artikel 33, stk. 1, være effektive, stå i rimeligt forhold til overtrædelsen og have en afskrækkende virkning under hensyntagen til omstændighederne i hver enkelt sag.

Det følger af den foreslåede bestemmelse, at Styrelsen for Samfundssikkerhed skal foretage en konkret vurdering af omstændighederne i hver enkelt sag, når centret anvender håndhævelsesforanstaltningerne over for vigtige udbydere. Styrelsen for Samfundssikkerhed skal derfor i overensstemmelse med NIS 2-direktivets artikel 32, stk. 7, litra a, jf. artikel 33, stk. 5, tage hensyn til: 1) overtrædelsens grovhed og vigtigheden af de overtrådte bestemmelser, idet bl.a. følgende under alle omstændigheder skal betragtes som alvorlige overtrædelser: a) gentagne overtrædelser, b) manglende underretning om eller afhjælpning af væsentlige hændelser, c) manglende afhjælpning af mangler efter bindende instrukser fra Styrelsen for Samfundssikkerhed, d) hindringer for audits eller overvågningsaktiviteter beordret af Styrelsen for Samfundssikkerhed efter konstatering af en overtrædelse, og e) afgivelse af urigtige eller klart unøjagtige oplysninger vedrørende cybersikkerhedsrisikostyringsforanstaltninger eller rapporteringsforpligtelser, der er fastsat i § 5 og §§ 11-14, 2) overtrædelsens varighed, 3) den pågældende udbyders relevante tidligere overtrædelser, 4) enhver fysisk eller ikke fysisk skade, der er forårsaget, herunder ethvert finansielt eller økonomisk tab, virkninger for andre tjenester og antallet af brugere, der er berørt, 5) hvorvidt der ved overtrædelsen er handlet forsætligt eller uagtsomt, 6) enhver foranstaltning truffet af udbyderen for at forebygge eller afbøde den fysisk eller ikke fysisk skade, 7) hvorvidt godkendte adfærdskodekser eller godkendte certificeringsmekanismer er overholdt, og 8) i hvilken udstrækning de fysiske eller juridiske personer, der holdes ansvarlige for overtrædelsen, samarbejder med Styrelsen for Samfundssikkerhed.

Det følger endvidere af NIS 2-direktivets artikel 32, stk. 7, at en kompetent myndighed ved anvendelsen af håndhævelsesforanstaltninger skal overholde retten til forsvar. Dette sikres ved, at et påbud eller forbud efter den foreslåede § 25, vil være omfattet af forvaltningslovens almindelige regler, herunder bestemmelserne i kapitel 3 (om vejledning og repræsentation mv.), kapitel 5 (om partshøring), kapitel 6 (om begrundelse mv.) og kapitel 7 (om klagevejledning). Der-

udover vil der være mulighed for at påklage afgørelsen i medfør af det ulovbestemte princip om administrativ rekurs, ligesom afgørelsen vil kunne indbringes for domstolene.

Der vil i forbindelse med en afgørelse om påbud eller forbud efter den foreslåede § 23 blive fastsat en frist, inden for hvilken udbyderen skal overholde indholdet i afgørelsen.

Det følger af det foreslåede *nr. 1,* at Styrelsen for Samfundssikkerhed kan udstede advarsler om teleudbyderens overtrædelse af kapitel 2-4, og regler udstedt i medfør heraf.

Den foreslåede bestemmelse indebærer, at Styrelsen for Samfundssikkerhed kan udstede advarsler om teleudbyderens overtrædelse af kapitel 2-4, og regler udstedt i medfør heraf.

Det følger af den foreslåede *nr. 2,* at Styrelsen for Samfundssikkerhed kan udstede bindende instrukser, herunder vedrørende foranstaltninger, der er nødvendige for at forhindre eller afhjælpe en hændelse, samt frister for gennemførelse af sådanne foranstaltninger og for rapportering om deres gennemførelse eller pålægge de pågældende enheder at afhjælpe de konstaterede mangler eller overtrædelserne af denne lov.

Det følger af det foreslåede *nr. 3,* at Styrelsen for Samfundssikkerhed kan meddele udbyderen påbud og forbud for at sikre overholdelsen af de krav, der er fastsat i loven eller regler udstedt i medfør af loven.

I tilfælde af, at udbyderen ikke lever op til de krav, der er fastsat i loven, vil Styrelsen for Samfundssikkerhed eksempelvis kunne angive, hvilke nærmere foranstaltninger udbyderen skal træffe. Det kan eksempelvis være organisatoriske foranstaltninger vedrørende passende rolle- og ansvarsfordeling, herunder forbud mod ansvarssammenfald eller procedurer i relation til erhvervelse og udvikling af net- og informationssystemer, tekniske foranstaltninger vedrørende sikkerhedskopiering af data, eller om udbyderens anvendelse af bestemte logningsmetoder.

Det følger af det foreslåede *nr. 4,* at Styrelsen for Samfundssikkerhed kan påbyde udbyderen at underrette de fysiske eller juridiske personer, til hvilke udbyderen leverer tjenester eller udfører aktiviteter, som potentielt kan være berørt af en væsentlig cybertrussel, om denne trussels karakter samt om eventuelle beskyttelsesforanstaltninger eller afhjælpende foranstaltninger, som de fysiske eller juridiske personer kan træffe som reaktion på denne trussel.

Bestemmelsen skal ses i sammenhæng med den foreslåede bestemmelse i § 12, stk. 2, som indeholder en forpligtelse for væsentlige teleudbydere og vigtige teleudbydere til i relevant omfang at underrette modtagerne af deres tjenester, som potentielt er berørt af en væsentlig cybertrussel, om eventuelle foranstaltninger eller modforholdsregler, som modtagerne kan træffe som reaktion på den pågældende trussel. Hvor det er relevant, skal udbyderne også informere de pågældende modtagere om den væsentlige cybertrussel.

Med det foreslåede nr. 4 vil Styrelsen for Samfundssikkerhed kunne påbyde, at der skal foretages underretning af modtagerne af udbyderens tjenester, uanset om udbyderen selv vurderer, at det er relevant.

Det følger af det foreslåede *nr. 5,* at Styrelsen for Samfundssikkerhed kan påbyde udbyderen at gennemføre de anbefalinger, der er fremsat i forbindelse med en gennemført sikkerhedsaudit.

Bestemmelsen skal ses i sammenhæng med den foreslåede § 22, stk. 1, nr. 2, hvorefter Styrelsen for Samfundssikkerhed kan foretage målrettede sikkerhedsaudits eller stille krav om, at udbyderen får et kvalificeret uafhængigt organ til at foretage disse audits.

Det følger af det foreslåede *nr. 6,* at Styrelsen for Samfundssikkerhed kan påbyde udbyderen i ikke-anonymiseret form og på en nærmere angiven måde at offentliggøre afgørelser om håndhævelsesforanstaltninger efter nr. 1-3 samt resumeer af domme eller bødevedtagelser, hvor der idømmes eller vedtages en bøde.

I overensstemmelse med principperne i betænkning nr. 1516 om offentlige myndigheders offentliggørelse af kontrolresultater, afgørelser mv. forudsættes det, at den kompetente myndighed ved beslutningen om, hvilke oplysninger en enhed pålægges at offentliggøre, i fornødent omfang bl.a. iagttager de hensyn til fortrolighed, der fremgår af forvaltningslovens § 27 om offentligt ansattes tavshedspligt, herunder bl.a. hensynene til enkeltpersoners private forhold, forretningshemmeligheder samt forebyggelse, efterforskning og forfølgning af lovovertrædelser.

Til § 24

Det følger af den foreslåede *§ 24,* at inden Styrelsen for Samfundssikkerhed træffer afgørelse om at anvende håndhævelsesforanstaltninger efter §§ 20, 21 og 23, underrettes den berørte væsentlige eller vigtige teleudbyder om de påtænkte håndhævelsesforanstaltninger og begrundelsen herfor. Styrelsen for Samfundssikkerhed skal give udbyderen en rimelig frist til at fremsætte bemærkninger, undtagen i tilfælde hvor formålet med foranstaltningen ellers ville forspildes.

