FOLKETINGET

Folketingstidende
Tillæg A

Lovforslag nr. **L 141** Folketinget 2024-25

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

Forslag

til

Lov om om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS 2-loven)[1)]

Kapitel 1

Anvendelsesområde, jurisdiktion, definitioner m.v.

§ 1. Loven finder anvendelse på offentlige og private enheder, der er omfattet af lovens bilag 1 og 2, jf. dog stk. 2-4 og 6.

Stk. 2. Loven finder ikke anvendelse på enheder i det omfang, de er omfattet af lov om styrket beredskab i energisektoren. Loven finder ikke anvendelse på enheder i det omfang, de er omfattet af lov om sikkerhed og beredskab i telesektoren, jf. dog § 1, stk. 2, i denne lov. Loven finder endvidere ikke anvendelse for enheder, der er udpeget i medfør af § 333, stk. 1, i lov om finansiel virksomhed.

Stk. 3. Loven finder ikke anvendelse på enheder, hvor sektorspecifikke EU-retsakter og eventuel national gennemførelse heraf har mindst samme virkning som bestemmelserne i §§ 6, 12, 13 og 15.

Stk. 4. Vedkommende minister kan inden for sit område træffe afgørelse om at undtage specifikke enheder, såfremt enhederne udfører aktiviteter inden for national sikkerhed, offentlig sikkerhed, forsvar eller retshåndhævelse, herunder forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger, eller som udelukkende leverer tjenester til offentlige forvaltningsenheder, der udfører disse aktiviteter, fra forpligtelserne i §§ 6, 8, 12, 13, 15 og 16 for så vidt angår disse aktiviteter eller tjenester. Udfører enheder udelukkende aktiviteter eller leverer tjenester af den type, som omhandlet i 1. pkt., kan vedkommende minister endvidere træffe afgørelse om at fritage disse enheder for forpligtelserne i medfør af §§ 9 og 10, jf. dog stk. 5.

Stk. 5. Der kan ikke fastsættes regler efter stk. 4, hvor en enhed fungerer som tillidstjenesteudbyder.

Stk. 6. Vedkommende minister kan efter forhandling med ministeren for samfundssikkerhed og beredskab fastsætte regler om, at loven helt eller delvist også finder anvendelse på henholdsvis offentlige forvaltningsenheder på lokalt plan og uddannelsesinstitutioner.

§ 2. Under dansk jurisdiktion hører enheder, der er omfattet af lovens anvendelsesområde, og som er etableret i Danmark, jf. dog stk. 2.

Stk. 2. DNS-tjenesteudbydere, topdomænenavneadministratorer, enheder, der leverer domænenavnsregistreringstjenester, og udbydere af henholdsvis cloudcomputingtjenester, datacentertjenester, indholdsleveringsnetværk, administrerede tjenester, administrerede sikkerhedstjenester, onlinemarkedspladser, onlinesøgemaskiner og platforme for sociale netværkstjenester, der har deres hovedforretningssted i Danmark, jf. stk. 3, hører under dansk jurisdiktion.

Stk. 3. En enhed som nævnt i stk. 2 anses for at have sit hovedforretningssted i Den Europæiske Union i den medlemsstat, hvor beslutningerne vedrørende foranstaltningerne til styring af cybersikkerhedsrisici overvejende træffes. Kan en sådan medlemsstat ikke fastslås, eller hvis sådanne beslutninger ikke træffes i Den Europæiske Union, anses hovedforretningsstedet for at være i den medlemsstat, hvor der udføres cybersikkerhedsoperationer. Kan en sådan medlemsstat ikke fastslås, anses hovedforretningsstedet for at være i den medlemsstat, hvor den pågældende enheds forretningssted med det største antal ansatte i Den Europæiske Union er beliggende.

Stk. 4. Er en enhed som nævnt i stk. 2 ikke etableret i Den Europæiske Union, men udbyder tjenester inden for Unionen, herunder i Danmark, skal enheden udpege en repræsentant, der er etableret i en af de medlemsstater i Uni-

[1)] Loven gennemfører 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. 2025-77

onen, hvor enhedens tjenester udbydes. Er repræsentanten etableret i Danmark, hører enheden under dansk jurisdiktion. Er der ikke udpeget en repræsentant efter 1. pkt., anses enheden for at høre under jurisdiktionen i de medlemsstater, hvor tjenesterne udbydes.

§ 3. I denne lov forstås ved følgende:

1) Centralt kontaktpunkt: Den myndighed, der udøver forbindelsesfunktionen for at sikre grænseoverskridende samarbejde mellem de danske myndigheder, myndigheder i andre medlemsstater i Den Europæiske Union og Den Europæiske Unions institutioner, samt for at sikre tværsektorielt samarbejde mellem de nationale kompetente myndigheder.
2) Cloudcomputingtjeneste: En digital tjeneste, som muliggør on demand-administration og giver bred fjernadgang til en skalerbar og fleksibel pulje af delbare computerressourcer, herunder hvor disse ressourcer er fordelt mellem flere lokaliteter.
3) Cybersikkerhed: De aktiviteter, der er nødvendige for at beskytte net- og informationssystemer, brugerne af sådanne systemer og andre personer berørt af cybertrusler.
4) 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.
5) Datacentertjeneste: En tjeneste, der omfatter strukturer eller grupper af strukturer, som er beregnet til central opbevaring, sammenkobling og drift af it- og netværksudstyr, der leverer datalagrings-, databehandlings- og datatransporttjenester, samt alle faciliteter og infrastrukturer til energidistribution og miljøkontrol.
6) Digital tjeneste: Enhver tjeneste i informationssamfundet, dvs. enhver tjeneste, der normalt ydes mod betaling, og som teleformidles ad elektronisk vej på individuel anmodning fra en tjenestemodtager.
7) DNS-tjenesteudbyder: En enhed, der leverer
   a) offentligt tilgængelige rekursive domænenavnsoversættelsestjenester til internetslutbrugere, eller
   b) autoritative domænenavnsoversættelsestjenester til tredjepartsbrug, med undtagelse af rodnavneservere.
8) Domænenavnesystem (DNS): Et hierarkisk distribueret navngivningssystem, der gør det muligt at identificere internettjenester og -ressourcer, således at slutbrugerudstyr kan benytte internetrouting- og konnektivitetstjenester til at nå disse tjenester og ressourcer.
9) Enhed: En fysisk eller juridisk person, der er oprettet og anerkendt som sådan i henhold til den nationale ret på det sted, hvor den er etableret, og som i eget navn kan udøve rettigheder og være underlagt forpligtelser.
10) Enhed, der leverer domænenavnsregistreringstjenester: En registrator eller en agent, der handler på vegne af registratorer, såsom en udbyder eller videresælger af privatlivs- eller proxyregistreringstjenester.
11) Forskningsorganisation: En enhed, hvis primære mål er at udføre anvendt forskning eller udvikling med henblik på at udnytte resultaterne af denne forskning til kommercielle formål. Indbefatter ikke uddannelsesinstitutioner.
12) 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.
13) 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.
14) IKT-proces: Aktiviteter, der udføres for at udforme, udvikle, levere eller vedligeholde et IKT-produkt eller en IKT-tjeneste.
15) IKT-produkt: Et element eller en gruppe af elementer i net- og informationssystemer.
16) IKT-tjeneste: En tjeneste, der helt eller hovedsageligt består af overførsel, lagring, indhentning eller behandling af oplysninger ved hjælp af net- og informationssystemer.
17) Indholdsleveringsnetværk: Et net af geografisk distribuerede servere med det formål at sikre høj tilgængelighed af, adgang til eller hurtig levering af digitalt indhold og digitale tjenester til internetbrugere på vegne af indholds- og tjenesteudbydere.
18) Kvalificeret tillidstjeneste: En tillidstjeneste, der opfylder de krav, der er fastsat i Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF.
19) Kvalificeret tillidstjenesteudbyder: En tillidstjenesteudbyder, der udbyder en eller flere kvalificerede tillidstjenester og har fået tildelt status som kvalificeret tillidstjenesteudbyder af tilsynsorganet i medfør af Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF.
20) Net- og informationssystem:
   a) Et elektronisk kommunikationsnet, hvorved forstås transmissionssystemer, uanset om de bygger på en permanent infrastruktur eller 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, samt kabel-tv-net, uanset hvilken type information der overføres.

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.

21) 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.

22) Onlinemarkedsplads: En tjenesteydelse, der gør brug af software, herunder et websted, en del af et websted eller en applikation, der drives af eller på vegne af den erhvervsdrivende, der giver forbrugere mulighed for at indgå fjernsalgsaftaler med andre erhvervsdrivende eller forbrugere.

23) Onlinesøgemaskine: En digital tjeneste, som giver brugerne mulighed for at indtaste forespørgsler for at foretage søgninger på principielt alle websteder eller alle websteder på et bestemt sprog på grundlag af en forespørgsel om et hvilket som helst emne ved hjælp af et søgeord, en stemmesøgning, en sætning eller andet input, og som fremviser resultater i et hvilket som helst format, hvor der kan findes oplysninger om det ønskede indhold.

24) Platform for sociale netværkstjenester: En platform, der sætter slutbrugere i stand til at komme i forbindelse med hinanden på tværs af forskellige anordninger, navnlig via chats, opslag, videoer og anbefalinger.

25) Repræsentant: En fysisk eller juridisk person, der er etableret i Den Europæiske Union, som udtrykkeligt er udpeget til at handle på vegne af en DNS-tjenesteudbyder, en topdomænenavneadministrator, en enhed, der leverer domænenavnsregistreringstjenester, eller en udbyder af cloudcomputingtjenester, af datacentertjenester, af indholdsleveringsnetværk, af administrerede tjenester, af administrerede sikkerhedstjenester, af onlinemarkedspladser, af onlinesøgemaskiner eller af platforme for sociale netværkstjenester, som ikke er etableret i Den Europæiske Union, og som kan kontaktes af en kompetent myndighed eller en Computer Incident Response Team (CSIRT) på enhedens sted for så vidt angår denne enheds forpligtelser i henhold til NIS 2-direktivet.

26) Risiko: Potentialet for tab eller forstyrrelse som følge af en hændelse, og som kommer til udtryk som en kombination af størrelsen af et sådant tab eller en sådan forstyrrelse og sandsynligheden for, at hændelsen indtræffer.

27) Sikkerhed i net- og informationssystemer: Net- og informationssystemers evne til, på et givent 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.

28) Sårbarhed: En svaghed, modtagelighed eller fejl ved IKT-produkter eller -tjenester, som kan udnyttes af en cybertrussel.

29) Tillidstjeneste: En elektronisk tjeneste, der normalt udføres mod betaling, og som består af

a) generering, kontrol og validering af elektroniske signaturer, elektroniske segl eller elektroniske tidsstempler eller elektroniske registrerede leveringstjenester og certifikater relateret til tjenester,

b) generering, kontrol og validering af certifikater for webstedsautentifikation eller

c) bevaring af elektroniske signaturer, segl eller certifikater relateret til disse tjenester.

30) Tillidstjenesteudbyder: En fysisk eller juridisk person, der udbyder en eller flere tillidstjenester, enten som en kvalificeret eller ikke-kvalificeret tillidstjenesteudbyder.

31) Topdomænenavneadministrator: En enhed, der har fået uddelegeret et specifikt topdomæne, og som er ansvarlig for at administrere topdomænet, herunder registrering af domænenavne under topdomænet og den tekniske drift af topdomænet, hvilket inkluderer driften af dets navneservere, vedligeholdelsen af dets databaser og distributionen af topdomænezonefiler til navneservere, uanset om nogen af disse operationer udføres af enheden selv eller outsources, men ikke situationer, hvor topdomænenavne kun anvendes af en administrator til eget brug.

32) Udbyder af administrerede sikkerhedstjenester: En udbyder af administrerede tjenester, der udfører eller yder assistance til aktiviteter vedrørende styring af cybersikkerhedsrisici.

33) Udbyder af administrerede tjenester: En enhed, der leverer tjenester i forbindelse med installation, administration, drift eller vedligeholdelse af IKT-produkter, -net, -infrastruktur, -applikationer eller andre net- og informationssystemer via assistance eller aktiv administration, der udføres enten i kundernes lokaler eller på afstand.

34) Væsentlig cybertrussel: En cybertrussel, som på grundlag af sine tekniske karakteristika kan antages at have potentiale til at få alvorlig indvirkning på en enheds net- og informationssystemer eller på brugerne af enhedens tjenester ved at forårsage betydelig fysisk eller ikke-fysisk skade.

Væsentlige enheder

§ 4. Enheder af en type, som er omfattet af lovens bilag 1 anses for at være væsentlige enheder, hvis enheden opfylder én af følgende betingelser, jf. dog stk. 2 og 3:

1) Enheden beskæftiger mere end 250 personer.

2) Enheden har en årlig omsætning på over 50 mio. EUR og en årlig samlet balance på over 43 mio. EUR.

Stk. 2. Kommuner og regioner anses som væsentlige enheder, såfremt de med et kommercielt formål udfører opgaver som udbydere af offentlige elektroniske kommunikationsnet eller udbydere af offentligt tilgængelige elektroniske kommunikationstjenester, og opfylder mindst én af følgende betingelser:

1) Enheden beskæftiger mere end 50 personer.
2) Enheden har en årlig omsætning på over 10 mio. EUR og en årlig samlet balance på over 10 mio. EUR.

Stk. 3. Uanset deres størrelse anses følgende enheder for at være væsentlige enheder:

1) Kvalificerede tillidstjenesteudbydere og topdomæneadministratorer samt DNS-tjenesteudbydere.
2) Offentlige forvaltningsenheder under den centrale forvaltning.
3) Enheder, der er identificeret som kritiske enheder i henhold til lov om kritiske enheders modstandsdygtighed (CER-loven).
4) Enheder, der er blevet identificeret som operatører af væsentlige tjenester i overensstemmelse med 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 I-direktivet), jf. dog § 5, stk. 2.
5) Øvrige enheder af en type, som er omfattet af lovens bilag 1 eller 2, hvor mindst én af følgende betingelser er opfyldt, jf. dog § 5, stk. 2:
   a) Enheden er den eneste udbyder i Danmark af en tjeneste, der er væsentlig for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter.
   b) En forstyrrelse af den tjeneste, som enheden leverer, vil kunne have væsentlig indvirkning på den offentlige sikkerhed eller folkesundheden.
   c) En forstyrrelse af den tjeneste, som enheden leverer, vil kunne medføre en væsentlig systemisk risiko, navnlig for sektorer hvor en sådan forstyrrelse kan have en grænseoverskridende virkning.
   d) 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 Danmark.

Stk. 4. Vedkommende minister kan efter forhandling med ministeren for samfundssikkerhed og beredskab fastsætte nærmere regler om, hvornår enheder er omfattet af stk. 3, nr. 5.

Vigtige enheder

§ 5. Enheder af en type, som er omfattet af lovens bilag 1 eller 2, anses for at være vigtige enheder, hvis enheden ikke opfylder kriterierne for at være væsentlige enheder i medfør af § 4, og enheden opfylder mindst én af følgende betingelser:

1) Enheden beskæftiger mere end 50 personer eller
2) Enheden har en årlig omsætning på over 10 mio. EUR og en årlig samlet balance på over 10 mio. EUR.

Stk. 2. Den kompetente myndighed kan træffe afgørelse om, at en enhed uanset størrelse, som er omfattet af § 4, stk. 3, nr. 4 eller 5, skal anses for at være en vigtig enhed.

Kapitel 2

Foranstaltninger til styring af cybersikkerhedsrisici

§ 6. Væsentlige og vigtige enheder 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 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 enhed og dens 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 cybersikkerhedsrisici.
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 enheden, hvor det er relevant.

Stk. 2. En enhed, 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. Vedkommende minister kan efter forhandling med ministeren for samfundssikkerhed og beredskab fastsætte nærmere regler om foranstaltninger efter stk. 1.

§ 7. De foranstaltninger, som en væsentlig eller vigtig enhed træffer på baggrund af § 6, stk. 1 og 2, samt regler fastsat i medfør af § 6, stk. 3, skal være godkendt af enhedens ledelsesorgan. Ledelsesorganet fører tilsyn med foranstaltningernes gennemførelse.

Stk. 2. Medlemmerne af en væsentlig eller vigtig enheds ledelsesorgan skal deltage i relevante kurser om styring af cybersikkerhedsrisici og tilskynde til at tilsvarende kurser tilbydes til enheden øvrige ansatte.

§ 8. Vedkommende minister kan efter forhandling med ministeren for samfundssikkerhed og beredskab fastsætte regler om, at væsentlige og vigtige enheder skal anvende særlige IKT-produkter, -tjenester og -processer, som er certificeret i henhold til en europæisk cybersikkerhedscertificeringsordning for at påvise overensstemmelse med bestemte krav i § 6, stk. 1, eller regler om foranstaltninger fastsat i medfør af § 6, stk. 3. Produktet kan udvikles af den væsentlige eller vigtige enhed eller indkøbes fra tredjeparter.

Kapitel 3

Registrerings- og underretningspligter

§ 9. DNS-tjenesteudbydere, topdomænenavneadministratorer, enheder der leverer domænenavnsregistreringstjenester og udbydere af cloudcomputingtjenester, datacentertjenester, indholdsleveringsnetværk, administrerede tjenester, administrerede sikkerhedstjenester, onlinemarkedspladser, onlinesøgemaskiner og platforme for sociale netværkstjenester skal registrere sig hos den relevante kompetente myndighed og i den forbindelse oplyse følgende:

1) Enhedens navn.
2) Enhedens adressen på enhedens hovedforretningssted og dens andre forretningssteder i Den Europæiske Union eller, hvis den ikke er etableret i Unionen, den repræsentant, der er udpeget i henhold til § 2, stk. 4, 1. pkt.
3) Den relevante sektor, delsektor og typen som enheden udgør, jf. lovens bilag 1 eller 2.
4) Ajourførte kontaktoplysninger, herunder e-mailadresser, IP-intervaller og telefonnumre på enheden og kontaktoplysninger på en eventuel udpeget repræsentant i henhold til § 2, stk. 4.
5) De medlemsstater i Den Europæiske Union, hvor enheden leverer tjenester.

Stk. 2. Oplysningerne efter stk. 1, skal indgives senest tre måneder efter, at enheden omfattes af loven.

Stk. 3. I tilfælde af ændringer i de oplysninger, der er afgivet i medfør af stk. 1, skal enheden give den relevante kompetente myndighed underretning herom senest tre måneder efter datoen for ændringen.

§ 10. Væsentlige og vigtige enheder samt enheder, der leverer domænenavnsregistreringstjenester, skal registrere sig hos den relevante kompetente myndighed og i den forbindelse oplyse følgende, jf. dog § 9:

1) Enhedens navn.
2) Adresse og ajourførte kontaktoplysninger, herunder e-mailadresser, IP-intervaller og telefonnumre.
3) Den relevante sektor og delsektor, som enheden er omfattet af, jf. lovens bilag 1 eller 2.
4) En liste over de øvrige medlemsstater i Den Europæiske Union, hvor enheden leverer tjenester, der er omfattet af anvendelsesområdet i artikel 2 i NIS 2-direktivet.

Stk. 2. Oplysningerne efter stk. 1 skal indgives senest to uger efter, at enheden omfattes af loven.

Stk. 3. I tilfælde af ændring i de oplysninger, der er afgivet i medfør af stk. 1, skal enheden give den relevante kompetente myndighed underretning herom senest to uger efter datoen for ændringen.

Database over domænenavnsregistreringsdata

§ 11. Topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester, skal føre en særskilt database, der indeholder nøjagtige og fuldstændige domænenavnsregistreringsdata.

Stk. 2. Databasen efter stk. 1 skal indeholde oplysninger om følgende:

1) Domænenavnet.
2) Registreringsdatoen.
3) Den registreredes navn, e-mailadresse og telefonnummer.
4) E-mailadresse og telefonnummer på det kontaktpunkt, der administrerer domænenavnet, hvis kontaktpunktet er forskelligt fra den registrerede.

Stk. 3. Topdomænenavneadministratorerne og enheder, der leverer domænenavnsregistreringstjenester, skal indføre politikker og procedurer, herunder verifikationsprocedurer, for at sikre, at databaserne indeholder nøjagtige og fuldstændige oplysninger. Politikkerne og procedurerne skal gøres offentligt tilgængelige.

Stk. 4. Topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester, skal uden unødigt ophold efter registreringen af et domænenavn gøre domænenavnsregistreringsdata, som ikke er personoplysninger, offentligt tilgængelige.

Stk. 5. Topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester, skal på baggrund af en anmodning og efter en konkret vurdering af nødvendigheden give legitime adgangssøgende adgang til specifikke domænenavnsregistreringsdata, herunder personoplysninger. Anmodninger skal besvares senest inden for 72 timer efter modtagelse af anmodningen. Topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester, skal indføre og offentliggøre politikker og procedurer for adgangen til data.

Stk. 6. Topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester, skal samarbejde om overholdelsen af de forpligtelser, der er fastsat i stk. 1-5, med henblik på at undgå dobbeltindsamling af domænenavnsregistreringsdata.

Stk. 7. Den kompetente myndighed kan meddele topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester, forbud eller påbud for at sikre overholdelsen af kravene efter stk. 1-6 eller regler udstedt i medfør af stk. 8.

Stk. 8. Digitaliseringsministeren kan fastsætte nærmere regler om krav til politikker og procedurer efter stk. 3 og 5.

Underretningspligter

§ 12. Væsentlige og vigtige enheder skal underrette den relevante kompetente myndighed og Computer Security Incident Response Team (CSIRT) om enhver væsentlig hændelse. En underretning skal indeholde oplysninger, der gør det muligt at fastslå eventuelle grænseoverskridende virkninger af hændelsen.

Stk. 2. En hændelse anses for at være væsentlig, hvis én af følgende betingelser er opfyldt:

1) Hændelsen har forårsaget eller er i stand til at forårsage alvorlige driftsforstyrrelser af tjenesterne eller økonomiske tab for den berørte enhed.
2) Hændelsen en har påvirket eller er i stand til at påvirke andre fysiske eller juridiske personer ved at forårsage betydelig fysisk eller ikke-fysisk skade.

Stk. 3. Vedkommende minister kan efter forhandling med ministeren for samfundssikkerhed og beredskab fastsætte nærmere regler om, hvornår en hændelse kan anses for at være væsentlig.

§ 13. Underretning efter § 12, stk. 1, 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 senest inden for 24 timer efter, at enheden 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 under alle omstændigheder inden for 72 timer efter, at enheden har fået kendskab til den væsentlige hændelse, jf. dog stk. 2.
3) En foreløbig rapport med relevante statusopdateringer sendes efter anmodning fra CSIRT'en.
4) En endelig rapport sendes senest én 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.
   d) De eventuelle grænseoverskridende virkninger af hændelsen.
5) Pågår hændelsen fortsat på tidspunktet for fremsendelsen af den endelige rapport, jf. nr. 4, skal den underrettende enhed indsende en statusrapport på det pågældende tidspunkt og en endelig rapport senest en måned efter, at hændelsen er håndteret.

Stk. 2. Tillidstjenesteudbydere skal i tilfælde af væsentlige hændelser afgive underretningen efter stk. 1, nr. 2, uden unødigt ophold og senest inden for 24 timer efter at være blevet bekendt med den væsentlige hændelse.

Stk. 3. CSIRT'en sikrer, at den underrettende enhed uden unødigt ophold og 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 enheden skal CSIRT'en desuden yde vejledning, operativ rådgivning om gennemførelsen af mulige afbødende foranstaltninger og supplerende teknisk bistand.

Frivillige underretninger

§ 14. Offentlige og private enheder kan, uanset at de ikke er omfattet af lovens anvendelsesområde, underrette CSIRT'en om hændelser, nærvedhændelser og cybertrusler.

Stk. 2. CSIRT'en behandler underretninger efter stk. 1 på samme måde som underretninger modtaget i medfør af § 13. CSIRT'en kan prioritere håndteringen af underretninger, der er modtaget i medfør af § 13 fremfor underretninger efter stk. 1.

Stk. 3. Underretninger efter stk. 1 er undtaget fra aktindsigt efter lov om offentlighed i forvaltningen og partsaktindsigt efter forvaltningsloven.

Kapitel 4

Underretning og oplysning om væsentlige hændelser

§ 15. Væsentlige og vigtige enheder underretter uden unødigt ophold modtagerne af deres tjenester om væsentlige hændelser, der sandsynligvis vil påvirke leveringen af deres tjenester negativt.

Stk. 2. Væsentlige og vigtige enheder 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 herpå. Enhederne skal også informere de pågældende modtagere om den væsentlige cybertrussel, hvor det er relevant.

§ 16. Den relevante kompetente myndighed kan efter høring af en enhed, der er ramt af en væsentlig hændelse, informere offentligheden om den væsentlige hændelse, hvis offentliggørelsen er nødvendig for at forebygge videre udbredelse af eller håndtere hændelsen, eller hvis offentliggørelse af hændelsen på anden vis er i offentlighedens interesse.

Stk. 2. Den kompetente myndighed kan i de situationer, der er nævnt i stk. 1, træffe afgørelse om, at den relevante enhed 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 5

CSIRT'ens opgaver

§ 17. CSIRT'en håndterer it-sikkerhedshændelser og varetager de opgaver, der relaterer sig hertil, herunder følgende opgaver i forhold til væsentlige og vigtige enheder:

1) Efter anmodning fra en væsentlig eller vigtig enhed at yde bistand vedrørende realtids- eller nærrealtidsmonitorering af enhedens net- og informationssystemer.

2) At reagere på hændelser og i den forbindelse yde bistand til de berørte enheder.
3) Efter anmodning fra en væsentlig eller vigtig enhed at foretage en proaktiv scanning af enhedens net- og informationssystemer, der anvendes til levering af enhedens tjenester, for at opdage sårbarheder med en potentielt væsentlig indvirkning.

Stk. 2. Ved udførelsen af opgaver efter stk. 1 kan CSIRT'en prioritere særlige opgaver ud fra en risikobaseret tilgang.

§ 18. CSIRT'en sikrer, at fysiske og juridiske personer i anonymiseret form kan rapportere om sårbarheder.

Stk. 2. Ministeren for samfundssikkerhed og beredskab kan fastsætte nærmere regler om rapportering, håndtering og videregivelse efter stk. 1.

§ 19. CSIRT'en faciliterer, at der på frivillig basis kan ske udveksling af oplysninger mellem enheder i cybersikkerhedsfællesskaber, herunder fællesskaber på europæisk niveau.

Stk. 2. Væsentlige og vigtige enheder, der indgår i eller udtræder af cybersikkerhedsfællesskaber efter stk. 1, skal underrette den kompetente myndighed herom.

Stk. 3. Offentlige og private enheder kan uanset, at de ikke er omfattet af lovens anvendelsesområde deltage i den frivillige udveksling af oplysninger mellem enheder i cybersikkerhedsfællesskaber efter stk. 1.

Kapitel 6

Tilsyn og håndhævelse

§ 20. Ministeren for samfundssikkerhed og beredskab fastsætter efter forhandling med vedkommende minister regler om, hvilken myndighed der skal varetage funktionen som kompetent myndighed inden for en given sektor eller delsektor, eller for en bestemt type enhed, jf. lovens bilag 1 eller 2. Ministeren for samfundssikkerhed og beredskab kan efter forhandling med den minister, som udnytter bemyndigelsen i § 1, stk. 6, fastsætte regler om hvilken myndighed, der skal varetage funktionen som kompetent myndighed for disse enheder.

Stk. 2. For at sikre operationel uafhængighed ved tilsyn med den offentlige forvaltning, kan ministeren for samfundssikkerhed og beredskab efter forhandling med en anden minister fastsætte regler om, at tilsyn med Ministeriet for Samfundssikkerhed og Beredskab, herunder underliggende myndigheder, helt eller delvist overlades til den pågældende minister.

Stk. 3. Ministeren for samfundssikkerhed og beredskab kan fastsætte regler om koordinering, ansvar, fordeling af opgaver og udveksling af oplysninger mellem henholdsvis de kompetente myndigheder samt de kompetente myndigheder og CSIRT'en, herunder i forhold til hændelsesunderretninger efter kapitel 3 og tilsyn samt håndhævelse efter dette kapitel.

Tilsyns- og kontrolforanstaltninger for væsentlige enheder

§ 21. De kompetente myndigheder fører på deres respektive områder tilsyn med væsentlige enheders overholdelse af denne lov og regler udstedt i medfør af loven. En kompetent myndighed kan som led i sit tilsyn anvende følgende tilsynsforanstaltninger over for en væsentlig enhed:

1) Uden retskendelse og mod behørig legitimation foretage kontrol på stedet og eksternt tilsyn, herunder stikprøvekontroller.
2) Foretage regelmæssige og målrettede sikkerhedsaudits eller stille krav om, at enheden får et kvalificeret uafhængigt organ til at foretage disse audits, og at resultaterne heraf stilles til rådighed for den kompetente myndighed.
3) Foretage sikkerhedsaudits.
4) Foretage sikkerhedsscanninger.
5) Kræve at få udleveret oplysninger, der er nødvendige for at vurdere de foranstaltninger til styring af cybersikkerhedsrisici, som den berørte enhed 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 cybersikkerhedspolitikker.

Stk. 2. Ved anvendelsen af tiltagene i stk. 1, nr. 5-7, skal den kompetente myndighed angive formålet hermed og præcisere, hvilke oplysninger der kræves udleveret, og hvordan og i hvilken form oplysningerne og materialet nævnt i stk. 1, nr. 5-7, skal udleveres.

Håndhævelsesforanstaltninger for væsentlige enheder

§ 22. Den kompetente myndighed kan anvende følgende håndhævelsesforanstaltninger over for en væsentlig enhed:

1) Udstede advarsler om enhedens overtrædelse af denne lov.
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) Påbyde enheden at træffe foranstaltninger, der er nødvendige for at forhindre eller afhjælpe en hændelse.
4) Meddele enheden påbud og forbud for at sikre overholdelsen af de krav, der er fastsat i loven eller regler udstedt i medfør af loven.
5) Påbyde enheden at underrette de fysiske eller juridiske personer, til hvilke enheden 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.