Den foreslåede bestemmelse vil gennemføre artikel 32, stk. 8, NIS 2-direktivet, for så vidt angår telesektoren. Artikel 32, stk. 8, fastsætter, at de kompetente myndigheder giver en detaljeret begrundelse for deres håndhævelsesforanstaltninger. Inden de kompetente myndigheder træffer sådanne foranstaltninger, underretter de kompetente myndigheder de berørte enheder om deres foreløbige resultater. De giver også disse enheder en rimelig frist til at fremsætte bemærkninger, undtagen i behørigt begrundede tilfælde, hvor øjeblikkelige foranstaltninger til at forebygge eller reagere på hændelser ellers ville blive hindret. Det bemærkes, at artikel 32, stk. 8, også finder anvendelse på vigtige enheder, jf. artikel 33, stk. 5.

Den foreslåede bestemmelse svarer indholdsmæssigt til NIS 2-direktivets artikel 32, stk. 8, jf. artikel 33, stk. 5, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Den foreslåede bestemmelse indeholder en forpligtelse for Styrelsen for Samfundssikkerhed til at foretage en høring af den væsentlige teleudbyder eller vigtige teleudbyder, før der træffes beslutning om at anvende en påtænkt håndhævelsesforanstaltning efter §§ 20-22.

Høringsskrivelsen skal være ledsaget af en nærmere begrundelse for den påtænkte håndhævelsesforanstaltning, ligesom det skal fremgå klart, at der er tale om en høring, at der ikke er truffet afgørelse i sagen endnu, at udbyderens bemærkninger til høringen kan få indflydelse på resultatet, og at Styrelsen for Samfundssikkerhed lader agterskrivelsen få virkning som en afgørelse, hvis udbyderen ikke kommer med bemærkninger til høringen inden dennes udløb.

Høringsskrivelsen skal indeholde en rimelig frist for udbyderen til at afgive bemærkninger til høringsskrivelsens indhold. Kravet om at fastsætte en rimelig frist gælder dog ikke i behørigt begrundede tilfælde, hvor øjeblikkelige foranstaltninger til at forebygge eller reagere på hændelser ellers ville blive hindret.

Det forudsættes, at høringen foretages i overensstemmelse med forvaltningslovens regler om partshøring.

Til § 25

Det foreslås i *stk. 1*, at Styrelsen for Samfundssikkerhed i ikke-anonymiseret form kan offentliggøre 1) afgørelser om påbud meddelt i medfør af af § 13, stk. 5 og 7 og 18, stk. 1 og 2, og afgørelser truffet i medfør af regler, der er udstedt i medfør af 7, stk. 5, nr. 1-3, § 13, stk. 5, 2. pkt., og § 18, stk. 2, 2. pkt., 2) resultater af tilsyn efter § 19 og 22, 3) resumeer af domme eller bødevedtagelser, hvor der idømmes eller vedtages en bøde for overtrædelse af denne lov eller regler, der er udstedt i medfør af denne lov, og 4) resumeer af domme i retssager, hvor Styrelsen for Samfundssikkerhed er part.

Bestemmelsen viderefører indholdet af § 10, stk. 1, i lov om sikkerhed i net og tjenester, jf. lovbekendtgørelse nr. 153 af 1. februar 2021, som ændret ved § 18 i lov nr. 1156 af 8. juni 2021.

Ministeriet for Samfundssikkerhed og Beredskab finder det således henset til vurderingen af det aktuelle trusselsniveau mod telesektoren væsentligt at opretholde det nuværende sikkerhedsniveau for sektoren. Der er med videreførelsen af bestemmelsen ikke tilsigtet materielle ændringer af bestemmelsens indhold.

Den foreslåede bestemmelse har til formål at give væsentlige og vigtige teleudbydere øget incitament til at overholde kravene til sikkerhed i net og informationssystemer og beredskab, ligesom bestemmelsen giver telekunder mulighed for at vurdere, i hvilket omfang de enkelte udbydere har levet op til lovgivningens krav.

Offentliggørelse af afgørelser efter *nr. 1*, indebærer, at der kan ske offentliggørelse i sager, hvor en væsentlig eller vigtig teleudbyder ikke lever op til kravene til sikkerhed i net og informationssystemer eller beredskab, såvel som i sager, hvor Styrelsen for Samfundssikkerhed giver påbud til en udbyder om eksempelvis at foretage nærmere angivne foranstaltninger til sikring af sikkerheden i net og informationssystemer. Der vil også kunne ske offentliggørelse i sager, hvor Styrelsen for Samfundssikkerhed på baggrund af eksempelvis en klage konstaterer, at en udbyder overholder kravene til sikkerhed i net og informationssystemer og beredskab. Styrelsen for Samfundssikkerheds beslutning om at overgive sager til politimæssig efterforskning vil også kunne offentliggøres efter bestemmelsen.

Efter *nr. 2*, kan Styrelsen for Samfundssikkerhed endvidere offentliggøre resultater af tilsyn udført efter §§ 19 og 22.

Sådanne tilsynsresultater kan omfatte styrelsens tilsynsrapporter, ligesom det vil kunne omfatte statistik, eksempelvis i form af en kvartalsvis eller årlig opgørelse over antallet af påbud til de enkelte teleudbydere.

Det foreslås endvidere med *nr. 3*, at resuméer af domme eller bødevedtagelser, hvor der idømmes eller vedtages en bøde for overtrædelse af denne lov eller regler, der er udstedt i medfør af denne lov, skal kunne offentliggøres.

Herudover skal der efter *nr. 4*, kunne ske offentliggørelse af resuméer af domme i retssager vedrørende sikkerhed i net og informationssystemer og beredskab på teleområdet, og hvor Styrelsen for Samfundssikkerhed er part om forhold omfattet af denne lov. Der sker ikke med bestemmelsen en fravigelse af retsplejelovens regler om aktindsigt i domme.

Offentliggørelse vil ske på Styrelsen for Samfundssikkerheds hjemmeside i ikke-anonymiseret form. Det vil således fremgå af det offentliggjorte materiale, hvilken udbyder afgørelsen, tilsynsresultatet, dommen eller bødevedtagelsen er rettet imod.

I overensstemmelse med principperne i betænkning nr. 1516 om offentlige myndigheders offentliggørelse af kontrolresultater, afgørelser mv. forudsættes det, at Styrelsen for Samfundssikkerhed ved beslutningen om, hvilke oplysninger en udbyder pålægges at offentliggøre, i fornødent omfang bl.a. iagttager de hensyn til fortrolighed, der fremgår af forvaltningslovens § 27 om offentlig ansattes tavshedspligt, herunder bl.a. hensynene til enkeltpersoners private forhold, forretningshemmeligheder samt forebyggelse, efterforskning og forfølgning af lovovertrædelser.

Det foreslås i *stk. 2*, at offentliggørelse efter stk. 1 ikke må indeholde de i bestemmelsens nr. 1-4 angivne oplysninger.

Bestemmelsen viderefører indholdet af § 10, stk. 2, i lov om sikkerhed i net og tjenester.

Det foreslås med *nr. 1*, at offentliggørelsen ikke må indeholde oplysninger vedrørende tekniske indretninger eller fremgangsmåder eller om drifts- eller forretningsforhold eller lignende, for så vidt det er af væsentlig økonomisk betydning for den væsentlige teleudbyder eller vigtige teleudbyder, oplysningerne angår. Definitionen af oplysninger vedrørende tekniske indretninger mv. skal forstås i overensstemmelse med § 30, nr. 2, i offentlighedsloven og skal fortolkes i overensstemmelse med denne bestemmelses forarbejder og relevante praksis.

Efter *nr. 2*, vil oplysninger undtages fra offentliggørelse i det omfang, det er af væsentlig betydning for statens sikkerhed eller rigets forsvar. Vurderingen af, hvornår offentliggørelse af oplysninger kan være af væsentlig betydning for statens sikkerhed eller rigets forsvar, skal foretages i overensstemmelse med principperne i § 31 i offentlighedsloven.

Desuden vil klassificerede informationer efter *nr. 3*, blive slettet i det materiale, der offentliggøres.

Efter *nr. 4*, vil der endvidere ikke ske offentliggørelse af fortrolige oplysninger, der hidrører fra myndigheder i andre EU-medlemsstater, jf. den foreslåede § 27, stk. 2, medmindre de myndigheder, der har afgivet oplysningerne, har givet deres udtrykkelige tilladelse til offentliggørelsen.

Endelig vil enkeltpersoners forhold efter *nr. 5* blive slettet inden offentliggørelsen. Det kan eksempelvis være oplysninger om navne, adresser eller telefonnumre på klagere eller andre berørte parter, som vil skulle undtages fra offentliggørelsen.

Det bemærkes i øvrigt, at Styrelsen for Samfundssikkerhed forudsættes ikke at offentliggøre afgørelser eller tilsynsresultater, såfremt efterforskningsmæssige hensyn taler derimod.

Det foreslås i *stk. 3*, at ministeren for samfundssikkerhed og beredskab kan fastsætte nærmere regler om sagsbehandlingen i forbindelse med offentliggørelse efter stk. 1.

Bestemmelsen er en videreførelse af § 10, stk. 3, i lov om sikkerhed i net og tjenester.

Bestemmelsens stk. 3, bemyndiger Styrelsen for Samfundssikkerhed til at fastsætte nærmere regler for styrelsens sagsbehandling i forbindelse med offentliggørelser efter stk. 1.

Styrelsen for Samfundssikkerhed vil med hjemmel i bestemmelsen eksempelvis kunne fastsætte regler for, hvornår der kan ske offentliggørelse. Styrelsen for Samfundssikkerhed vil endvidere kunne fastsætte regler om forudgående høring eller orientering af en udbyder vedrørende spørgsmålet om en forestående offentliggørelse af en afgørelse eller tilsynsresultat mv.

Styrelsen for Samfundssikkerhed vil herudover kunne fastsætte regler om, at det skal fremgå af offentliggørelsen, såfremt en afgørelse er påklaget til Ministeriet for Samfundssikkerhed og Beredskab, eller såfremt der verserer en sag for domstolene.

Endelig vil Styrelsen for Samfundssikkerhed kunne fastsætte regler om, hvor lang tid den pågældende afgørelse, tilsynsresultat mv. skal være offentligt tilgængelige på styrelsens hjemmeside.

Til § 26

Det foreslås i *stk. 1,* at de forpligtelser, der er fastsat i denne lov eller i regler udstedt i medfør af loven, ikke omfatter meddelelse af oplysninger, hvis videregivelse ville stride mod væsentlige interesser af hensyn til den nationale sikkerhed, offentlige sikkerhed eller forsvar.

Bestemmelsen gennemfører artikel 2, stk. 11, i NIS 2-direktivet, for så vidt angår telesektoren. Artikel 2, stk. 11, fastsætter, at de forpligtelser, der er fastsat i direktivet, ikke omfatter meddelelse af oplysninger, hvis videregivelse ville stride mod væsentlige interesser med hensyn til medlemsstaternes nationale sikkerhed, offentlige sikkerhed eller forsvar.

Ved vurderingen af, om der er tale om en oplysning, der er omfattet af undtagelsen skal det ifølge NIS 2-direktivets præambelbetragtning nr. 9, 4. pkt., tages hensyn til, om videregivelse ville stride mod dens væsentlige interesser med hensyn til national sikkerhed, offentlig sikkerhed eller forsvar. Det følger samme sted, at nationale regler eller EU-regler om beskyttelse af fortrolige oplysninger, hemmeligholdelsesaftaler og uformelle hemmeligholdelsesaftaler, f.eks. Traffic Light Protocol, bør tages i betragtning i denne sammenhæng. Traffic Light Protocol skal forstås som et middel til at informere om eventuelle begrænsninger, for så vidt angår den videre spredning af oplysninger. Den anvendes i næsten alle enheder, der håndterer it-sikkerhedshændelser (CSIRT'er), og i nogle informationsanalyse- og informationsdelingscentre.

Den foreslåede bestemmelse svarer indholdsmæssigt til NIS 2-direktivets artikel 2, stk. 11, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Det følger af det foreslåede *stk. 2*, at oplysninger, der modtages eller hidrører fra myndigheder i andre EU-medlemsstater, behandles som fortrolige, såfremt den afgivende myndighed betragter oplysningerne som fortrolige i henhold til EU-regler eller nationale regler.

Den foreslåede bestemmelse vil bl.a. sikre, at oplysninger, som de danske myndigheder modtager fra andre medlemsstater eller EU-institutioner i medfør af NIS 2-direktivets artikel 23, stk. 6, vil blive behandlet med den fornødne fortrolighed.

Det følger således af NIS 2-direktivets artikel 23, stk. 6, at hvor det er relevant, og navnlig hvor en væsentlig hændelse berører to eller flere medlemsstater, informerer CSIRT'en, den kompetente myndighed eller det centrale kontaktpunkt

uden unødigt ophold de øvrige berørte medlemsstater og ENISA om den væsentlige hændelse.

Den foreslåede bestemmelse vil finde anvendelse, uanset om oplysningerne modtages direkte fra den pågældende nationale myndighed eller via andre, herunder Europa-Kommissionen.

Til § 27

Det foreslås i *stk. 1*, at Styrelsen for Samfundssikkerhed hos væsentlige og vigtige teleudbydere kan indsamle oplysninger med henblik på at videregive disse til Kommissionen, Den Europæiske Unions Agentur for Cybersikkerhed eller nationale tilsynsmyndigheder i andre EU-medlemsstater, idet omfang det er nødvendigt for, at disse kan opfylde deres opgaver i forhold til traktatmæssige forpligtelser eller forpligtelser i henhold til den gældende EU-ret.

Bestemmelsen viderefører § 12, stk. 1, i lov om sikkerhed i net og tjenester, jf. lovbekendtgørelse nr. 153 af 1. februar 2021, som ændret ved § 18 i lov nr. 1156 af 8. juni 2021.

Bestemmelsen gennemfører delvist artikel 20, stk. 2, i EU's telekodeks samt artikel 40, stk. 2, i EU's telekodeks, som ophæves ved artikel 43 i NIS 2-direktivet.

Efter det foreslåede stk. 1, kan Styrelsen for Samfundssikkerhed indsamle oplysninger om sikkerhed i net og informationssystemer og beredskab på teleområdet hos teleudbydere med henblik på at videregive oplysningerne til Kommissionen eller nationale tilsynsmyndigheder i andre EU-medlemsstater. Det foreslås, at bestemmelsen også skal omfatte indsamling af oplysninger om sikkerhed i net og informationssystemer med henblik på videregivelse af oplysningerne til ENISA, som har til opgave at sikre en høj grad af net- og informationssikkerhed i EU, og som bl.a. fungerer som et forum for erfaringsudveksling for de nationale tilsynsmyndigheder.

Det foreslås i *stk. 2*, at Styrelsen for Samfundssikkerhed orienterer teleudbydere, der er indsamlet oplysninger fra, forud for videregivelse af oplysningerne til Kommissionen, Den Europæiske Unions Agentur for Cybersikkerhed eller nationale tilsynsmyndigheder i andre EU-medlemsstater.

Bestemmelsen viderefører 12, stk. 2, i lov om sikkerhed i net og tjenester.

Bestemmelsen gennemfører delvist artikel 20, stk. 2, i EU's telekodeks.