6) Påbyde enheden 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 enhedens overholdelse af §§ 6, 12, 13, 15 og 16, stk. 2, samt regler udstedt i medfør heraf.
8) Påbyde enheden 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.

§ 23 Har én eller flere af håndhævelsesforanstaltninger, der er pålagt i medfør af § 22, nr. 1-4, vist sig at være utilstrækkelige, kan den kompetente myndighed fastsætte en frist, inden for hvilken den væsentlige enhed skal foretage de nødvendige tiltag for at afhjælpe manglerne eller opfylde den kompetente myndigheds krav. Er tiltagene ikke foretaget inden for den fastsatte frist, kan den kompetente myndighed træffe afgørelse om følgende, jf. dog stk. 4:

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

Stk. 2. Suspensioner eller forbud, som er pålagt i medfør af stk. 1, kan kun anvendes, indtil enheden 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 ikke indbringes for anden administrativ myndighed, men kan af den enhed eller den fysiske person, som afgørelsen vedrører, forlanges indbragt for domstolene.

Stk. 4. Bestemmelserne i stk. 1-3 finder ikke anvendelse på offentlige forvaltningsenheder.

Stk. 5. Vedkommende minister fastsætter efter forhandling med ministeren for samfundssikkerhed og beredskab regler om, hvilke certificeringer og godkendelser der er omfattet af stk. 1, nr. 1.

Tilsyns- og kontrolforanstaltninger for vigtige enheder

§ 24. De kompetente myndigheder fører reaktivt tilsyn med vigtige enheders overholdelse af denne lov og regler udstedt i medfør af loven. En kompetent myndighed kan som led i dette tilsyn efter indikationer på, at en vigtig enhed ikke overholder eller ikke har overholdt denne lov eller regler udstedt i medfør af loven anvende følgende tilsynsforanstaltninger:

1) Uden retskendelse og mod behørig legitimation foretage kontrol på stedet og eksternt efterfølgende tilsyn.
2) Foretage målrettede sikkerhedsaudits eller stille krav om, at enheden får et kvalificeret uafhængigt organ til at foretage disse audits, og at resultaterne heraf stilles til rådighed for den kompetente myndighed.
3) Foretage sikkerhedsscanninger.
4) Kræve at få udleveret oplysninger, der er nødvendige for efterfølgende at vurdere de foranstaltninger til styring af cybersikkerhedsrisici, som den berørte enhed 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 cybersikkerhedspolitikker.

Stk. 2. Ved anvendelse af tiltagene i stk. 1, nr. 4-6, skal den kompetente myndighed angive formålet med kravet og præcisere, hvilke oplysninger der kræves udleveret og hvordan og i hvilken form oplysningerne og materialet nævnt i stk. 1, nr. 4-6, skal udleveres.

Håndhævelsesforanstaltninger over vigtige enheder

§ 25. En kompetent myndighed kan anvende følgende håndhævelsesforanstaltninger over for en vigtig enhed:

1) Udstede advarsler om enhedens overtrædelse af denne lov.
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 enheden påbud og forbud for at sikre overholdelsen af de krav, der er fastsat i loven eller regler udstedt i medfør af loven.
4) Påbyde enheden at underrette de fysiske eller juridiske personer, til hvilke den 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 enheden at gennemføre de anbefalinger, der er fremsat i forbindelse med en gennemført sikkerhedsaudit.
6) Påbyde enheden 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 enheder

§ 26. Inden den kompetente myndighed træffer afgørelse om at anvende håndhævelsesforanstaltninger efter §§ 22, 23 eller 25, underrettes den berørte enhed om de påtænkte håndhævelsesforanstaltninger og begrundelsen herfor. Den kompetente myndighed skal give enheden en rimelig frist til at fremsætte bemærkninger, undtagen i tilfælde hvor formålet med foranstaltningen ellers ville forspildes.

Kapitel 7

Gensidig bistand

§ 27. Hvor en enhed leverer tjenester i mere end én medlemsstat i Den Europæiske Union, eller hvor enheden leverer tjenester i en eller flere medlemsstater, og enhedens net- og informationssystemer er beliggende i en eller flere andre medlemsstater, samarbejder de kompetente myndigheder med de andre medlemsstaters kompetente myndigheder i relevant omfang. Samarbejdet indebærer følgende:

1) De kompetente myndigheder underretter via det centrale kontaktpunkt de kompetente myndigheder i relevante medlemsstater om anvendte tilsyns- og håndhævelsesforanstaltninger.
2) De kompetente myndigheder kan anmode en anden medlemsstats kompetente myndigheder om at anvende tilsyns- og håndhævelsesforanstaltninger over for enheder i det pågældende land.
3) De kompetente myndigheder yder i rimeligt omfang bistand til en anden medlemsstats kompetente myndighed efter modtagelse af en begrundet anmodning herom.

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

Stk. 3. Modtages der en anmodning om gensidig bistand, jf. stk. 1, vedrørende DNS-tjenesteudbydere, topdomænenavneadministratorer, enheder, der leverer domænenavnsregistreringstjenester, og udbydere af henholdsvis cloudcomputingtjenester, datacentertjenester, indholdsleveringsnetværk, administrerede tjenester, administrerede sikkerhedstjenester, onlinemarkedspladser, onlinesøgemaskiner og platforme for sociale netværkstjenester, kan der træffes passende tilsyns- og håndhævelsesforanstaltninger over for enheden, hvis denne leverer tjenester eller har et net- og informationssystem i Danmark.

Kapitel 8

Videregivelse af oplysninger, digital kommunikation, gennemførelsesretsakter og operativ uafhængighed

§ 28. De kompetente myndigheder kan videregive oplysninger til andre medlemsstaters myndigheder og til institutioner i Den Europæiske Union for at varetage de opgaver, som følger af denne lov eller regler udstedt i medfør af denne lov.

§ 29. 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.

§ 30. Vedkommende minister kan efter forhandling med ministeren for samfundssikkerhed og beredskab fastsætte regler, som er nødvendige for at gennemføre retsakter udstedt af Europa-Kommissionen i medfør af NIS 2-direktivet.

§ 31. 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

§ 32. Med bøde straffes den, der

1) overtræder § 6, stk. 1 eller 2, §§ 9 eller 10, § 11, stk. 1-6, § 12, stk. 1, § 13, stk. 1 eller 2, eller § 15,
2) undlader at efterkomme en kompetent myndigheds afgørelse efter § 23, stk. 1, nr. 1 eller 2,
3) undlader at efterkomme påbud eller forbud efter § 22, stk. 1, nr. 3-6 eller § 25, stk. 1, nr. 3-6,
4) undlader at efterkomme en afgørelse efter § 16, stk. 2, § 21, stk. 1, nr. 2 eller nr. 5-7, eller § 24, stk. 1, nr. 2 eller nr. 4-6 eller
5) hindrer de kompetente myndigheder i at føre tilsyn efter bestemmelserne i § 21, stk. 1, nr. 1-4, eller § 24, 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 bestemmelser i forskrifterne.

Kapitel 10

Ikrafttrædelse, overgangsbestemmelser og ændringer i anden lovgivning

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

Stk. 2. Senest 3 år efter lovens ikrafttræden udarbejder ministeren for samfundssikkerhed og beredskab en rapport om erfaringerne med loven, som oversendes til Folketinget.

Stk. 3. Oplysningerne efter §§ 9, stk. 1 og § 10, stk. 1, skal indgives senest den 1. oktober 2025.

Stk. 4. Lov nr. 436 af 8. maj 2018 om net- og informationssikkerhed for domænenavnssystemer og visse digitale tjenester ophæves.

Stk. 5. Lov nr. 437 af 8. maj 2018 om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudviklingspunkter mv. ophæves.

Stk. 6. Lov nr. 440 af 8. maj 2018 om krav til sikkerhed for net- og informationssystemer inden for sundhedssektoren ophæves.

Stk. 7. Lov nr. 441 af 8. maj 2018 om sikkerhed i net- og informationssystemer i transportsektoren ophæves.

Kapitel 11

Territorialbestemmelse

§ 34. Loven gælder ikke for Færøerne og Grønland, men kan ved kongelig anordning helt eller delvist sættes i kraft for Færøerne og Grønland med de ændringer, som de hen-

holdsvis færøske og grønlandske forhold tilsiger. Lovens bestemmelser kan sættes i kraft på forskellige tidspunkter.

Bilag 1

Sektorer af særlig kritisk betydning

Sektor	*Delsektor*	*Type enhed*
1. Energi	a) Elektricitet	– Elektricitetsvirksomheder som defineret i artikel 2, nr. 57), i Europa-Parlamentets og Rådets direktiv (EU) 2019/944, der varetager »levering« som defineret i nævnte direktivs artikel 2, nr. 12)
		– Distributionssystemoperatører som defineret i artikel 2, nr. 29), i direktiv (EU) 2019/944
		– Transmissionssystemoperatører som defineret i artikel 2, nr. 35), i direktiv (EU) 2019/944
		– Producenter som defineret i artikel 2, nr. 38), i direktiv (EU) 2019/944
		– Udpegede elektricitetsmarkedsoperatører som defineret i artikel 2, nr. 8), i Europa-Parlamentets og Rådets forordning (EU) 2019/943 – Markedsdeltagere som defineret i artikel 2, nr. 25), i forordning (EU) 2019/943, der leverer tjenester, der vedrører aggregering, fleksibelt elforbrug eller energilagring som defineret i artikel 2, nr. 18), 20) og 59), i direktiv (EU) 2019/944 – Operatører af ladestationer, der er ansvarlige for forvaltningen og driften af en ladestation, som leverer en ladetjeneste til slutbrugere, herunder i en mobilitetstjenesteudbyders navn og på dennes vegne
	b) Fjernvarme og fjernkøling	– Operatører af fjernvarme eller fjernkøling som defineret i artikel 2, nr. 19), i Europa-Parlamentets og Rådets direktiv (EU) 2018/2001
	c) Olie	– Olierørledningsoperatører
		– Operatører af olieproduktionsanlæg, -raffinaderier og -behandlingsanlæg, olielagre og olietransmission
		– Centrale lagerenheder som defineret i artikel 2, litra f), i Rådets direktiv 2009/119/EF

	d) Gas	– Forsyningsvirksomheder som defineret i artikel 2, nr. 8), i Europa-Parlamentets og Rådets direktiv 2009/73/EF
		– Distributionssystemoperatører som defineret i artikel 2, nr. 6), i direktiv 2009/73/EF
		– Transmissionssystemoperatører som defineret i artikel 2, nr. 4), i direktiv 2009/73/EF
		– Lagersystemoperatører som defineret i artikel 2, nr. 10), i direktiv 2009/73/EF
		– LNG-systemoperatører som defineret i artikel 2, nr. 12), i direktiv 2009/73/EF
		– Naturgasvirksomheder som defineret i artikel 2, nr. 1), i direktiv 2009/73/EF
		– Operatører af naturgasraffinaderier og -behandlingsanlæg
	d) Brint	– Operatører inden for brintproduktion, -lagring og -transmission
2) Transport	a) Luft	– Luftfartsselskaber som defineret i artikel 3, nr. 4), i forordning (EF) nr. 300/2008, der anvendes til kommercielle formål
		– Lufthavnsdriftsorganer som defineret i artikel 2, nr. 2), i Europa-Parlamentets og Rådets direktiv 2009/12/EF, lufthavne som defineret i nævnte direktivs artikel 2, nr. 1), herunder de hovedlufthavne, der er anført i afsnit 2 i bilag II til Europa-Parlamentets og Rådets forordning (EU) nr. 1315/2013; og enheder med tilknyttede anlæg i lufthavne
		– Trafikledelses- og kontroloperatører, der udøver flyvekontroltjenester som defineret i artikel 2, nr. 1), i Europa-Parlamentets og Rådets forordning (EF) nr. 549/2004
	b) Jernbane	– Infrastrukturforvaltere som defineret i artikel 3, nr. 2), i Europa-Parlamentets og Rådets direktiv 2012/34/EU
		– Jernbanevirksomheder som defineret i artikel 3, nr. 1), i direktiv 2012/34/EU, herunder operatører af servicefaciliteter som defineret i nævnte direktivs artikel 3, nr. 12)
	c) Vand	– Rederier, som udfører passager- og godstransport ad indre vandveje, i høj-

		søfarvand eller kystnært farvand som defineret for søtransport i bilag I til Europa-Parlamentets og Rådets forordning (EF) nr. 725/2004, bortset fra de enkelte fartøjer, som drives af disse rederier
		– Driftsorganer i havne som defineret i artikel 3, nr. 1), i Europa-Parlamentets og Rådets direktiv 2005/65/EF, herunder deres havnefaciliteter som defineret i artikel 2, nr. 11), i forordning (EF) nr. 725/2004; og enheder, der opererer anlæg og udstyr i havne
		– Operatører af skibstrafiktjenester som defineret i artikel 3, litra o), i Europa-Parlamentets og Rådets direktiv 2002/59/EF
	d) Vejtransport	– Vejmyndigheder som defineret i artikel 2, nr. 12), i Kommissionens delegerede forordning (EU) 2015/962, der er ansvarlige for trafikledelse, med undtagelse af offentlige enheder, for hvilke trafikledelse eller drift af intelligente transportsystemer er en ikkevæsentlig del af deres generelle aktivitet
		– Operatører af intelligente transportsystemer som defineret i artikel 4, nr. 1), i Europa-Parlamentets og Rådets direktiv 2010/40/EU
3. Bankvirksomhed		– Kreditinstitutter som defineret i artikel 4, nr. 1), i Europa-Parlamentets og Rådets forordning (EU) nr. 575/2013
4. Finansielle markedsinfrastruktur		– Operatører af markedspladser som defineret i artikel 4, nr. 24), i Europa-Parlamentets og Rådets direktiv 2014/65/EU
		– Centrale modparter (CCP'er) som defineret i artikel 2, nr. 1), i Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012
5. Sundhed		– Sundhedstjenesteydere som defineret i artikel 3, litra g), i Europa-Parlamentets og Rådets direktiv 2011/24/EU
		– EU-referencelaboratorier, der er omhandlet i artikel 15, i Europa-Parlamentets og Rådets forordning (EU) 2022/2371
		– Enheder, der udfører forsknings- og udviklingsaktiviteter vedrørende lægemid-

		ler som defineret i artikel 1, nr. 2), i Europa-Parlamentets og Rådets direktiv 2001/83/EF – Enheder, der fremstiller farmaceutiske råvarer og farmaceutiske præparater som omhandlet i hovedafdeling C, hovedgruppe 21, i NACE rev. 2 – Enheder, som fremstiller medicinsk udstyr, som den anser for at være kritisk i en folkesundhedsmæssig krisesituation (»liste over kritisk medicinsk udstyr til folkesundhedsmæssige krisesituationer«) i den i artikel 22 i Europa-Parlamentets og Rådets forordning (EU) 2022/123 anvendte betydning
6. Drikkevand		– Leverandører og distributører af drikkevand som defineret i artikel 2, nr. 1), litra a), i Europa-Parlamentets og Rådets direktiv (EU) 2020/2184bortset fra distributører, for hvilke distribution af drikkevand er en ikkevæsentlig del af deres generelle aktivitet med distribution af andre råvarer og varer
7. Spildevand		– Virksomheder, der indsamler, bortskaffer eller behandler byspildevand, husspildevand eller industrispildevand som defineret i artikel 2, nr. 1), 2) og 3), i Rådets direktiv 91/271/EØF, bortset fra virksomheder, for hvilke indsamling, bortskaffelse eller behandling af byspildevand, husspildevand eller industrispildevand er en ikkevæsentlig del af deres generelle aktivitet
8. Digital infrastruktur		– Udbydere af internetudvekslingspunkter
		– DNS-tjenesteudbydere, bortset fra operatører af rodnavneservere
		– Topdomænenavneadministratorer
		– Udbydere af cloudcomputingtjenester
		– Udbydere af datacentertjenester
		– Udbydere af indholdsleveringsnetværk
		– Tillidstjenesteudbydere
		– Udbydere af offentlige elektroniske kommunikationsnet
		– Udbydere af offentligt tilgængelige elektroniske kommunikationstjenester

9. Forvaltning af IKT-tjenester (business-to-business)		– Udbydere af administrerede tjenester – Udbydere af administrerede sikkerheds-tjenester
10. Offentlig forvaltning		– Offentlige forvaltningsenheder under den centrale forvaltning som defineret af en medlemsstat i overensstemmelse med national ret
		– Offentlige forvaltningsenheder på regionalt plan som defineret af en medlemsstat i overensstemmelse med national ret
11. Rummet		– Operatører af jordbaseret infrastruktur, der ejes, forvaltes og drives af medlemsstater eller private parter, og som understøtter levering af rumbaserede tjenester, undtagen udbydere af offentlige elektroniske kommunikationsnet

Bilag 2

Andre kritiske sektore

Sektor	*Delsektor*	*Type enhed*
1. Post- og kurertjenester		– Postbefordrende virksomheder som defineret i artikel 2, nr. 1a), i direktiv 97/67/EF, herunder udbydere af kurertjenester
2. Affaldshåndtering		– Virksomheder, der varetager affaldshåndtering som defineret i artikel 3, nr. 9), i Europa-Parlamentets og Rådets direktiv 2008/98/EF, bortset fra virksomheder, for hvilke affaldshåndtering ikke er deres vigtigste økonomiske aktivitet
3. Fremstilling, produktion og distribution af kemikalier		– Virksomheder, der beskæftiger sig med fremstilling af stoffer og distribution af stoffer eller blandinger som omhandlet i artikel 3, nr. 9) og 14), i Europa-Parlamentets og Rådets forordning (EF) nr. 1907/2006 og virksomheder, der beskæftiger sig med produktion af artikler som defineret i artikel 3, nr. 3), i nævnte forordning ud af stoffer eller blandinger
4. Produktion, tilvirkning og distribution af fødevarer		– Fødevarevirksomheder som defineret i artikel 3, nr. 2), i Europa-Parlamentets og Rådets forordning (EF) nr. 178/2002, der beskæftiger sig med engrosdistribution og industriel produktion og tilvirkning
5. Fremstilling	a) Fremstilling af medicinsk udstyr og medicinsk udstyr til in vitro-diagnostik	– Enheder, der fremstiller medicinsk udstyr som defineret i artikel 2, nr. 1), i Europa-Parlamentets og Rådets forordning (EU) 2017/745, og enheder, der fremstiller medicinsk udstyr til in vitro-diagnostik som defineret i artikel 2, nr. 2), i Europa-Parlamentets og Rådets forordning (EU) 2017/746, med undtagelse af enheder, der fremstiller medicinsk udstyr omhandlet i dette direktivs bilag I, punkt 5, femte led
	b) Fremstilling af computere og elektroniske og optiske produkter	– Virksomheder, der udøver en af de økonomiske aktiviteter, der er omhandlet i hovedafdeling C, hovedgruppe 26, i NACE rev. 2

	c) Fremstilling af elektrisk udstyr	– Virksomheder, der udøver en af de økonomiske aktiviteter, der er omhandlet i hovedafdeling C, hovedgruppe 27, i NACE rev. 2
	d) Fremstilling af maskiner og udstyr i.a.n.	– Virksomheder, der udøver en af de økonomiske aktiviteter, der er omhandlet i hovedafdeling C, hovedgruppe 28, i NACE rev. 2
	e) Fremstilling af motorkøretøjer, påhængsvogne og sættevogne	– Virksomheder, der udøver en af de økonomiske aktiviteter, der er omhandlet i hovedafdeling C, hovedgruppe 29, i NACE rev. 2
	f) Fremstilling af andre transportmidler	– Virksomheder, der udøver en af de økonomiske aktiviteter, der er omhandlet i hovedafdeling C, hovedgruppe 30, i NACE rev. 2
6. Digitale udbydere		– Udbydere af onlinemarkedspladser
		– Udbydere af onlinesøgemaskiner
		– Udbydere af platforme for sociale netværkstjenester
7. Forskning		– Forskningsorganisationer

Bemærkninger til lovforslaget

Almindelige bemærkninger

Indholdsfortegnelse

1. Indledning

Net- og informationssystemer spiller i dag en afgørende rolle i samfundet, både for virksomheder, myndigheder og borgere, som alle i stigende grad er afhængige af velfungerende digitale systemer i hverdagen. Med den høje grad af digitalisering følger dog også en høj grad af sårbarhed, herunder f.eks. i forhold til nedbrud forårsaget af systemsvigt og menneskelige fejl, og i forhold til aktører, der udfører cyberspionage og cybersabotage. I dag er cybertruslen således en af de mest alvorlige trusler mod vores samfund, idet hackere, andre kriminelle og fjendtlige statsaktører sætter vores digitale sikkerhed under pres med stadigt mere avancerede angreb.

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 i 2024 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. I dag er truslen fra cyberspionage blandt de mest alvorlige trusler, som vores samfund står overfor.

Dette er en problemstilling, der gør sig gældende på tværs af EU, og det er baggrunden for, at der i EU-regi er taget initiativ til at styrke cybersikkerhedsniveauet i hele Unionen. Bl.a. på denne baggrund har Europa-Parlamentet og Rådet derfor 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 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). Der henvises til pkt. 2.1., hvor overgangen fra NIS 1- til NIS 2-direktivet beskrives nærmere.

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, herunder bl.a. sektorerne for energi, transport, bankvirksomhed, sundhed, drikke- og spildevand, digital infrastruktur og den offentlige forvaltning. Samtidig fastsættes en række oplysnings- og underretningspligter over for de kompetente myndigheder, 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 og indfører bl.a. mulighed for, at myndighederne midlertidigt kan suspendere topledere i enhederne.

Formålet med dette lovforslag er at gennemføre NIS 2-direktivet ved en fælles hovedlov på tværs af størstedelen af de sektorer, der er omfattet af direktivet. Hermed vil der blive skabt en fælles lovgivningsmæssig ramme til gavn for de enheder, der omfattes af lovgivningen, og de myndigheder der skal anvende lovgivningen. Den eksisterende nationale gennemførelse af NIS 1-direktivet vil samtidig blive ophævet.

Nærværende lovforslag finder ikke anvendelse for tele-, energi- og finanssektorerne. Det skal navnlig ses i lyset af, at der for disse sektorer allerede findes en omfattende sektorspecifik regulering af cybersikkerheden. For disse sektorer gælder således særlige hensyn, som begrunder, at implementeringen af NIS 2-direktivet for disse sektorer bør ske sektorvist med henblik på at, implementeringen kan ske gennem en integration med den eksisterende regulering inden for sektorerne.

NIS 2-direktivet implementeres for telesektoren gennem det samtidigt fremsatte forslag til lov om sikkerhed og beredskab i telesektoren. For energisektoren implementeres

NIS 2-direktivet gennem L 111, forslag til lov om styrket beredskab i energisektoren som fremsat den 4. december 2024. For finanssektoren er NIS 2-direktivet implementeret gennem lov om finansiel virksomhed.

2. Lovforslagets baggrund

2.1. Fra NIS 1- til NIS 2-direktivet

NIS 1-direktivet havde til formål at sikre et højt fælles sikkerhedsniveau for net- og informationssystemer inden for en række udvalgte sektorer i hele EU. NIS 2-direktivet ophæver og erstatter NIS 1-direktivet.

NIS 1-direktivet fastlagde bl.a. krav til rammerne for arbejdet med sikkerhed i net- og informationssystemer både nationalt og på EU-niveau, herunder krav til samarbejdsorganer og myndighedsstruktur. Derudover stillede NIS 1-direktivet krav om fastsættelse af sikkerhedskrav og underretningspligter for operatører af væsentlige tjenester og udbydere af digitale tjenester.

Med vedtagelsen af NIS 1-direktivet blev der således taget skridt hen mod at øge cybersikkerheden på tværs af EU. I forbindelse med evalueringen af NIS 1-direktivet konstaterede EU-Kommissionen, at der var store forskelle mellem medlemsstaternes gennemførelse af direktivet, herunder med hensyn til dets anvendelsesområde, hvis afgrænsning i vid udstrækning blev overladt til medlemsstaternes skøn. Evalueringen viste derudover, at NIS 1-direktivet gav medlemsstaterne meget vide skønsbeføjelser med hensyn til gennemførelsen af de sikkerheds- og hændelsesrapporteringsforpligtelser, der er fastsat heri. Disse forpligtelser blev ifølge evalueringen gennemført på vidt forskellige måder på nationalt plan. Det samme var tilfældet for medlemsstaternes gennemførelse af NIS 1-direktivets krav om tilsyn og håndhævelse. Sådanne forskellige kan i sidste ende føre til, at visse medlemsstater har en højere sårbarhed over for cybertrusler, hvilket potentielt kan have afsmittende virkninger i hele Unionen.

Formålet med NIS 2-direktivet er derfor at fjerne sådanne forskelle mellem medlemsstaterne, herunder navnlig ved at fastsætte minimumsregler for, hvordan en koordineret reguleringsramme fungerer.

NIS 2-direktivet udvider antallet af omfattede sektorer og typer af enheder (direktivets bilag I og II). Derudover fastsætter direktivet 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. Samlet set overlader NIS 2-direktivet et væsentligt mindre skøn til medlemsstaterne, end tilfældet var med NIS 1-direktivet.

Det følger af artikel 41, stk. 1, i NIS 2-direktivet, at direktivet skulle være gennemført i dansk ret senest den 17. oktober 2024 og træde i kraft senest den 18. oktober 2024. Med den foreslåede bestemmelse i § 33 vil loven dermed træde i kraft den 1. juli 2025, og således lidt over ni måneder efter direktivets implementeringsfrist. Den 28. november 2024 indledte EU-Kommissionen traktatbrudssager mod 23 medlemsstater, herunder Danmark for ikke at have gennemført NIS 2-direktivet.

2.2. Model for implementering af NIS 2-direktivet

2.2.1. Lovgivningsmodel

NIS 2-direktivet finder anvendelse for en lang række sektorer, og direktivet har således et meget bredt anvendelsesområde.

Ved implementeringen af NIS 2-direktivet anser Ministeriet for Samfundssikkerhed og Beredskab det på den ene side for væsentligt, at direktivets krav målrettes og tilpasses de enkelte sektorers særlige forhold. Samtidig er det væsentligt, at der i videst muligt omfang skabes ensartethed og koordination på tværs af de enkelte sektorer, således at enheder, der opererer i flere sektorer, ikke rammes af modsatrettede krav.

For at tage højde for disse hensyn vil implementeringen af NIS 2-direktivet tage udgangspunkt i sektoransvarsprincippet, således at de enkelte ressortministerier bevarer deres ansvar for cybersikkerhed og tilsyn inden for deres respektive sektorer, mens Styrelsen for Samfundssikkerhed tillægges en tværgående rolle og får til opgave at facilitere et tæt samarbejde mellem de ressortansvarlige myndigheder.

Med lovforslaget foreslås det, at de relevante ressortministre på visse områder bemyndiges til at fastsætte nærmere regler i bekendtgørelsesform. Muligheden for nærmere udmøntning af visse specifikke krav i bekendtgørelsesform har til formål at give de relevante ressortministre mulighed for at udmønte lovens krav i bekendtgørelser, såfremt særlige sektorspecifikke forhold påkræver dette. Muligheden for i særlige tilfælde at udstede sektorspecifikke bekendtgørelser vil bl.a. sikre, at der i nødvendigt omfang hurtigere kan gennemføres ændringer på baggrund af eksempelvis den teknologiske udvikling eller ændringer i trusselsbilledet inden for en givne sektor.

For i videst muligt omfang at sikre ensartethed og koordination på tværs af de enkelte sektorer, vil bl.a. de nærmere regler om krav til foranstaltninger til styring af cybersikkerhedsrisici skulle fastsættes af vedkommende minister efter forhandling med ministeren for samfundssikkerhed og beredskab.

Ved gennemførelsen tages der således hensyn til, at det er ressortministerierne og de sektoransvarlige myndigheder, der med deres indgående kendskab til forholdene i de enkelte sektorer har de bedste forudsætninger for at vurdere, om der konkret er behov for nærmere udmøntning af lovens krav, således at implementeringen af direktivet udmøntes på den måde, der er mest hensigtsmæssig for sektoren.

Med dette lovforslag har Ministeriet for Samfundssikkerhed og Beredskab lagt afgørende vægt på, at gennemførelsen af NIS 2-direktivet sker i overensstemmelse med regeringens principper for implementering af erhvervsrettet EU-regulering, hvorefter den nationale regulering som udgangspunkt ikke bør gå videre end minimumskravene i EU-reguleringen. Ved at anvende minimumsimplementering sikres det, at danske virksomheder ikke pålægges flere byrder end andre europæiske virksomheder. Samtidig lægger Ministeriet for Samfundssikkerhed og Beredskab vægt på i videst muligt omfang at foretage en direktivnær gennemførelse, således at direktivets formuleringer, betegnelser, definitioner mv. som udgangspunkt gengives ordret i dette lovforslag.

Den valgte lovgivningsmodel for gennemførelsen af NIS 2-direktivet, hvor der med lovforslaget skabes en fælles lovgivningsramme på tværs af de omfattede sektorer, indebærer, at den nuværende regulering, der gennemfører NIS 1-direktivet for de omfattede sektorer, der omfattes af denne lov, ophæves.

2.2.2. Nationale myndigheder og samarbejde

NIS 2-direktivet 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. NIS 1-direktivet indeholdt tilsvarende forpligtelser.

Der lægges med lovforslaget op til, at de kompetente myndigheder inden for de enkelte sektorer omfattet af denne lov udpeges af ministeren for samfundssikkerhed og beredskab efter forhandling med de ressortansvarlige ministre. Det vil være de kompetente myndigheders ansvar at føre tilsyn med deres respektive sektorer. Der er allerede på baggrund af NIS 1-direktivet udpeget kompetente myndigheder for så vidt angår de sektorer, som var omfattet af direktivet. Med NIS 2-direktivet omfattes imidlertid en række yderligere sektorer, og der skal derfor også udpeges kompetente myndigheder for disse sektorer. Der henvises i øvrigt til bemærkningerne til den foreslåede § 20, stk. 1.