Efter det foreslåede stk. 2 skal den væsentlige eller vigtige teleudbyder hvis oplysninger videregives til Kommissionen eller til myndigheder i andre EU-medlemsstater, orienteres forud for videregivelsen. Styrelsen for Samfundssikkerhed skal ikke afvente udbyderens eventuelle kommentarer eller accept af videregivelsen. Det vil således være tilstrækkeligt, at der i forbindelse med indsamlingen af oplysningerne orienteres om videregivelsen. På baggrund af det foreslåede stk. 1, vedrørende videregivelse af oplysninger til ENISA, foreslås det, at Styrelsen for Samfundssikkerhed også orienterer de udbydere, der er indsamlet oplysninger fra, forud for videregivelse af oplysningerne til ENISA.

Til § 28

Det foreslås i *stk. 1,* at hvor en væsentlig teleudbyder eller en vigtig teleudbyder leverer tjenester i mere end én medlemsstat i Den Europæiske Union, eller hvor udbyderen leverer tjenester i en eller flere medlemsstater, og udbyderens net- og informationssystemer er beliggende i en eller flere andre medlemsstater, samarbejder Styrelsen for Samfundssikkerhed med de andre medlemsstaters kompetente myndigheder i relevant omfang. Samarbejdet indebærer, at: 1) Styrelsen for Samfundssikkerhed underretter de kompetente myndigheder i relevante medlemsstater om tilsyns- og håndhævelsesforanstaltninger iværksat over for teleudbydere i Danmark, 2) Styrelsen for Samfundssikkerhed kan anmode en anden medlemsstats kompetente myndigheder om at anvende tilsyns- og håndhævelsesforanstaltninger, og 3) Styrelsen for Samfundssikkerhed yder i rimeligt omfang bistand til en anden medlemsstats kompetente myndighed efter modtagelse af en begrundet anmodning herom om at anvende tilsyns- og håndhævelsesforanstaltninger.

Bestemmelsen vil gennemføre artikel 37, stk. 1, i NIS 2-direktivet, for så vidt angår telesektoren.

Det følger af NIS 2-direktivets artikel 37, stk. 1, 2. led, at den gensidige bistand, der er omhandlet i litra c, kan omfatte anmodninger om oplysninger og tilsynsforanstaltninger, herunder anmodninger om at foretage inspektioner på stedet eller eksternt tilsyn eller målrettede sikkerhedskontroller. En kompetent myndighed, som en anmodning om bistand er rettet til, må ikke afvise anmodningen, medmindre det er fastslået, at den ikke er kompetent til at yde den ønskede bistand, at den bistand, der anmodes om, ikke står i et rimeligt forhold til den kompetente myndigheds tilsynsopgaver, eller anmodningen vedrører oplysninger eller indebærer aktiviteter, som, hvis de blev videregivet eller udført, ville stride mod den medlemsstats væsentlige interesser med hensyn til national sikkerhed, offentlige sikkerhed eller forsvar. Før den kompetente myndighed afslår en sådan anmodning, hører den de øvrige berørte kompetente myndigheder samt, efter anmodning fra en af de berørte medlemsstater, Europa-Kommissionen og ENISA.

Den foreslåede bestemmelse svarer indholdsmæssigt til NIS 2-direktivets artikel 37, stk. 1, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Den foreslåede bestemmelse indebærer, at Styrelsen for Samfundssikkerhed i relevant omfang skal samarbejde med de kompetente myndigheder i andre medlemsstater om deres opgaveudførelse vedrørende væsentlige og vigtige teleudbydere, der leverer tjenester i mere end én medlemsstat i Den Europæiske Union, og udbyderens net- og informationssystemer er beliggende i én eller flere andre medlemsstater.

Samarbejdet indebærer, at der skal ske underretning af de kompetente myndigheder i relevante medlemsstater om anvendte tilsyns- og håndhævelsesforanstaltninger. At der skal ske underretning til kompetente myndigheder i »relevante medlemsstater« betyder, at der skal ske underretning til de kompetente myndigheder i medlemsstater, hvor udbyderen leverer tjenester, eller hvor udbyderens net- og informationssystemer er beliggende.

Samarbejdet indebærer desuden, at Styrelsen for Samfundssikkerhed kan anmode en anden medlemsstats kompetente myndigheder om at iværksætte tilsyns- og håndhævelsesforanstaltninger.

Samarbejdet indebærer endvidere, at Styrelsen for Samfundssikkerhed i rimeligt omfang skal yde bistand til en anden medlemsstats kompetente myndighed efter modtagelse af en begrundet anmodning herom. Denne bistand kan omfatte anmodninger om oplysninger og tilsynsforanstaltninger, herunder eksempelvis anmodninger om at foretage kontrol på stedet eller målrettede sikkerhedsaudits.

En anmodning om bistand kan afvises, hvis anmodningen ikke står i rimeligt forhold til Styrelsen for Samfundssikkerheds tilsynsopgaver og ressourcer.

En anmodning om bistand kan desuden afvises, hvis anmodningen vedrører videregivelsen af oplysninger eller indebærer udførelsen af aktiviteter, som ville stride mod væsentlige interesser med hensyn til national sikkerhed, offentlige sikkerhed eller forsvar. Før der kan ske afvisning af en anmodning, skal Styrelsen for Samfundssikkerhed høre de relevante kompetente myndigheder i andre medlemsstater samt, efter anmodning fra en af de relevante kompetente myndigheder i andre medlemsstater, Europa-Kommissionen og ENISA.

Efter NIS 2-direktivets præambelbetragtning nr. 134 er formålet med bestemmelsen i direktivets artikel 37 at sikre, at enhederne overholder de forpligtelser, der er fastsat i direktivet. En anmodning om gensidig bistand efter den foreslåede stk. 1 vil derfor ikke blive imødekommet, såfremt anmodningen entydigt vedrører en anden medlemsstats nationale overimplementering af NIS 2- direktivet.

Det følger af det foreslåede *stk. 2*, at Styrelsen for Samfundssikkerhed efter nærmere aftale kan gennemføre fælles tilsynstiltag med kompetente myndigheder fra andre medlemsstater i Den Europæiske Union.

Bestemmelsen vil gennemføre NIS 2-direktivets artikel 37, stk. 2, for så vidt angår telesektoren. Det følger af artikel 37, stk. 2, at hvor det er hensigtsmæssigt og efter fælles overenskomst, kan de kompetente myndigheder fra forskellige medlemsstater gennemføre fælles tilsynstiltag.

Den foreslåede bestemmelse svarer således indholdsmæssigt til NIS 2-direktivets artikel 37, stk. 2, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Der stilles med den foreslåede bestemmelse ikke nærmere formkrav til den aftale, der indgås om udførelsen af fælles tilsynstiltag.

Den foreslåede bestemmelse indebærer ikke, at andre medlemsstaters myndigheder selvstændigt kan udøve tilsynsbeføjelser her i landet. Tilsynsforanstaltninger vil således altid foretages under Styrelsen for Samfundssikkerheds ansvar.

Til § 29

Det følger af den foreslåede *§ 29,* at ministeren for samfundssikkerhed og beredskab kan fastsætte regler, som er nødvendige for at gennemføre retsakter udstedt af Europa-Kommissionen i medfør af NIS 2-direktivet.

Europa-Kommissionen er flere steder i NIS 2-direktivet tillagt kompetence til at vedtage retsakter, der nærmere udmønter bestemte dele af direktivet.

For så vidt angår væsentlige teleudbydere og vigtige teleudbydere, kan Europa-Kommissionen i medfør af artikel 21, stk. 5, 2. led, vedtage gennemførelsesretsakter, der fastsætter de tekniske og metodologiske samt om nødvendigt sektorspecifikke krav til de foranstaltninger, der er omhandlet i direktivets artikel 21, stk. 2 (foranstaltninger til styring af cybersikkerhedsrisici).

Ved udarbejdelsen af de nævnte gennemførelsesretsakter følger Europa-Kommissionen i videst muligt omfang europæiske og internationale standarder samt relevante tekniske specifikationer. Europa-Kommissionen samarbejder med samarbejdsgruppen og ENISA om udkastene til gennemførelsesretsakter.