Det forudsættes, at der vil være en tæt koordination mellem de kompetente myndigheder i forbindelse med tilrettelæggelsen af tilsynsarbejdet, således at der i videst muligt omfang anlægges en fælles tilgang. Dette vil særligt være relevant for tilsynet med enheder, der måtte indgå i flere forskellige sektorer, og hvor der potentielt er flere kompetente myndigheder, som skal føre tilsyn med samme enhed.

Det er på den baggrund Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at det i visse tilfælde vil være relevant og hensigtsmæssigt at gennemføre fælles tilsynsbesøg. Det er endvidere Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at der i sådanne tilfælde bør være mulighed for at samarbejde om tilsynsressourcer, eksempelvis i form af et fælles sekretariat, således at de nødvendige kompetencer kan bringes i spil på tværs af ministerområder. Det er samtidig Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at der bør være mulighed for at fastsætte nærmere regler om koordinering, ansvar og udveksling af oplysninger mellem henholdsvis de kompetente myndigheder og CSIRT'en, herunder i forhold til hændelsesunderretninger efter kapitel 3 og tilsyn samt håndhævelse efter kapitel 6. Sådanne regler bør fastsættes med henblik på at skabe en mere tydelig ansvarsdeling mellem henholdsvis kompetente myndigheder og CSIRT'en, herunder vedrørende deres samarbejde.

Det centrale kontaktpunkt skal udøve en forbindelsesfunktion for at sikre grænseoverskridende samarbejde mellem de nationale kompetente myndigheder og andre medlemsstaters kompetente myndigheder og – hvor det er relevant – Europa-Kommissionen og Den Europæiske Unions Agentur for Cybersikkerhed (ENISA). Dertil skal det centrale kontaktpunkt sikre tværsektorielt samarbejde mellem de nationale kompetente myndigheder, hvorfor det centrale kontaktpunkt bl.a. vil facilitere koordinationen vedrørende tilsynsarbejde mellem de kompetente myndigheder. De kompetente myndigheder vil via det centrale kontaktpunkt således bl.a. oversende oplysninger til Europa-Kommissionen om omfattede væsentlige og vigtige enheder i overensstemmelse med NIS 2-direktivets artikel 3, stk. 5.

Opgaven som centralt kontaktpunkt efter NIS 1-direktivet varetages i dag af Styrelsen for Samfundssikkerhed (tidligere Center for Cybersikkerhed), og den opgave vil styrelsen fortsat skulle varetage. Det gælder også i forhold til de sektorer, hvor NIS 2-direktivet gennemføres ved sektorspecifik regulering, jf. afsnit 1 ovenfor.

Center for Cybersikkerhed blev ved implementeringen af NIS 1-direktivet endvidere udpeget som CSIRT i Danmark. Opgaven har hidtil været varetaget af netsikkerhedstjenesten under Center for Cybersikkerhed, og den opgave vil netsikkerhedstjenesten for nuværende fortsat skulle varetage.

Med den kongelige resolution af 29. august 2024 er Center for Cybersikkerhed, bortset fra netsikkerhedstjenesten, blevet ressortoverdraget til Ministeriet for Samfundssikkerhed og Beredskab fra Forsvarsministeriet. 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 indbe-¬rettes til både den kompetente myndighed og CSIRT'en. Det forudsættes på¬den baggrund, at der vil være et tæt samarbejde mellem den kompetente myndighed og CSIRT'en. Der lægges med lovforslaget op til, at ministeren for samfundssikkerhed og beredskab kan fastsætte nærmere regler om samarbejdet mellem de kompetente myndigheder og CSIRT'en.

CSIRT'en vil skulle leve op til kravene i NIS 2-direktivets artikel 10 og 11. Der henvises i øvrigt til den foreslåede § 17.

I medlemsstater, hvor opgaverne som kompetent myndighed, centralt kontaktpunkt og CSIRT varetages af forskellige myndigheder, er det forudsat i NIS 2-direktivet, at disse myndigheder skal samarbejde på tværs.

NIS 2-direktivet foreskriver endvidere, at medlemsstaterne skal udpege eller oprette en eller flere såkaldte cyberkrisestyringsmyndigheder med ansvar for styring af omfattende cybersikkerhedshændelser og -kriser.

Det bemærkes i den forbindelse, at opgaven som cyberkrisestyringsmyndighed forventes at blive varetaget af CSIRT'en. Cyberkrisestyringsmyndigheden får til opgave at styre omfattende cybersikkerhedshændelser inden for de eksisterende rammer for national krisestyring. I situationer, hvor Den Nationale Operative Stab (NOST) aktiveres, koordineres indsatsen inden for rammerne af NOST.

Der vil i overensstemmelse med NIS 2-direktivets artikel 9, stk. 4, blive udarbejdet en national beredskabsplan for omfattende cybersikkerhedshændelser og -kriser. Direktivets artikel 9, stk. 4, stiller nærmere krav til indholdet af den nationale beredskabsplan, herunder bl.a. at planen skal fastlægge mål, foranstaltninger og procedurer samt cyberkrisestyringsmyndighedernes opgaver og ansvarsområder.

Europa-Kommissionen skal underrettes om, hvilken myndighed der fungerer som cyberkrisestyringsmyndighed, inden for tre måneder efter, at myndigheden udpeges eller oprettes samt ved senere ændringer. Senest tre måneder efter vedtagelsen af den nationale beredskabsplan skal oplysninger om planen forelægges for Europa-Kommissionen og EU-CyCLONe, som er det europæiske netværk af forbindelsesorganisationer for cyberkriser.

Der vil desuden i overensstemmelse med NIS 2-direktivets artikel 7 blive udarbejdet en national cybersikkerhedsstrategi, der fastlægger strategiske mål, de nødvendige ressourcer til at nå disse mål og passende politiske og lovgivningsmæssige foranstaltninger med henblik på at opnå og opretholde et højt cybersikkerhedsniveau. Direktivets artikel 7, stk. 1, stiller nærmere krav til indholdet heraf, herunder bl.a. mål, prioriteter, foranstaltninger og styringsrammer, ligesom direktivets artikel 7, stk. 2, foreskriver, at der som led i strategien skal vedtages en række nærmere bestemte politikker.

Europa-Kommissionen skal underrettes om den nationale cybersikkerhedsstrategi senest tre måneder efter vedtagelsen heraf, og strategien skal regelmæssigt og mindst hvert femte år vurderes og om nødvendigt ajourføres.

Danmark har siden 2014 haft en national strategi for cyber- og informationssikkerhed. Den nationale strategi er blevet opdateret flere gange, og den nuværende strategi gælder for 2022-2024.

2.2.3. Samarbejdsfora i EU

Med NIS 2-direktivet etableres der i EU-regi tre samarbejdsfora, hvor medlemsstaterne er repræsenteret.

Det første forum er Samarbejdsgruppen, der hovedsageligt består af repræsentanter fra medlemsstaterne, Europa-Kommissionen og ENISA. Samarbejdsgruppen fokuserer på strategisk samarbejde om et højt cybersikkerhedsniveau i EU og udveksling af oplysninger mellem medlemsstaterne.

Det andet forum er CSIRT-netværket, som består af repræsentanter for medlemsstaternes CSIRT'er, der er de nationale enheder, som håndterer it-sikkerhedshændelser, og it-beredskabsenheden for Unionens institutioner og agenturer (CERT-EU). CSIRT-netværket fokuserer på det operationelle samarbejde mellem medlemsstaternes CSIRT'er.

Det tredje forum er det europæiske netværk af forbindelsesorganisationer for cyberkriser (EU-CyCLONe). EU-CyCLONe består af repræsentanter for medlemsstaternes cyberkrisestyringsmyndigheder samt under visse omstændigheder Europa-Kommissionen. EU-CyCLONe har til formål at støtte håndteringen af omfattende cybersikkerhedshændelser og kriser på operationelt plan og at sikre regelmæssig udveksling af relevant information mellem medlemsstaterne og EU-institutioner.

2.3. 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).

CER-direktivet har til formål at øge kritiske enheders modstandsdygtighed, med henblik på at gøre dem i bedre stand til at håndtere risici for deres drift, som kan føre til forstyrrelse i leveringen af væsentlige tjenester.

Enheder, der leverer væsentlige tjenester, herunder samfundsvigtige ydelser som eksempelvis produktion af elektricitet og levering af drikkevand, og som i øvrigt opfylder kriterierne for at blive betragtet som kritiske enheder, skal således bl.a. i medfør af CER-direktivet styrke deres evne til at forebygge, reagere på, modstå, afbøde og komme på fode igen efter hændelser, der har potentiale til at forstyrre leveringen af væsentlige tjenester. CER-direktivet stiller bl.a. krav om gennemførelse af modstandsdygtighedsforanstaltninger, underretning til myndighederne om hændelser samt tilsyns- og håndhævelsesbeføjelser.

Det følger af CER-direktivets artikel 1, stk. 2, at CER-direktivet ikke finder anvendelse på spørgsmål, der er omfattet af NIS 2-direktivet. Med andre ord er cybersikkerhed reguleret særskilt i NIS 2-direktivet og undtages derfor fra CER-direktivet. Henset til cybersikkerhedens betydning for kritiske enheders modstandsdygtighed er det dog i CER-direktivet forudsat, at der sker en koordineret gennemførelse af CER- og NIS 2-direktiverne.

Sammenhængen mellem NIS 2-direktivet og CER-direktivet understreges desuden af, at enheder, der er identificeret som kritiske enheder i henhold til CER-direktivet, allerede af den grund er omfattet af anvendelsesområdet for NIS 2-direkti-

vet som en væsentlig enhed, jf. NIS 2-direktivets artikel 3, stk. 1, litra f, jf. artikel 2, stk. 3.

Ministeriet for Samfundssikkerhed og Beredskab fremsætter samtidig med dette lovforslag forslag til lov om kritiske enheders modstandsdygtighed, som har til formål at gennemføre CER-direktivet. Det er Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at der i mange sektorer vil være sammenfald mellem de udpegede kompetente myndigheder efter henholdsvis NIS 2-direktivet og CER-direktivet. Det forudsættes derfor, at myndigheder med opgaver i medfør af de to direktiver også i praksis vil koordinere på tværs i relevant omfang.

2.4. Nuværende implementering af NIS 1-direktivet

I Danmark er NIS 1-direktivet gennemført gennem sektorvis regulering.

I oliesektoren er NIS 1-direktivet gennemført ved bekendtgørelse nr. 424 af 25. april 2018 om beredskab for oliesektoren. Bekendtgørelsen er udstedt med hjemmel i § 3, § 13, stk. 3, § 16, stk. 3, § 17, stk. 5, § 21, stk. 5, og § 23, stk. 2, i lov nr. 354 af 24. april 2012 om olieberedskab.

I sektorerne for elektricitet og naturgas er NIS 1-direktivet gennemført ved bekendtgørelse nr. 2647 af 28. december 2021 om it-beredskab for el- og naturgassektorerne med senere ændringer. Bekendtgørelsen er udstedt med hjemmel i § 69, stk. 5, § 85 c, stk. 5 og 6, og §§ 90 og 92 i lov om elforsyning, jf. lovbekendtgørelse nr. 984 af 12. maj 2021 med senere ændringer, og § 15 b, stk. 5 og 6, og §§ 52 og 54 i lov om gasforsyning, jf. lovbekendtgørelse nr. 1100 af 16. august 2023.

I transportsektoren er NIS 1-direktivet gennemført ved lov nr. 441 af 8. maj 2018 om sikkerhed i net- og informationssystemer i transportsektoren. Direktivet er desuden gennemført ved bekendtgørelse nr. 1042 af 6. august 2018 om sikkerhed i net- og informationssystemer i transportsektoren. For de elementer af NIS 1-direktivet, der vedrører rederier, som udfører passager- og godstransport, og skibstrafiktjenesteoperatører, skete gennemførelsen dog ved bekendtgørelse nr. 46 af 15. januar 2019 om sikkerhed i net- og informationssystemer af betydning for skibes sikkerhed og deres sejlads. Bekendtgørelsen er udstedt med hjemmel i § 3, stk. 1, nr. 2, 5 og 7, § 6, stk. 3, og § 32, stk. 9, i lov nr. 1629 af 17. december 2018 om sikkerhed til søs med senere ændringer.

I sektoren for bankvæsen er NIS 1-direktivet gennemført ved bekendtgørelse nr. 1103 af 30. juni 2022 om ledelse og styring af pengeinstitutter m.fl. Bekendtgørelsen er udstedt med hjemmel i § 65, stk. 2, § 70, stk. 6, § 71, stk. 2, § 152, stk. 2, og § 373, stk. 4, i lov om finansiel virksomhed, jf. lovbekendtgørelse nr. 406 af 29. marts 2022, § 67, stk. 5, § 68, stk. 2, § 94, stk. 2, og § 270, stk. 1, i lov nr. 1155 af 8. juni 2021 om fondsmæglerselskaber og investeringsservice og -aktiviteter med senere ændringer, § 21, stk. 5, og § 39, stk. 3, i lov om realkreditlån og realkreditobligationer mv., jf. lovbekendtgørelse nr. 315 af 11. marts 2022, og § 180 g, stk. 3, og § 255 i lov om kapitalmarkeder, jf. lovbekendtgørelse nr. 2014 af 1. november 2021 med senere ændringer.

I sektoren for finansielle markedsinfrastrukturer er NIS 1-direktivet gennemført ved bekendtgørelse nr. 457 af 9. maj 2018 om hændelsesrapportering for operatører af væsentlige tjenester. Bekendtgørelsen er udstedt med hjemmel i § 58 a, stk. 3, i lov om kapitalmarkeder, jf. lovbekendtgørelse nr. 41 af 13. januar 2023.

I sundhedssektoren er NIS 1-direktivet gennemført ved lov nr. 440 af 8. maj 2018 om krav til sikkerhed for net- og informationssystemer inden for sundhedssektoren. Direktivet er desuden gennemført ved bekendtgørelse nr. 458 af 9. maj 2018 om operatører af væsentlige tjenester. Bekendtgørelsen er udstedt med hjemmel i § 3, stk. 3, § 4, stk. 3, § 5, stk. 5, og § 6, stk. 1 og 3, i lov nr. 440 af 8. maj 2018 om krav til sikkerhed for net- og informationssystemer inden for sundhedssektoren. Med bekendtgørelse nr. 459 af 9. maj 2018 om delegation af opgaver fra sundhedsministeren til Sundhedsdatastyrelsen blev opgaverne i medfør af lov om krav til sikkerhed for net- og informationssystemer inden for sundhedssektoren delegeret fra sundhedsministeren til Sundhedsdatastyrelsen. Denne bekendtgørelse blev udstedt med hjemmel i § 9 i lov nr. 440 af 8. maj 2018 om krav til sikkerhed for net- og informationssystemer inden for sundhedssektoren.

I sektoren for drikkevandsforsyning og -distribution er NIS 1-direktivet gennemført ved bekendtgørelse nr. 429 af 4. maj 2018 om krav til sikkerheden i visse vandforsyningers net- og informationssystemer. Bekendtgørelsen er udstedt med hjemmel i § 56 a, § 57, stk. 2, § 63, stk. 3, og § 84, stk. 2 og 3, i lov om vandforsyning, jf. lovbekendtgørelse nr. 118 af 22. januar 2022 med senere ændringer.

I sektoren for digital infrastruktur er NIS 1-direktivet gennemført ved lov nr. 437 af 8. maj 2018 om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudviklingspunkter m.v. samt ved bekendtgørelse nr. 454 af 8. maj 2018 om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter. NIS 1-direktivet er endvidere gennemført i sektoren ved bekendtgørelse nr. 453 af 8. maj 2018 om sikkerhed i net- og informationssystemer for operatører af væsentlige tjenester på domænenavnsområdet og bekendtgørelse nr. 452 af 8. maj 2018 om net- og informationssikkerhed for visse digitale tjenester, der begge er udstedt med hjemmel i lov nr. 436 af 8. maj 2018 om net- og informationssikkerhed for domænenavnssystemer og visse digitale tjenester.

Med lovforslaget ophæves relevante dele af den sektorvise regulering, der gennemførte NIS 1-direktivet.

3. Lovforslagets hovedpunkter

3.1. Væsentlige og vigtige enheder

3.1.1. Gældende ret

NIS 1-direktivet fastsatte forpligtelser for operatører af væsentlige tjenester og udbydere af digitale tjenester inden for direktivets anvendelsesområde.

Det påhvilede efter NIS 1-direktivet medlemsstaterne at identificere de operatører af væsentlige tjenester, der er etableret på deres område for hver sektor og delsektor, som er omhandlet i direktivets bilag II. Udbydere af digitale tjenester skal derimod ikke identificeres, idet direktivet finder anvendelse for alle udbydere af digitale tjenester inden for dets anvendelsesområde.

Af NIS 1-direktivets bilag II fremgår sektorerne: 1) Energi med delsektorerne: a) Elektricitet, b) olie og c) gas, 2) transport med delsektorerne: a) Lufttransport, b) jernbanetransport, c) søfart og d) vejtransport, 3) bankvæsen, 4) finansielle markedsinfrastrukturer, 5) sundhedssektoren med delsektoren sundhedstjenestemiljøer (herunder hospitaler og private klinikker), 6) drikkevandsforsyning og distribution og 7) digital infrastruktur.

Kriterierne for identificering af operatører af væsentlige tjenester er, at: a) En enhed leverer en tjeneste, der er væsentlig for opretholdelsen af kritiske samfundsmæssige og/eller økonomiske aktiviteter, b) leveringen af denne tjeneste afhænger af net- og informationssystemer og c) en hændelse ville få væsentlige forstyrrende virkninger for leveringen af den nævnte tjeneste.

NIS 1-direktivet blev i dansk ret gennemført sektorvist i regulering gældende for de specifikke sektorer, hvor direktivet finder anvendelse, jf. afsnit 2.4 ovenfor.

3.1.2. NIS 2-direkivet

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.

Direktivet finder anvendelse på bestemte typer af offentlige og private enheder, der leverer tjenester eller udfører aktiviteter inden for Den Europæiske Union inden for de af direktivet oplistede sektorer af særlig kritisk betydning eller andre kritiske sektorer (henholdsvis direktivets bilag I og II).

Af direktivets bilag I fremgår sektorer af særligt kritisk betydning: 1) energi med delsektorerne: a) elektricitet, b) fjernvarme og fjernkøling, c) olie, d) gas og e) brint, 2) transport med delsektorerne: a) Luft, b) jernbane, c) vand og d) vejtransport, 3) bankvirksomhed, 4) finansielle markedsinfrastrukturer, 5) sundhed, 6) drikkevand, 7) spildevand, 8) digital infrastruktur, 9) forvaltning af IKT-tjenester (informations- og kommunikationstjenester) (business to business), 10) offentlig forvaltning og 11) rummet. Der henvises til lovens bilag 1.

Af direktivets bilag II fremgår andre sektorer: 1) post- og kurertjenester, 2) affaldshåndtering, 3) fremstilling, produktion og distribution af kemikalier, 4) produktion, tilvirkning og distribution af fødevarer, 5) fremstilling med delsektorerne: a) Fremstilling af medicinsk udstyr og medicinsk udstyr til in vitro-diagnostik, b) fremstilling af computere og elektroniske og optiske produkter, c) fremstilling af elektrisk udstyr, d) fremstilling af maskiner og udstyr intet andetsteds nævnt, e) fremstilling af motorkøretøjer, påhængsvogne og sættevogne og f) fremstilling af andre transportmidler, 6) digitale udbydere og 7) forskning. Der henvises til lovens bilag 2.

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

Direktivets artikel 3 fastsætter en række kriterier for, hvordan enhederne inddeles i henholdsvis væsentlige og vigtige enheder.

Som væsentlige enheder anses ifølge direktivets artikel 3, stk. 1, således: a) enheder inden for sektorer af særligt kritisk betydning, jf. direktivets bilag I, som overskrider tærsklerne for mellemstore virksomheder, b) kvalificerede tillidstjenesteudbydere og topdomænenavneadministratorer samt DNS-tjenesteudbydere, uanset deres størrelse, c) udbydere af offentlige elektroniske kommunikationsnet eller af offentligt tilgængelige elektroniske kommunikationstjenester, der udgør mellemstore virksomheder, d) offentlige forvaltningsenheder under den centrale forvaltning, e) alle andre enheder af en type omhandlet i direktivets bilag I eller II, som en medlemsstat har identificeret som væsentlige enheder i medfør af direktivets mere kvalitative kriterier i relation til deres samfundsmæssige betydning, f) enheder, der er identificeret som kritiske enheder i medfør af gennemførelsen af CER-direktivet, og g) hvis medlemsstaten træffer afgørelse herom, enheder, som den pågældende medlemsstat inden den 16. januar 2023 har identificeret som operatører af væsentlige tjenester i overensstemmelse med NIS 1-direktivet eller national ret.

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.

Indenfor 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.

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.

En virksomhed vil således overskride tærsklerne for en mellemstor virksomhed, når enheden beskæftiger mere end 250 personer og enheden har en årlig omsætning på over 50 mio. EUR eller en årlig samlet balance på over 43 mio. EUR.

Det følger af NIS 2-direktivets artikel 3, stk. 2, 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

Med NIS 2-direktivets artikel 44 ophæves NIS 1-direktivet.

Som nærmere beskrevet ovenfor under afsnit 3.1.2., fastsætter NIS 2-direktivet detaljerede regler for, hvilke virksomheder, myndigheder og organisationer (enheder), der omfattes af direktivets anvendelsesområde. Dette er modsat NIS 1-direktivet, hvor medlemsstaterne havde ansvaret for at identificere omfattede enheder.

I NIS 2-direktivet defineres en enhed som en fysisk eller juridisk person, der er oprettet og anerkendt som sådan i henhold til den nationale ret på det sted, hvor den er etableret, og som i eget navn kan udøve rettigheder og være underlagt forpligtelser. Det er på denne baggrund Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at en enhed – udover at kunne være en fysisk person – må anses for at være virksomheder, foreninger, organisationer og offentlige myndigheder mv. (juridiske personer), der er tildelt et CVR-nummer. Et selskab med et underliggende datterselskab vil således være at anse for to separate enheder, forudsat at de har fået tildelt hver deres CVR-nummer.

Det følger af EU-Kommissionens meddelelse C(2023) 6068 af 13. september 2023 om retningslinjer for anvendelsen af artikel 4, stk. 1, og 2, i NIS 2-direktivet, at NIS 2-direktivets forpligtelse i artikel 21, stk. 1, der kræver, at væsentlige og vigtige enheder træffer passende og forholdsmæssige foranstaltninger til styring af cybersikkerhedsrisici, vedrører alle den pågældende enheds operationer og tjenester, ikke kun specifikke it-aktiver eller kritiske tjenester, som enheden leverer.

Det er på denne baggrund Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at formuleringen »i net- og informationssystemer, som disse enheder anvender til deres operationer eller til at levere deres tjenester« i NIS 2-direktivets artikel 21, stk. 1, skal forstås som alle de net- og informationssystemer, som disse enheder anvender til deres operationer, eller til at levere deres tjenester, og ikke kun specifikke informationsteknologiske (it) aktiver eller kritiske tjenester, som enheden leverer.

I tilfælde hvor en enhed anvender flere forskellige typer af net- og informationssystemer, og hvor kun nogle af disse systemer er omfattet af lovens bilag, vil samtlige af de net- og informationssystemer, som enheden anvender til sine operationer, eller til at levere sine tjenester, således blive underlagt direktivets krav.

Som nærmere beskrevet under pkt. 3.1.2., finder direktivet anvendelse på bestemte typer af offentlige og private enheder, der leverer tjenester eller udfører aktiviteter inden for Den Europæiske Union inden for de af direktivet oplistede sektorer af særlig kritisk betydning eller andre kritiske sektorer, jf. direktivets bilag I og II. Der henvises til pkt. 3.1.2. for en nærmere beskrivelse af direktivets anvendelsesområde.

Det er Ministeriet for Samfundssikkerhed og Beredskabs vurdering, at loven som udgangspunkt kun bør omfatte enheder af en vis størrelse, således at enheder af en størrelse svarende til mikrovirksomheder og små virksomheder som udgangspunkt ikke omfattes af direktivets anvendelsesområde. For så vidt angår størrelseskravene henvises NIS 2-direktivet til EU-Kommissionens henstilling 2003/361/EF af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder. Der henvises til lovforslagets pkt. 3.1.2., hvor henstillingens størrelseskrav beskrives nærmere.

Dog vil visse typer af enheder blive omfattet uanset deres størrelse. Det gælder eksempelvis tillidstjenesteudbydere, topdomænenavneadministratorer, udbydere af domænenavnssystemer, offentlige forvaltningsenheder under den centrale forvaltning (statslige myndigheder) samt regionale forvaltningsenheder, i det omfang de leverer kritiske tjenester. Det gælder også enheder, der ud fra mere kvalitative kriterier i relation til deres samfundsmæssige betydning omfattes af direktivet, herunder bl.a. hvis enheden er den eneste udbyder af en væsentlig tjeneste, eller hvis forstyrrelser af tjenesten kan have alvorlige samfundsmæssige følgevirkninger.

Herudover omfattes uanset deres størrelse – og uanset om de måtte være omfattet af de i direktivet oplistede sektorer – enheder, der er identificeret som kritiske i medfør af gennemførelsen af CER-direktivet, og enheder, der leverer domænenavnsregistreringstjenester.

Det er ifølge direktivet op til medlemsstaterne, om direktivet også skal finde anvendelse på offentlige forvaltningsenheder på lokalt plan samt uddannelsesinstitutioner, navnlig hvis uddannelsesinstitutionerne udfører kritiske forskningsaktiviteter.

Det er dog Ministeriet for Samfundssikkerhed og Bered-

skabs opfattelse, at offentlige forvaltningsenheder på lokalt plan eller uddannelsesinstitutioner, der leverer tjenester inden for sektorerne i lovens bilag 1 eller 2, vil blive underlagt lovens krav. I lyset af ovenstående definition af 'net- og informationssystemer' bemærkes det, at offentlige forvaltningsenheder på lokalt plan, herunder kommuner, og uddannelsesinstitutioner ikke alene vil skulle træffe passende og forholdsmæssige foranstaltninger for at styre risiciene for sikkerheden i net- og informationssystemer vedrørende de aktiviteter, der er oplistet i lovens bilag, men for samtlige af de net- og informationssystemer, som de anvender til deres operationer, eller til at levere deres tjenester.

Direktivet finder ikke anvendelse på offentlige forvaltningsenheder, der udfører deres aktiviteter inden for national og offentlig sikkerhed, forsvar eller retshåndhævelse, jf. artikel 2, stk. 7. Derudover kan specifikke enheder, som udfører aktiviteter eller leverer tjenester inden for disse retsområder, undtages fra hele eller dele af direktivets materielle forpligtelser, for så vidt angår disse aktiviteter eller tjenester, jf. artikel 2, stk. 8.

Der vil også være enheder, som udøver aktiviteter i flere af de sektorer, der er omhandlet i lovens bilag. Dermed vil der efter omstændighederne kunne opstå en situation, hvor enheden isoleret set ville være at betragte som en vigtig enhed ud fra en vurdering af enhedens aktiviteter i én sektor, mens samme enhed vil være at betragte som væsentlig ud fra en vurdering af enhedens aktiviteter i en anden sektor.

Det er Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at en enhed, som har aktiviteter i flere sektorer, i sin helhed vil skulle anses for en væsentlig enhed, såfremt enheden i én af sektorerne lever op til kriterierne for at være en væsentlig enhed. Det skal dog understreges, at de kompetente myndigheder vil føre deres tilsyn ud fra en risikobaseret tilgang, således at frekvensen for tilsynene og tilsynets omfang tilpasses enhedens aktiviteter.

Der henvises i den forbindelse bl.a. til NIS 2-direktivets præambelbetragtning nr. 82, hvoraf det følger, at foranstaltninger til styring af cybersikkerhedsrisici bør stå i et passende forhold til graden af de væsentlige eller vigtige enheders risikoeksponering og til den samfundsmæssige og økonomiske indvirkning, som en hændelse ville have. Det følger endvidere af præambelbetragtningen, at 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.

3.1.4. Den foreslåede ordning

Det foreslås, at loven finder anvendelse på den samme kreds af væsentlige og vigtige enheder, som omfattes af NIS 2-direktivet. Loven vil dog, med undtagelse af enkelte tværgående bestemmelser, ikke finde anvendelse på enheder, i det omfang de omfattes af den samtidigt fremsatte lov om sikkerhed og beredskab i telesektoren, L 111, forslag til lov om styrket beredskab i energisektoren som fremsat den 4. december 2024 eller lov om finansiel virksomhed. Enheder vil dog fortsat kunne være omfattet af denne lov, hvis de udover aktiviteterne i f.eks. energisektoren også udfører aktiviteter inden for en af de øvrige sektorer, som er nævnt i lovens bilag 1 eller 2.

Det foreslås endvidere, at vedkommende minister efter forhandling med ministeren for samfundssikkerhed og beredskab bemyndiges til ved bekendtgørelse at bestemme, at loven helt eller delvist også finder anvendelse på henholdsvis offentlige forvaltningsenheder på lokalt plan og uddannelsesinstitutioner.

Særligt i relation til de enheder, der uanset deres størrelse omfattes af direktivet på baggrund af mere kvalitative kriterier i relation til deres samfundsmæssige betydning, jf. artikel 2, stk. 2, litra b-e, herunder 1) om enheden er den eneste udbyder af en tjeneste, der er væsentlig for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter, en forstyrrelse af den tjeneste, 2) enheden leverer vil kunne have en væsentlig indvirkning på den offentlige sikkerhed eller folkesundhed, 3) en forstyrrelse af den tjeneste, enheden leverer, vil kunne medføre en væsentlig systemisk risiko, navnlig for sektorer, hvor en sådan forstyrrelse kan have en 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, bemærkes, at direktivet lægger op til, at medlemsstaterne identificerer disse enheder som enten væsentlige og vigtige enheder.