Det følger desuden af NIS 2-direktivets artikel 23, stk. 11, at Europa-Kommissionen kan vedtage gennemførelsesretsakter, der yderligere præciserer typen af oplysninger, formatet og proceduren for en underretning indgivet i henhold til artikel 23, stk. 1 (underretning af myndighederne om hændelser), og artikel 30 (frivillig meddelelse af relevante oplysninger) og for en meddelelse, der er indgivet i henhold til artikel 23, stk. 2 (oplysning til modtagerne af tjenester).

Det følger endvidere af NIS 2-direktivets artikel 24, stk. 2, at Europa-Kommissionen tillægges beføjelser til at vedtage delegerede retsakter for at supplere NIS 2-direktivet ved at præcisere, hvilke kategorier af væsentlige og vigtige enheder der skal anvende visse certificerede IKT-produkter, -tjenester og -processer eller indhente en attest i henhold til en europæisk cybersikkerhedscertificeringsordning, der er vedtaget i henhold til artikel 49 i Europa-Parlamentets og Rådets forordning (EU) 2019/881 af 17. april 2019 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed), om cybersikkerhedscertificering af informations- og kommunikationsteknologi og om ophævelse af forordning (EU) nr. 526/2013 (forordningen om cybersikkerhed). Disse delegerede retsakter vedtages, når der er identificeret utilstrækkelige cybersikkerhedsniveauer og skal indeholde en gennemførelsesperiode.

Ministeren for samfundssikkerhed og beredskab får efter bestemmelsen hjemmel til inden for telesektoren at fastsætte regler, som er nødvendige for at gennemføre retsakter udstedt af Europa-Kommissionen.

Til § 30

Det følger af den foreslåede *§ 30,* at ministeren for samfundssikkerhed og beredskab kan fastsætte regler om digital kommunikation, herunder om anvendelsen af bestemte it-systemer og særlige digitale formater samt digital signatur eller lignende.

Den foreslåede bestemmelse indebærer, at det kan gøres obligatorisk for væsentlige teleudbydere og vigtige teleudbydere at anvende bestemte internetløsninger, herunder selvbetjeningsløsninger.

Der kan endvidere med hjemmel i bestemmelsen fastsættes regler om, hvem der omfattes af pligten til at kommunikere digitalt, om hvilke forhold, og på hvilken måde.

Bestemmelsen forventes navnlig anvendt til at fastsætte regler om, hvordan væsentlige teleudbydere og vigtige teleudbydere skal foretage underretninger om hændelser i medfør af de foreslåede §§ 8 og 9. Der vil eksempelvis kunne fastsættes regler om anvendelse af bestemte digitale internetløsninger såsom Virk.dk. Det kan eksempelvis også være relevant at fastsætte regler om, at bl.a. registreringspligterne i de foreslåede § 7 skal efterkommes ved anvendelse af bestemte internetløsninger såsom Virk.dk.

Der kan med hjemmel i bestemmelsen fastsættes regler om, at skriftlige henvendelser til Styrelsen for Samfundssikkerhed om forhold, som er omfattet af et krav om digital kommunikation, ikke anses for behørigt modtaget af styrelsen, hvis de indsendes på anden vis end den foreskrevne digitale måde.

Hvis en væsentlig eller vigtig teleudbyder retter henvendelse til Styrelsen for Samfundssikkerhed på anden måde end den foreskrevne digitale måde, følger det af den almindelige vejledningspligt, jf. forvaltningslovens § 7, stk. 2, at styrelsen skal vejlede om reglerne på området, herunder om pligten til at kommunikere digitalt.

Der kan desuden fastsættes regler om fritagelse for pligten til digital kommunikation. Fritagelsesmuligheden tænkes navnlig anvendt, hvor det er påkrævet at anvende en dansk digital signatur, men der er tale om en virksomhed med hjemsted i udlandet, og som dermed ikke kan få udstedt en dansk digital signatur. Det bemærkes i den forbindelse, at fritagelsesmuligheden er stærkt begrænset, idet der er tale om kommunikation om erhvervsforhold, og idet virksomheder med hjemsted i udlandet kun i begrænset omfang vil høre under dansk jurisdiktion.

Det forhold, at en væsentlig eller vigtig teleudbyders computere ikke fungerer, at udbyderen har mistet koden til sin digitale signatur, eller at der opstår lignende hindringer, som det er op til udbyderen at overvinde, vil ikke kunne føre til fritagelse for pligten til digital kommunikation. I så fald må den pågældende udbyder eksempelvis anmode en rådgiver om at varetage kommunikationen på virksomhedens vegne.

Der kan efter bestemmelsen også fastsættes regler om, at en digital meddelelse anses for at være kommet frem til adressaten for meddelelsen på det tidspunkt, hvor meddelelsen er tilgængelig digitalt for adressaten. Dermed er der tale om samme retsvirkning som ved fysisk post, der anses for at være kommet frem, når den pågældende meddelelse mv. er lagt i adressatens fysiske postkasse. En meddelelse vil normalt anses for at være kommet frem, når meddelelsen er tilgængelig digitalt for adressaten, således at vedkommende har mulighed for at behandle meddelelsen. Dette tidspunkt vil normalt blive registreret automatisk i adressatens it-system.

Det bemærkes, at Europa-Kommissionen på visse punkter er tillagt kompetence til at fastsætte nærmere regler om, hvordan oplysninger skal afgives fra de væsentlige teleudbydere og de vigtige teleudbydere. Europa-Kommissionen kan således bl.a. fastsætte nærmere regler om formatet og proceduren for en underretning indgivet i henhold til artikel 23, stk. 1 (underretning af myndighederne om hændelser), og artikel 30 (frivillig meddelelse af relevante oplysninger) og for en meddelelse, der er indgivet i henhold til artikel 23, stk. 2 (oplysning til modtagerne af tjenester). Såfremt Europa-Kommissionen måtte vælge at udnytte denne kompetence til at fastsætte nærmere regler, vil det skulle sikres, at regler om digital kommunikation, der måtte være udstedt eller siden udstedes i medfør af den foreslåede bestemmelse, er i overensstemmelse med Europa-Kommissionens retsakter.

Til § 31

Det foreslås i *stk. 1,* at den, der 1) overtræder § 5, stk. 1, eller 2, § 7, stk. 1-3, § 8, stk. 2, jf. stk. 3, § 9, stk. 1 og § 11, stk. 1 og 2, 2) undlader at efterkomme Styrelsen for Samfundssikkerheds afgørelse efter § 21, stk. 1, nr. eller 2, 3) undlader at efterkomme Styrelsen for Samfundssikkerheds påbud efter § 13, stk. 5, eller § 18, stk. 1 og 2, 4) undlader at efterkomme Styrelsen for Samfundssikkerheds krav efter § 19, stk. 1, nr. 5-8, eller § 22, stk. 1, nr. 4-7 eller 5) hindrer Styrelsen for Samfundssikkerhed i at føre tilsyn efter bestemmelserne i § 19, stk. 1, nr. 1-4, eller § 22, stk. 1, nr. 1-3, straffes med bøde.

Den foreslåede bestemmelse vil gennemføre artikel 36, stk. 1, NIS 2-direktivet. Artikel 36, stk. 1, forpligter medlemsstaterne til at fastsætte regler om sanktioner, der skal anvendes i tilfælde af overtrædelser af de nationale foranstaltninger, der er vedtaget i medfør af NIS 2-direktivet og til at træffe alle nødvendige foranstaltninger for at sikre, at de gennemføres. Sanktionerne skal være effektive, stå i rimeligt forhold til overtrædelsen og have afskrækkende virkning.

Den foreslåede bestemmelse svarer med sproglige tilpasnin-

ger indholdsmæssigt til NIS 2-direktivets artikel 36, stk. 1, og skal således forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Den foreslåede bestemmelse vil gennemføre artikel 36, stk. 1, i NIS 2-direktivet. Artikel 36, stk. 1, forpligter medlemsstaterne til at fastsætte regler om sanktioner, der skal anvendes i tilfælde af overtrædelser af de nationale foranstaltninger, der er vedtaget i medfør af NIS 2-direktivet og til at træffe alle nødvendige foranstaltninger for at sikre, at de gennemføres. Sanktionerne skal være effektive, stå i rimeligt forhold til overtrædelsen og have afskrækkende virkning.

Den foreslåede bestemmelse vil endvidere gennemføre NIS 2-direktivets artikel 34, hvoraf det følger, at medlemsstaterne sikrer, at de administrative bøder, der pålægges væsentlige og vigtige enheder i henhold til artiklen, for så vidt angår overtrædelser af direktivet, er effektive, står i rimeligt forhold til overtrædelsen og har afskrækkende virkning, under hensyntagen til omstændighederne i hver enkelt sag.

Efter artikel 34, stk. 2, kan administrative bøder pålægges i tillæg til en hvilken som helst af foranstaltningerne omhandlet i artikel 32, stk. 4, litra a-h, artikel 32, stk. 5, og artikel 33, stk. 4, litra a-g.

Efter artikel 34, stk. 4, skal medlemsstaterne sikre, at hvor væsentlige enheder overtræder artikel 21 (foranstaltninger til styring af cybersikkerhedsrisici) eller 23 (rapporteringsforpligtelser), straffes de i overensstemmelse med artiklernes stk. 2 og 3 med administrative bøder med et maksimum på mindst 10.000.000 euro eller et maksimum på mindst 2 pct. af den samlede globale årsomsætning i det foregående regnskabsår i den virksomhed, som den væsentlige enhed tilhører, alt efter hvad der er højest.

Det følger af artikel 34, stk. 5, at medlemsstaterne sikrer, at hvor vigtige enheder overtræder artikel 21 (foranstaltninger til styring af cybersikkerhedsrisici) eller 23 (rapporteringsforpligtelser), straffes de i overensstemmelse med artiklernes stk. 2 og 3 med administrative bøder med et maksimum på mindst 7.000.000 euro eller et maksimum på mindst 1,4 pct. af den samlede globale årsomsætning i det foregående regnskabsår i den virksomhed, som den vigtige enhed tilhører, alt efter hvad der er højest.

Det følger endvidere af artikel 34, stk. 8, 1. og 2. pkt., at hvis en medlemsstats retssystem ikke giver mulighed for at pålægge administrative bøder, sørger den pågældende medlemsstat for, at artiklen anvendes på en sådan måde, at den kompetente myndighed tager skridt til bøder, og de kompetente nationale domstole pålægger dem, idet det sikres, at disse retsmidler er effektive, og at deres virkning svarer til virkningen af administrative bøder, som pålægges af de kompetente myndigheder. De bøder, der pålægges, skal under alle omstændigheder være effektive, stå i rimeligt forhold til overtrædelsen og have afskrækkende virkning.

Endelig vil den foreslåede bestemmelse – i kombination med den foreslåede bestemmelse i § 6, stk. 1 – gennemføre NIS 2-direktivets artikel 20, stk. 1, hvoraf det følger, at medlemsstaterne sikrer, at de væsentlige og vigtige teleudbyderes ledelsesorganer godkender de foranstaltninger til styring af cybersikkerhedsrisici, som disse enheder har truffet med henblik på at overholde artikel 21, fører tilsyn med dens gennemførelse og kan gøres ansvarlige for enhedernes overtrædelser af forpligtelserne i nævnte artikel.

Det forudsættes i overensstemmelse med en minimumsimplementering af NIS 2-direktivets artikel 34, stk. 4, at bødens størrelse for væsentlige teleudbydere maksimalt vil kunne udgøre et beløb svarende til 10.000.000 euro eller 2 pct.af den væsentlige teleudbyders samlede globale årsomsætning i det foregående regnskabsår alt efter, hvad der er højest.

Det forudsættes endvidere i overensstemmelse med en minimumsimplementering af NIS 2-direktivets artikel 34, stk. 5, at bødens størrelse for vigtige teleudbyderes maksimalt vil udgøre et beløb svarende til 7.000.000 euro eller 1,4 pct.af den vigtige teleudbyders samlede globale årsomsætning i det foregående regnskabsår alt efter, hvad der er højest.

Der forudsættes ikke i tilknytning til øvrige bestemmelser end de specifikt angivne ovenfor anlagt særlige forudsætninger for så vidt angår udmålingen af bøders størrelse. Det samme gælder eventuel udmåling af bøder til fysiske personer, hvor det dog i overensstemmelse med direktivets præambelbetragtning nr. 130, 2. pkt., forudsættes, at der lægges vægt på det generelle indkomstniveau og personens økonomiske stilling.

Det forudsættes i overensstemmelse med NIS 2-direktivets artikel 34, stk. 3, jf. artikel 32, stk. 7, at der lægges vægt på følgende hensyn ved pålæg af en bøde og ved udmåling af bødens størrelse: 1) overtrædelsens grovhed og vigtigheden af de overtrådte bestemmelser, idet bl.a. følgende under alle omstændigheder skal betragtes som alvorlige overtrædelser: a) Gentagne overtrædelser, b) manglende underretning om eller afhjælpning af væsentlige hændelser, c) manglende afhjælpning af mangler efter bindende instrukser fra kompetente myndigheder, d) hindringer for audits eller overvågningsaktiviteter beordret af den kompetente myndighed efter konstatering af en overtrædelse og e) afgivelse af urigtige eller klart unøjagtige oplysninger vedrørende cybersikkerhedsrisikostyringsforanstaltninger eller rapporteringsforpligtelser, 2) overtrædelsens varighed, 3) den pågældende enheds relevante tidligere overtrædelser, 4) enhver fysisk eller ikke-fysisk skade, der er forårsaget, herunder ethvert finansielt eller økonomisk tab, virkninger for andre tjenester og antallet af brugere, der er berørt, 5) hvorvidt der ved overtrædelsen er handlet forsætligt eller uagtsomt, 6) enhver foranstaltning truffet af enheden for at forebygge eller afbøde den fysiske eller ikke-fysiske skade, 7) hvorvidt godkendte adfærdskodekser eller godkendte certificeringsmekanismer er overholdt, og 8) i hvilken udstrækning de fysiske eller juridiske personer, der holdes ansvarlige for overtrædelsen, samarbejder med de kompetente myndigheder.

Den fastsatte bøde skal i overensstemmelse med NIS 2-direktivets artikel 34, stk. 1, være effektiv, stå i et rimeligt forhold til overtrædelsen og have afskrækkende virkning under hensyntagen til omstændighederne i den konkrete sag.

Bøde vil i overensstemmelse med NIS 2-direktivets artikel 34, stk. 2, kunne pålægges i tillæg til håndhævelsesforanstaltningerne i de foreslåede §§ 20-23.

Det bemærkes, at fastsættelsen af straffen fortsat vil bero på domstolenes konkrete vurdering i det enkelte tilfælde af samtlige omstændigheder i sagen, og de angivne strafniveauer vil kunne fraviges i op- eller nedadgående retning, hvis der i den konkrete sag foreligger skærpende eller formildende omstændigheder, jf. herved de almindelige regler om straffens fastsættelse i straffelovens 10. kapitel.

Det foreslås i *nr. 1,* at den, der overtræder § 5, stk. 1, eller 2, § 7, stk. 1-3, § 8, stk. 2, jf. stk. 3, § 9, stk. 1 og § 11, stk. 1 og 2, straffes med bøde.

Den foreslåede bestemmelse indebærer for det første, at væsentlige og vigtige teleudbydere, der ikke træffer passende og forholdsmæssige tekniske, operationelle og organisatoriske foranstaltninger for at styre risiciene for sikkerheden i net- og informationssystemer efter den foreslåede § 5, stk. 1, straffes med bøde.

Det samme gælder tilfælde, hvor en væsentlig elle vigtig teleudbyder bliver bekendt med, at denne ikke overholder ét eller flere af de krav, der er nævnt i den foreslåede § 5, stk. 1, eller regler om krav til foranstaltninger fastsat i medfør af stk. 3, og ikke unødigt ophold træffer alle nødvendige, passende og forholdsmæssige korrigerende foranstaltninger.