Det er Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at disse enheder som udgangspunkt skal anses for at være væsentlige enheder. Det foreslås, at den relevante kompetente myndighed ud fra en konkret vurdering kan træffe afgørelse om, at en enhed, der ifølge de nævnte kriterier, som udgangspunkt anses for at være væsentlig i stedet skal anses for at være vigtig. Det kan eksempelvis være relevant i en situation, hvor en enhed anses som væsentlig på baggrund af, at enheden tidligere har været identificeret som operatør af væsentlige tjenester i medfør af NIS 1-direktivet, og hvor omstændighederne for identifikationen efterfølgende har ændret sig, således at det ikke forekommer rimeligt, at enheden fortsat anses for at være væsentlig.

Der henvises i øvrigt til bemærkningerne til de foreslåede §§ 1, 2, 4 og 5.

3.2. Foranstaltninger til styring af cybersikkerhedsrisici

3.2.1. Gældende ret

NIS 1-direktivets artikel 14, stk. 1 og 2, samt artikel 16, stk. 1 og 2, indeholder bestemmelser om, at der skal fastsættes

sikkerhedskrav for operatører af væsentlige tjenester og udbydere af digitale tjenester.

Sikkerhedskravene omfatter overordnet en forpligtelse til, at de omfattede operatører og udbydere skal træffe passende sikkerhedsforanstaltninger på baggrund af en vurdering af de risici, som virksomheden konkret står over for. Udbydere af digitale tjenester skal ved fastlæggelsen af passende sikkerhedsforanstaltninger tage hensyn til følgende elementer: a) systemers og faciliteters sikkerhed, b) håndtering af hændelser, c) styring af driftskontinuitet, d) monitorering, audit og testning og e) overholdelse af internationale standarder.

For at opnå en større harmoniseringsgrad for så vidt angår de digitale tjenester – særligt henset til de digitale tjenesters grænseoverskridende karakter – fik Europa-Kommissionen i medfør af direktivets artikel 16, stk. 8, til opgave at vedtage gennemførelsesretsakter, der yderligere specificerede bl.a. sikkerhedskravene til udbydere af digitale tjenester. Europa-Kommissionen har vedtaget gennemførelsesforordning (EU) 2018/151 af 30. januar 2018 om regler for anvendelsen af Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 for så vidt angår yderligere specifikation af de elementer, som udbydere af digitale tjenester skal tage i betragtning for at styre risiciene i forhold til sikkerheden i net- og informationssystemer, og af kriterierne for bestemmelse af, om en hændelses konsekvenser er betydelige.

NIS 1-direktivet blev i dansk ret gennemført sektorvist i regulering gældende for de specifikke sektorer, hvor direktivet finder anvendelse, jf. afsnit 2.4 nedenfor.

3.2.2. NIS 2-direktivet

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.

Europa-Kommissionens gennemførelsesforordning (EU) 2024/2690 fastsætter de tekniske og metodologiske krav til de foranstaltninger, der er omhandlet i NIS 2-direktivets artikel 21, stk. 2, for så vidt angår DNS-tjenesteudbydere, topdomænenavneadministratorer og udbydere af cloudcomputingtjenester, at datacentertjenester, af indholdsleveringsnetværk, af administrerede tjenester, af administrerede sikkerhedstjenester, af onlinemarkedspladser af onlinesøgemaskiner og af platforme for sociale netværkstjenester og af tillidstjenester.

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

Med NIS 2-direktivets artikel 44 ophæves NIS 1-direktivet.

Det er Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at NIS 2-direktivets krav om foranstaltninger til styring af cybersikkerhedsrisici bør implementeres således, at direktivets krav om foranstaltninger skrives ind i loven, således at der skabes en fælles ramme for foranstaltninger på tværs af de sektorer, der er omfattet af lovens anvendelsesområde.

Det er endvidere Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at de ansvarlige ressortministre bør bemyndiges til at konkretisere lovens generelle krav om foranstaltninger, såfremt særlige sektorspecifikke hensyn tilsiger dette. En sådan 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. Reglerne bør udstedes af de enkelte ressortministre efter forhandling med ministeren for samfundssikkerhed og beredskab, jf. pkt. 2.2 ovenfor.

Baggrunden for kravet om forhandling er at sikre, at de bekendtgørelser, der konkretiserer denne lovs krav om foranstaltninger, udarbejdes inden for rammerne af direktivet og de gennemførelsesforordninger, som EU-Kommissionen vedtager. Dette skal også ses som led i Ministeriet for Samfundssikkerheds koordinerende rolle, hvor ministeriet skal sikre en tæt koordination og samarbejde mellem tilsynsmyndighederne, herunder i forhold til tilsyn og håndhævelse.

Det er derudover Ministeriet for Samfundssikkerhed og Beredskab opfattelse, at ministeren for samfundssikkerhed og beredskab bør kunne fastsætte nærmere regler i bekendtgørelsesform om anvendelse af særlige IKT-produkter, -tjenester og -processer med henblik på, 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 enheder til at 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. Det foreslås endvidere, at foranstaltningerne skal omfatte eller tage højde for de elementer, der fremgår af direktivets artikel 21, stk. 2.

Det foreslås i forlængelse heraf, at de relevante ressortministre inden for deres områder – efter forhandling med ministeren for samfundssikkerhed og beredskab – kan fastsætte nærmere regler om de krav til foranstaltninger, som væsentlige og vigtige enheder skal træffe til styring af cybersikkerhedsrisici. Bemyndigelsesbestemmelsen forudsættes anvendt i tilfælde, hvor særlige sektorspecifikke hensyn tilsiger et behov for konkretisering af denne lovs krav til foranstaltninger. Nærmere konkretisering kan navnlig foretages, hvor risikobilledet tilsiger det.

Kravene vil kunne tilpasses de enkelte sektorers specifikke forhold, ligesom der i overensstemmelse med direktivets forudsætninger ud fra en risikobaseret tilgang vil kunne differentieres i kravene til kategorier af enheder inden for samme sektor, henset til forskelle i enhedernes risikoeksponering, størrelse og den potentielle samfundsmæssige og økonomiske betydning af eventuelle hændelser.

Det bemærkes i den forbindelse, at enheder med flere forskellige virksomhedsområder kan indgå i flere af de sektorer, der er defineret i direktivet. Disse enheder vil i givet fald skulle efterleve de krav, der gælder for de forskellige virksomhedsområder.

Med henblik på at sikre, at der ikke fastsættes indbyrdes modsatrettede regler, vil en ressortministers eventuelle fastsættelse af regler om krav til foranstaltninger til styring af cybersikkerhedsrisici inden for sektoren skulle ske efter forhandling med ministeren for samfundssikkerhed og beredskab. Dette skal også ses som led i Ministeriet for Samfundssikkerhed og Beredskabs koordinerende rolle, hvor ministeriet skal sikre en tæt koordination og samarbejde mellem tilsynsmyndighederne, herunder i forhold til tilsyn og håndhævelse. Der henvises herom til afsnit 2.2.2 samt bemærkningerne til det foreslåede § 20, stk. 3.

Det foreslås endvidere, at en enhed, der finder, at den ikke overholder 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 enhedens 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.

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) be-

styrelsen 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.

Der henvises til bemærkningerne til den foreslåede § 7.

Endelig foreslås det på baggrund af direktivets artikel 24, at vedkommende ressortminister efter forhandling med ministeren for samfundssikkerhed og beredskab kan fastsætte regler om, at væsentlige og vigtige enheder 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 enhed eller indkøbes fra tredjeparter.

Der henvises i øvrigt til bemærkningerne til de foreslåede §§ 6-8.

3.3. Hændelsesrapportering

3.3.1. Gældende ret

NIS 1-direktivet forpligtede i artikel 14, stk. 3 og 4, og artikel 16, stk. 3-5, operatører af væsentlige tjenester og udbydere af digitale tjenester til hurtigst muligt at underrette myndighederne om eventuelle hændelser, der har væsentlig forstyrrende virkning på levering af de pågældende tjenester. Direktivet fastsætter nærmere kriterier for, hvornår en hændelse anses for at være væsentlig.

Det følger endvidere af direktivets artikel 14, stk. 6, og artikel 16, stk. 7, at myndighederne under visse betingelser kan informere offentligheden om væsentlige hændelser eller kræve, at den relevante operatør eller udbyder gør det. Myndighederne kan endvidere i relevant omfang informere øvrige EU-medlemsstater, som måtte være berørt.

NIS 1-direktivet blev i dansk ret gennemført sektorvist i regulering gældende for de specifikke sektorer, hvor direktivet finder anvendelse, jf. afsnit 2.4 nedenfor.

Underretninger om hændelser indgives i dag via selvbetjeningsløsningen Virk.dk. Når der indgives en hændelsesrapportering på Virk.dk, fordeles denne automatisk til den eller de relevante kompetente myndigheder, CSIRT'en og til det centrale kontaktpunkt.

De kompetente myndigheder kan anvende hændelsesunderretningerne til arbejdet med at styrke cybersikkerheden på tværs af sektorerne samt til at vurdere, om de som tilsynsmyndighed skal iværksætte opfølgende skridt, herunder indlede tilsyn, mens underretningerne til CSIRT'en og til det centrale kontaktpunkt sker med et mere operationelt sigte i relation til bl.a. at skabe et situationsoverblik og i relevant omfang bistå med håndtering af hændelsen.

Det er i dag de enkelte tilsynsmyndigheder, der foretager orientering af offentligheden om en væsentlig hændelse. CSIRT'en og det centrale kontaktpunkt foretager dog i dag orientering af offentligheden i tilfælde, hvor en hændelse berører flere sektorer.

3.3.2. NIS 2-direktivet

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 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 til-

svarende 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.

NIS 2-direktivet fastsætter i artikel 23, stk. 4, 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, 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.

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.

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.

3.3.3. Ministeriet for Samfundssikkerhed og Beredskabs overvejelser

Det foreslås, at der fastsættes rapporteringsforpligtelser, som i deres indhold svarer til NIS 2-direktivets artikel 23. Kriterierne vil således fastsætte de generelle rammer for, hvornår en hændelse anses for at være væsentlig.

Det foreslås endvidere, at væsentlige og vigtige enheder uden unødigt ophold skal underrette den relevante kompetente myndighed og CSIRT'en om, enhver væsentlig hændelse, og at kravene til fremgangsmåden og fristerne for underretningerne indholdsmæssigt svarer til direktivets.

Det er Ministeriet for Samfundssikkerhed og Beredskabs vurdering, at de ansvarlige ressortministre bør bemyndiges til at fastsætte nærmere regler om hvornår en hændelse anses for at være væsentlig. Det forudsættes, at bemyndigelsen benyttes i særlige tilfælde til at kunne fastsætte nærmere regler om væsentlige hændelser inden for deres respektive sektor, som tager de fornødne hensyn til særligt kritiske systemer mv.

Det er Ministeriet for Samfundssikkerhed og Beredskabs vurdering, at den nærmere konkretisering i bekendtgørelser skal ske efter forhandling med ministeren for samfundssikkerhed og beredskab, navnlig for i videst muligt omfang at sikre ensartethed under hensyn til de sektorspecifikke forhold.

Det skal samtidig sikres, at der ikke fastsættes indbyrdes modsatrettede regler. Dette skal også ses som led i Ministeriet for Samfundssikkerheds koordinerende rolle, hvor ministeriet skal sikre en tæt koordination og samarbejde mellem tilsynsmyndighederne, herunder i forhold til tilsyn og håndhævelse.

Det er endvidere Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at underretninger om hændelser, nærvedhændelser og cybertrusler bør være undtaget fra reglerne om aktindsigt efter lov om offentlighed i forvaltningen og partsaktindsigt efter forvaltningsloven.

Særligt for virksomheder kan oplysninger om, at der f.eks. er gennemført et vellykket hackerangreb, hvor virksomheden har mistet data, i høj grad skade virksomhedens omdømme, og det kan i praksis afholde mange virksomheder fra frivilligt at underrette CSIRT'en om et sådant hackerangreb. Derfor foreslås det med bestemmelsen, at underretningerne i deres helhed undtages fra aktindsigt, herunder partsaktindsigt efter forvaltningsloven. Undtagelsen kan omfatte underretningssagen som helhed. Der henvises til Folketingstidende 2015-16, tillæg A, L 10 som fremsat, side 22.

Undtagelse af frivillige underretninger fra aktindsigt vil på denne baggrund øge enheders incitament til frivilligt at underrette om hændelser, nærvedhændelser og cybertrusler.

Undtagelsen fra aktindsigt omfatter derimod ikke virksomheders adgang til at gøre sig bekendt med oplysninger, der vedrører deres egne forhold. Dette gælder allerede i dag. Der henvises til Folketingstidende 2015-16, tillæg A, L 10 som fremsat, side 22.

Det bemærkes, at undtagelsen ikke omfatter de foreslåede obligatoriske underretninger om væsentlige hændelser.

3.3.4. Den foreslåede ordning

Det foreslås, at der fastsættes rapporteringsforpligtelser, som i deres indhold svarer til NIS 2-direktivets artikel 23. Kriterierne vil således fastsætte de generelle rammer for, hvornår en hændelse anses for at være væsentlig.

Det foreslås endvidere, at væsentlige og vigtige enheder uden unødigt ophold skal underrette den relevante kompetente myndighed og CSIRT'en om enhver væsentlig hæn-

delse, og at kravene til fremgangsmåden og fristerne for underretningerne indholdsmæssigt svarer til direktivets.

Henset til kriteriernes generelle udformning finder Ministeriet for Samfundssikkerhed det hensigtsmæssigt, at der gives mulighed for, at der sektorvist kan fastsættes nærmere regler om, hvornår en hændelse anses for at være væsentlig. De kompetente myndigheder vil herefter i særlige tilfælde kunne fastsætte nærmere regler om væsentlige hændelser inden for deres respektive sektor, som tager de fornødne hensyn til særligt kritiske systemer mv.

Det foreslås på den baggrund desuden, at vedkommende ressortminister bemyndiges til – efter forhandling med ministeren for samfundssikkerhed og beredskab – inden for sit område at fastsætte nærmere regler om, hvornår en hændelse anses for at være væsentlig. Det foreslås, at reglerne udstedes efter forhandling med ministeren for samfundssikkerhed og beredskab, navnlig for i videst muligt omfang at sikre ensartethed under hensyn til de sektorspecifikke forhold. Det forudsættes, at de kompetente myndigheder i relevant omfang vil være særligt opmærksomme på at yde vejledning til enheder, der omfattes af særlige sektorspecifikke krav om væsentlige hændelser.

Det bemærkes, at der vil være tale om en oplysningspligt 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 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 herudover i overensstemmelse med artikel 23, stk. 1, 2. pkt., i NIS 2-direktivet, at væsentlige og vigtige enheder uden unødigt ophold skal underrette modtagerne af deres tjenester om væsentlige hændelser, der sandsynligvis vil påvirke leveringen af deres tjenester negativt. Enhederne 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 oplyse om selve truslen.

Endelig foreslås det, at den relevante kompetente myndighed under visse betingelser kan informere offentligheden om den væsentlige hændelse eller kræve, at enheden gør det. 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 være CSIRT'en, der vil kunne informere offentligheden om den væsentlige hændelse.

Forud for orientering af offentligheden vil den relevante kompetente myndighed eller CSIRT'en skulle høre den væsentlige eller vigtige enhed, der har underrettet om hændelsen, herunder med henblik på vurdering af, om der er oplysninger, der af enheden betragtes som fortrolige. Det bemærkes, at en kompetent myndighed eller CSIRT'en ved overvejelse om orientering af offentligheden om en hændelse skal sikre, at orienteringen sker inden for rammerne af forvaltningslovens § 27.