Vurderingen af, om foranstaltningerne er truffet uden unødigt ophold vil bero på en konkret vurdering af sagens omstændigheder.

Den foreslåede bestemmelse indebærer endvidere, at væsentlige og vigtige enheder, der overtræder registrerings- og oplysningsforpligtelserne i den foreslåede § 7, stk. 1-3, straffes med bøde.

Den foreslåede bestemmelse indebærer endvidere, at væsentlige og vigtige teleudbydere, der overtræder hændelsesunderretningsforpligtelsen i den foreslåede § 8, stk. 2, straffes med bøde. Det samme gælder, hvis den væsentlige eller vigtige teleudbyder ikke overholder proceduren til foretagelse af hændelsesunderretningen efter den foreslåede bestemmelse i § 9, stk. 1.

Den foreslåede bestemmelse vil endelig medføre, at en væsentlig eller vigtig teleudbyder, der ikke overholder forpligtelsen til at underrette modtagere af sine tjenester om hændelser efter de foreslåede bestemmelser i § 11, stk. 1 og 2, vil blive straffet med bøde.

Det foreslås i *nr. 2,* at den, der undlader at efterkomme Styrelsen for Samfundssikkerheds afgørelse efter § 21, stk. 1, nr. eller 2, straffes med bøde.

Det følger af den foreslåede bestemmelse, at væsentlige teleudbydere, der undlader at efterkomme Styrelsen for Samfundssikkerheds afgørelse om midlertidig suspension af en certificering eller godkendelse efter den foreslåede § 21, stk. 1, nr. 1, eller en afgørelse om midlertidigt forbud mod at udøve ledelsesfunktioner efter den foreslåede § 21, stk. 1, nr. 2, vil blive straffet med bøde.

Det foreslås i *nr. 3*, at den, der undlader at efterkomme Styrelsen for Samfundssikkerheds påbud efter § 13, stk. 5, eller § 18, stk. 1 og 2, straffes med bøde.

Det følger af den foreslåede bestemmelse, at den, der undlader at efterkomme Styrelsen for Samfundssikkerheds påbud om at iværksætte nærmere angivne sikkerhedsforanstaltninger i beredskabssituationer og andre ekstraordinære situationer efter den foreslåede § 13, stk. 5, vil blive straffet med bøde.

Det følger endvidere af den foreslåede bestemmelse, at den væsentlige eller vigtige teleudbydere, der undlader at efterkomme Styrelsen for Samfundssikkerheds påbud om at inddrage nærmere angivne områder af deres virksomhed og nærmere angivne trusler mod sikkerheden i net- og informationssystemer i deres foranstaltninger efter § 5, stk. 1, vil blive straffet med bøde.

Det foreslås i *nr. 4,* at den, der undlader at efterkomme Styrelsen for Samfundssikkerheds krav efter § 19, stk. 1, nr. 5-8, eller § 22, stk. 1, nr. 4-7, straffes med bøde.

Det følger af den foreslåede bestemmelse, at en væsentlig teleudbyder, der undlader at efterkomme Styrelsen for Samfundssikkerheds krav efter § 19, stk. 1, nr. 5-8, om udlevering af oplysninger, få adgang til data, dokumenter og oplysninger, udlevering af dokumentation mv., vil blive straffet med bøde.

Det følger endvidere af den foreslåede bestemmelse en vigtig teleudbyder, der undlader at efterkomme Styrelsen for Samfundssikkerheds krav efter § 22, stk. 1, nr. 4-7, om udlevering af oplysninger, adgang til data, dokumenter og oplysninger, udlevering af dokumentation mv., vil blive straffet med bøde.

Det foreslås i *nr. 5,* at den, der hindrer Styrelsen for Samfundssikkerhed i at føre tilsyn efter bestemmelserne i § 19, stk. 1, nr. 1-4, eller § 22, stk. 1, nr. 1-3, straffes med bøde.

Det følger af den foreslåede bestemmelse, at væsentlige teleudbydere, der hindrer Styrelsen for Samfundssikkerhed i at føre tilsyn efter bestemmelserne i den foreslåede § 19, stk. 1, nr. 1-4, om kontrol, sikkerhedsaudits, sikkerhedsscanninger mv., vil blive straffes med bøde.

Det følger endvidere af den foreslåede bestemmelse, at vigtige teleudbydere, der hindrer Styrelsen for Samfundssikker-

hed i at føre tilsyn efter bestemmelserne i den foreslåede § 22, stk. 1, nr. 1-3, om kontrol, sikkerhedsaudits, sikkerhedsscanninger mv, vil blive straffet med bøde.

Det følger af det foreslåede *stk. 2,* at der kan pålægges selskaber mv. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.

Den foreslåede bestemmelse indebærer, at selskaber mv. (juridiske personer) kan pålægges strafansvar for overtrædelse af denne lov eller regler udstedt i medfør af loven efter reglerne i straffelovens kapitel 5.

Det følger af det foreslåede *stk. 3,* at der i forskrifter, der udstedes i medfør af loven fastsættes straf af bøde for overtrædelse af bestemmelserne i forskrifterne.

Med bestemmelsen bemyndiges ministeren for samfundssikkerhed og beredskab til at fastsætte straf i form af bøde for overtrædelse af bestemmelser i regler, som udstedes i medfør af loven.

Det følger af artikel 34, stk. 4, i NIS 2-direktivet, at medlemsstaterne skal sikre, at hvor væsentlige enheder overtræder artikel 21 (foranstaltninger til styring af cybersikkerhedsrisici) eller artikel 23 (rapporteringsforpligtelser), straffes de i overensstemmelse med nærværende artikels stk. 2 og 3 med administrative bøder med et maksimum på mindst 10.000.000 euro eller et maksimum på mindst 2 pct. af den samlede globale årsomsætning i det foregående regnskabsår i den virksomhed, som den væsentlige enhed tilhører, alt efter hvad der er højest.

Efter NIS 2-direktivets artikel 34, stk. 5, skal medlemsstaterne sikre, at hvor vigtige enheder overtræder artikel 21 (foranstaltninger til styring af cybersikkerhedsrisici) eller artikel 23 (rapporteringsforpligtelser), straffes de i overensstemmelse med nærværende artikels stk. 2 og 3 med administrative bøder med et maksimum på mindst 7.000.000 euro eller et maksimum på mindst 1,4 pct. af den samlede globale årsomsætning i det foregående regnskabsår i den virksomhed, som den vigtige enhed tilhører, alt efter hvad der er højest.

Det forudsættes i overensstemmelse med en minimumsimplementering af NIS 2-direktivets artikel 34, stk. 4, at bødens størrelse for væsentlige enheders overtrædelse af regler fastsat i medfør af den foreslåede bestemmelse i § 6, stk. 3, maksimalt vil udgøre et beløb svarende til 10.000.000 euro eller 2 pct. af den væsentlige enheds samlede globale årsomsætning i det foregående regnskabsår alt efter, hvad der er højest.

Det forudsættes i overensstemmelse med en minimumsimplementering af NIS 2-direktivets artikel 34, stk. 5, at bødens størrelse for vigtige enheders overtrædelse af regler fastsat i medfør af den foreslåede bestemmelse i § 6, stk. 3, maksimalt vil udgøre et beløb svarende til 7.000.000 euro eller 1,4 pct. af den vigtige enheds samlede globale årsomsætning i det foregående regnskabsår alt efter, hvad der er højest.

Der forudsættes ikke i tilknytning til øvrige bestemmelser end § 6, stk. 3, anlagt særlige forudsætninger for så vidt angår udmålingen af bøders størrelse. Det samme gælder eventuel udmåling af bøder til fysiske personer, hvor det dog i overensstemmelse med direktivets præambelbetragtning nr. 130, 2. pkt., forudsættes, at der lægges vægt på det generelle indkomstniveau og personens økonomiske stilling.

Det forudsættes i overensstemmelse med NIS 2-direktivets artikel 34, stk. 3, jf. artikel 32, stk. 7, at der lægges vægt på følgende hensyn ved pålæg af en bøde og ved udmåling af bødens størrelse: 1) overtrædelsens grovhed og vigtigheden af de overtrådte bestemmelser, idet bl.a. følgende under alle omstændigheder skal betragtes som alvorlige overtrædelser: a) Gentagne overtrædelser, b) manglende underretning om eller afhjælpning af væsentlige hændelser, c) manglende afhjælpning af mangler efter bindende instrukser fra kompetente myndigheder, d) hindringer for audits eller overvågningsaktiviteter beordret af den kompetente myndighed efter konstatering af en overtrædelse og e) afgivelse af urigtige eller klart unøjagtige oplysninger vedrørende cybersikkerhedsrisikostyringsforanstaltninger eller rapporteringsforpligtelser, der er fastsat i §§ 6, 13, 14, 16 og 17, 2) overtrædelsens varighed, 3) den pågældende enheds relevante tidligere overtrædelser, 4) enhver materiel eller immateriel skade, der er forårsaget, herunder ethvert finansielt eller økonomisk tab, virkninger for andre tjenester og antallet af brugere, der er berørt, 5) hvorvidt der ved overtrædelsen er handlet forsætligt eller uagtsomt, 6) enhver foranstaltning truffet af enheden for at forebygge eller afbøde den materielle eller immaterielle skade, 7) hvorvidt godkendte adfærdskodekser eller godkendte certificeringsmekanismer er overholdt, og 8) i hvilken udstrækning de fysiske eller juridiske personer, der holdes ansvarlige for overtrædelsen, samarbejder med de kompetente myndigheder.

Den fastsatte bøde skal i overensstemmelse med NIS 2-direktivets artikel 34, stk. 1, være effektiv, stå i et rimeligt forhold til overtrædelsen og have afskrækkende virkning under hensyntagen til omstændighederne i den konkrete sag.

Bøde vil i overensstemmelse med NIS 2-direktivets artikel 34, stk. 2, kunne pålægges i tillæg til håndhævelsesforanstaltningerne i de foreslåede §§ 20, 21 og 23.

Det bemærkes, at fastsættelsen af straffen fortsat vil bero på domstolenes konkrete vurdering i det enkelte tilfælde af samtlige omstændigheder i sagen, og de angivne strafniveauer vil kunne fraviges i op- eller nedadgående retning, hvis der i den konkrete sag foreligger skærpende eller formildende omstændigheder, jf. herved de almindelige regler om straffens fastsættelse i straffelovens 10. kapitel.

Der henvises i øvrigt til lovforslagets pkt. 3.9.

Til § 32

Det foreslås i *stk. 1*, at loven træder i kraft den 1. juli 2025.

Det følger af artikel 41, stk. 1, i NIS 2-direktivet, at direktivet skal være gennemført i dansk ret senest den 17. oktober 2024 og træde i kraft senest den 18. oktober 2024. Med den foreslåede bestemmelse vil loven træde i kraft 9 måneder efter direktivets implementeringsfrist.

Det foreslås i *stk. 2,* at lov om sikkerhed i net og tjenester, jf. lovbekendtgørelse nr. 153 af 1. februar 2021, som ændret ved § 18 i lov nr. 1156 af 8. juni 2021, ophæves ved denne lovs ikrafttræden.

Det foreslås i *stk. 3,* at oplysninger efter stk. 7, skal indgives senest den 1. oktober 2025.

Det bemærkes, at der er tale om en overgangsbestemmelse.

Der henvises i den forbindelse til den foreslåede bestemmelse i § 7, stk. 2, hvorefter væsentlige og vigtige teleudbydere senest to uger efter, at teleudbyderen er bekendt med, at denne er omfattet af loven, skal indgive de i den foreslåede § 7, stk. 1, nævnte oplysninger.

Til § 33

Det foreslås i *§ 33*, at loven ikke skal gælde for Færøerne og Grønland.

Baggrunden for den foreslåede territorialbestemmelse er, at sagsområdet for telekommunikation er overtaget af henholdsvis de færøske og grønlandske myndigheder.

Til § 34

Det foreslås i *nr. 1,* at § 1, nr. 3 i lov om leverandørsikkerhed i den kritiske teleinfrastruktur ændres, således at definitionerne i nærværende lovforslag og den nævnte lov er ensartede.

Det foreslås således, at vigtige teleudbydere i lov om leverandørsikkerhed i den kritiske teleinfrastruktur defineres som en teleudbyder, som er identificeret som en vigtig teleudbyder i henhold til lov om sikkerhed og beredskab i telesektoren.

Det foreslås i nr. *2,* at nærværende lovforslags definition af væsentlige teleudbydere indsættes i lov om leverandørsikkerhed i den kritiske teleinfrastruktur.

Det foreslås i *nr. 3,* at der foretages konsekvensrettelser af definitionerne af teleudbydere i overensstemmelse med definitionerne i nærværende lov med henblik på at sikre ensartet begrebsanvendelse.

Bilag 1

Lovforslaget sammenholdt med gældende lov

Gældende formulering	*Lovforslaget*
	§ 34
	I lov. nr. 1156 af 8. juni 2021 om leverandørsikkerhed i den kritiske teleinfrastruktur foretages følgende ændringer:
§ 1. I denne lov forstås ved:	**1.** *§ 1, nr. 3,* affattes således:
1) ---	»3) Vigtig teleudbyder: En teleudbyder, som er identificeret som en vigtig teleudbyder i henhold til lov om sikkerhed og beredskab i telesektoren «.
2) ---	
3) Væsentlig erhvervsmæssig udbyder af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester:	
a) ---	
b) ---	
	2. I § 1 indsættes som *nr. 4:*
	»4) Væsentlig teleudbyder: En teleudbyder, som er identificeret som en væsentlig teleudbyder i henhold til lov om sikkerhed og beredskab i telesektoren.«
§ 2. Center for Cybersikkerhed kan i særlige tilfælde forbyde en væsentlig erhvervsmæssig udbyder af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester at indgå en aftale, der vedrører kritiske netkomponenter, systemer og værktøjer, herunder varetagelsen af driften heraf, hvis aftalen vurderes at udgøre en trussel mod statens sikkerhed.	**3.** *§ 2, stk. 1, § 3, stk. 1* og *2,* og
	§ 15, ændres »væsentlig erhvervsmæssig udbyder af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester« til: »væsentlig eller vigtig teleudbyder«.
Stk. 2. ---	
1) ---	
2) ---	
3) ---	
4) ---	
Stk. 3. ---	
§ 3. Center for Cybersikkerhed kan i særlige tilfælde forbyde en væsentlig erhvervsmæssig udbyder af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester at opretholde en indgået aftale, der vedrører kritiske netkomponenter, systemer og værktøjer, herunder varetagelsen af driften heraf, hvis opretholdelse af aftalen vurderes at udgøre en væsentlig trussel mod statens sikkerhed. Ved vurderingen heraf kan Center for Cybersikkerhed lægge vægt på de forhold, som fremgår af § 2, stk. 2.	

Stk. 2. Center for Cybersikkerhed kan endvidere i særlige tilfælde forbyde en væsentlig erhvervsmæssig udbyder af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester at anvende kritiske netkomponenter, systemer og værktøjer, der er leveret, hvis anvendelsen vurderes at udgøre en væsentlig trussel mod statens sikkerhed. Ved vurderingen heraf kan Center for Cybersikkerhed lægge vægt på de forhold, som fremgår af § 2, stk. 2.

Stk. 3. ---

Stk. 4. ---

§ 15. Hvis en væsentlig erhvervsmæssig udbyder af offentligt tilgængelige elektroniske kommunikationsnet og –tjenester ikke efterlever et forbud efter § 2, stk. 1, eller § 3, stk. 1 eller 2, kan Center for Cybersikkerhed træffe afgørelse om at afsætte medlemmer af udbyderens ledelse.