I tilfælde, hvor CSIRT'en orienterer offentligheden, vil dette ske efter forudgående koordination med de relevante kompetente myndigheder, hvor det bl.a. vil blive drøftet, hvilke oplysninger der anses for fortrolige, og som dermed ikke skal offentliggøres.

Det foreslås, at underretninger om hændelser, nærvedhændelser og cybertrusler bør være undtaget fra reglerne om aktindsigt efter lov om offentlighed i forvaltningen og partsaktindsigt efter forvaltningsloven.

Der henvises i øvrigt til bemærkningerne til de foreslåede §§ 12-16

3.4. Tilsyn og håndhævelse

3.4.1. Gældende ret

NIS 1-direktivets artikel 15 og 17 fastsatte forpligtelser for de kompetente myndigheder til at føre tilsyn med opfyldelsen af direktivet i de omfattede sektorer.

Det følger af direktivet, at de kompetente myndigheder skal have beføjelser og midler til at pålægge operatører af væsentlige tjenester at levere de oplysninger, der er nødvendige for at vurdere sikkerheden i deres net- og informationssystemer, herunder dokumenterede sikkerhedspolitikker og dokumentation for den faktiske gennemførelse af sikkerhedspolitikker. Tilsvarende følger det for udbydere af digitale tjenester, at de kompetente myndigheder skal have beføjelser og midler til at pålægge udbyderne at forelægge de oplysninger, der er nødvendige for at vurdere sikkerheden i deres net- og informationssystemer, herunder dokumenterede sikkerhedspolitikker, og afhjælpe mangler i opfyldelsen af direktivets sikkerhedskrav.

NIS 1-direktivet blev i dansk ret gennemført sektorvist i re-

gulering gældende for de specifikke sektorer, hvor direktivet finder anvendelse, jf. pkt. 2.4 ovenfor.

3.4.2. NIS 2-direktivet

3.4.2.1. Tilsyn

NIS 2-direktivets artikel 31, stk. 1, fastsætter 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.

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.

3.4.2.2. Håndhævelse

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.

Over for 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 foranstalt-

ninger til styring af cybersikkerhedsrisici og underretningsforpligtelser.

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

3.4.3. Ministeriet for Samfundssikkerhed og Beredskabs overvejelser

Det foreslås, at der fastsættes regler om de kompetente myndigheders tilsynsforanstaltninger, som i deres indhold svarer til NIS 2-direktivets artikel 31-33.

Det bemærkes, at det fremgår af direktivets præambelbetragtning nr. 122, at der ved direktivet indføres en differentiering af tilsynsordningen for henholdsvis væsentlige og vigtige enheder med henblik på at sikre en rimelig balance mellem forpligtelser for disse enheder og for de kompetente myndigheder. Væsentlige enheder bør derfor være underlagt en omfattende forudgående og efterfølgende tilsynsordning, mens vigtige enheder bør være underlagt en lettere, rent efterfølgende tilsynsordning. Vigtige enheder bør derfor ikke være forpligtet til systematisk at dokumentere overholdelsen af foranstaltninger til styring af cybersikkerhedsrisici, mens de kompetente myndigheder bør anvende en reaktiv efterfølgende tilgang til tilsyn og dermed ikke have en generel forpligtelse til at føre tilsyn med disse enheder. Det efterfølgende tilsyn med vigtige enheder kan udløses af dokumentation, tegn eller oplysninger, som de kompetente myndigheder gøres opmærksom på, og som efter deres opfattelse tyder på potentielle overtrædelser af dette direktiv. Sådan dokumentation, sådant tegn eller sådanne oplysninger kunne være af den type, som de kompetente myndigheder modtager fra andre myndigheder, enheder, borgere, medier eller andre kilder eller offentligt tilgængelige oplysninger, eller kunne hidrøre fra andre aktiviteter, der indgår i de kompetente myndigheders udførelse af deres opgaver.

Det er på den baggrund Ministeriet for Samfundssikkerhed og Beredskabs vurdering, at der for så vidt angår tilsynsforanstaltninger bør sondres mellem foranstaltninger over for henholdsvis væsentlige og vigtige enheder, således at væsentlige enheder underlægges et omfattende forudgående og efterfølgende tilsyn, mens vigtige enheder derimod underlægges et lettere og 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 i 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.

For så vidt angår håndhævelsesforanstaltningerne er det Ministeriet for Samfundssikkerhed og Beredskabs vurdering, at der bør fastsættes regler om de kompetente myndigheders håndhævelsesforanstaltninger, som i deres indhold svarer til NIS 2-direktivets artikel 31-33.

Som nærmere beskrevet ovenfor, oplister NIS 2-direktivet de håndhævelsesforanstaltninger, der som minimum skal kunne anvendes over for henholdsvis væsentlige og vigtige enheder. Der er navnlig tale om, at myndighederne skal kunne pålægge enhederne at afhjælpe konstaterede mangler eller på en nærmere angivet måde at overholde kravene til deres foranstaltninger til styring af cybersikkerhedsrisici eller at efterleve underretningsforpligtelserne. Også disse oplistninger af foranstaltninger over for henholdsvis væsentlige og vigtige enheder er i vidt omfang identiske, idet den kompetente myndighed over for væsentlige enheder dog som noget særligt kan udpege en monitoreringsansvarlig med veldefinerede opgaver til i en nærmere fastsat periode at føre tilsyn med den pågældende enheds overholdelse af kravene til foranstaltninger til styring af cybersikkerhedsrisici og underretningsforpligtelser.

I overensstemmelse med NIS 2-direktivets præambelbetragtning nr. 127, bør der ved udøvelse af håndhævelsesforanstaltninger tages behørigt hensyn til overtrædelsen af dette direktivs art, grovhed og varighed, den forvoldte materielle eller immaterielle skade, hvorvidt overtrædelsen var forsætlig eller uagtsom, tiltag truffet for at forebygge eller afbøde den materielle eller immaterielle skade, graden af ansvar eller eventuelle relevante tidligere overtrædelser, graden af samarbejde med den kompetente myndighed og enhver anden skærpende eller formildende omstændighed. Ved valg af håndhævelsesforanstaltning skal den kompetente myndighed foretage en konkret vurdering, som overholder det forvaltningsretlige proportionalitetsprincip.

3.4.3.1. 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.

Der findes i dansk ret og på cybersikkerhedsområdet i øvrigt et stort antal certificerings- og godkendelsesordninger, og området er i hastig udvikling.

På den baggrund er der efter Ministeriet for Samfundssikkerhed og Beredskabs opfattelse behov for at foretage et nærmere analysearbejde for at klarlægge, i hvilket omfang der er ordninger, som bør være omfattet af den af direktivet foreskrevne mulighed for at suspendere certificerings- og godkendelsesordninger. På den baggrund foreslås det, at vedkommende minister bemyndiges til – efter forhandling med ministeren for samfundssikkerhed og beredskab – at fastsætte nærmere regler om, hvilke certificeringer og godkendelser der kan blive genstand for suspension efter den foreslåede bestemmelse. Dette skal også ses i lyset af, at en potentielt vidtrækkende mulighed for suspension af en certificering eller godkendelse stiller desto højere krav til forudsigeligheden af reguleringen. Ved at fastsætte nærmere regler i bekendtgørelsesform sikres det endvidere, at reglerne løbende kan tilpasses den udvikling, der er på området.

Det bemærkes i denne forbindelse, 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, hvorefter »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. Med henblik på at sikre en minimumsimplementering af direktivet foreslås det, at betegnelsen »enhver fysisk person med ledelsesansvar på niveau med administrerende direktør« anvendes.

Hensynene, som er oplistet i NIS 2-direktivets artikel 32, stk. 7, og som er beskrevet ovenfor, vil også skulle indgå i en afgørelse om midlertidige suspensioner eller midlertidige forbud mod, at fysiske personer må udøve ledelsesfunktioner.

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. De midlertidige suspensioner eller forbud må endvidere alene anvendes, hvor en række mindre indgribende midler har vist sig ikke at være tilstrækkelige.

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.

Det er efter Ministeriet for Samfundssikkerhed og Beredskabs opfattelsemest 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 bør træffes af den relevante kompetente myndighed, der vil kunne belyse og begrunde, hvorfor indgrebet vurderes påkrævet.

Det er Ministeriet for Samfundssikkerhed og Beredskabs vurdering, at afgørelser om midlertidige suspensioner og forbud ikke bør kunne indbringes for anden administrativ myndighed. Adgangen til administrativ rekurs afskæres således. Dette skyldes navnlig, at denne lov vil finde anvendelse for en lang række af sektorer, hvor der er forskellig praksis for administrativ rekurs. Det er således Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at der med nærværende lov bør skabes en fælles ramme for implementering af NIS 2-direktivet på tværs af de omfattede sektorer, hvorfor enheder inden for de forskellige sektorer som altovervejende udgangspunkt bør have samme rettigheder og pligter.

Det er endvidere Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at den person eller væsentlige enhed, som afgørelsen vedrører, bør kunne forlange, at den relevante myndighed indbringer afgørelsen for domstolene. Myndigheden bør således efter begæringens fremsættelse indbringe sagen for domstolene.

3.4.4. Den foreslåede ordning

Det foreslås, at de kompetente myndigheder inden for deres respektive områder fører tilsyn med væsentlige og vigtige enheders efterlevelse af loven og de regler, der udstedes i medfør af loven.

Det foreslås endvidere, at myndighederne tillægges tilsyns- og håndhævelsesbeføjelser, der indholdsmæssigt svarer til det, som NIS 2-direktivet foreskriver, herunder med de for-

udsatte forskelle i tilgangen til væsentlige og vigtige enheder.

I overensstemmelse med forudsætningerne i NIS 2-direktivet foreslås det i den forbindelse, at de kompetente myndigheder, ved tilrettelæggelsen af deres tilsyn med væsentlige og vigtige enheder, anlægger en differentieret tilgang, således at der løbende føres tilsyn med væsentlige enheders efterlevelse af lovgivningen, mens der ved tilsynet med vigtige enheder anlægges en reaktiv tilgang, således at der først ved tegn på, at den vigtige enhed ikke overholder lovgivningen, iværksættes et tilsyn.

For så vidt angår den særlige suspensions- og forbudsordning, som direktivet foreskriver for så vidt angår væsentlige enheder, foreslås det, at såfremt den kompetente myndighed vurderer, at allerede pålagte håndhævelsesforanstaltninger har vist sig at være utilstrækkelige, kan den kompetente myndighed fastsætte en frist, inden for hvilken den væsentlige enhed skal foretage de nødvendige tiltag for at afhjælpe manglerne eller opfylde den kompetente myndigheds krav. Er tiltagene ikke foretaget inden for den fastsatte frist, kan den kompetente myndighed træffe afgørelse om 1) midlertidigt at suspendere en certificering eller godkendelse vedrørende dele af eller alle de relevante tjenester, enheden leverer, eller aktiviteter, der udføres af enheden, og 2) midlertidigt at forbyde enhver fysisk person med ledelsesansvar på direktionsniveau eller juridisk repræsentant i enheden at udøve ledelsesfunktioner i den pågældende enhed.

Det foreslås, at vedkommende minister efter forhandling med ministeren for samfundssikkerhed og beredskab 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 vedkommende minister 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 enheden træffer de nødvendige tiltag for at afhjælpe de mangler eller opfylde de krav, som gav anledning til, at foranstaltningerne blev anvendt.

Det foreslås, at enheden 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.

Den relevante myndighed anlægger i givet fald sag inden for rammerne af den civile retspleje mod den enhed eller person, som har forlangt sagen indbragt.

Der henvises i øvrigt til de foreslåede bestemmelser i §§ 20-25.

3.5. Ansvar og sanktioner

3.5.1. Gældende ret

Efter NIS 1-direktivets artikel 21 skal medlemsstaterne fastsætte regler om sanktioner, der anvendes i tilfælde af overtrædelser af de nationale regler, som er vedtaget i medfør af direktivet, og 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 1-direktivet indeholder ikke nærmere bestemmelser om strafansvar for bestemte fysiske personer.

NIS 1-direktivet blev i dansk ret gennemført sektorvist i regulering gældende for de specifikke sektorer, hvor direktivet finder anvendelse, jf. afsnit 2.4 ovenfor.

3.5.2. 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.

Der lægges 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.

3.5.3. Ministeriet for Samfundssikkerhed og Beredskabs overvejelser

Med NIS 2-direktivets artikel 44 ophæves NIS 1-direktivet.

I lighed med NIS 1-direktivet indeholder NIS 2-direktivet i artikel 36 en bestemmelse, hvorefter medlemsstaterne skal 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.

Det følger af NIS 2-direktivets artikel 36, at sanktionerne skal være effektive, stå i et rimeligt forhold til overtrædelsen og have afskrækkende virkning.

Det følger af NIS 2-direktivets artikel 34, at sanktionen for væsentlige og vigtige enheders overtrædelser af bestem-

melserne i NIS 2-direktivet er en administrativ bøde, som kompetente myndigheder sanktionerer.

NIS 2-direktivets artikel 34, stk. 1-7, indeholder således en række generelle betingelser for pålæggelse af administrative bøder til væsentlige og vigtige enheder.

I medfør af artikel 34, stk. 8, er det imidlertid muligt at vælge strafferetlige sanktioner frem for administrative bøder. Det følger således af artikel 34, stk. 8, at hvis en medlemsstats nationale retssystem ikke giver mulighed for at pålægge administrative bøder, kan bestemmelsen anvendes på en sådan måde, at de kompetente myndigheder tager skridt til bøder, som de kompetente nationale domstole pålægger dem. Det skal sikres, at disse retsmidler er effektive, og at deres virkning svarer til virkningen af administrative bøder, som pålægges af de kompetente myndigheder.

Indførelse af administrative bøder giver i dansk ret betænkeligheder i forhold til grundlovens § 3 om magtens tredeling. Bestemmelsen antages at indebære, at lovgivningsmagten ikke i almindelighed kan henlægge behandlingen af strafferetlige bødesager til administrative myndigheder. I dansk retspleje er det i øvrigt et grundlæggende princip, at bøder, der har karakter af en strafferetlig sanktion, kun kan idømmes ved domstolene og i strafferetsplejens former, der sikrer den sigtede en effektiv beskyttelse. Det er på den baggrund Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at direktivets undtagelsesbestemmelse i forhold til administrative bøder finder anvendelse. Direktivets bestemmelser om administrative bøder vil således skulle fortolkes og gennemføres på en måde, hvor bøder ikke pålægges administrativt, men i det almindelige strafferetlige system. Det indebærer, at de kompetente myndigheder i givet fald vil skulle indgive politianmeldelse, såfremt de konstaterer strafbelagte overtrædelser af denne lov eller regler udstedt i medfør af denne lov.

Det følger af NIS 2-direktivet, 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.

De kompetente myndigheder vil skulle påse, at denne lov og regler udstedt i medfør af loven efterleves, herunder undersøge mulige overtrædelser af lovgivningen. I en situation, hvor en kompetent myndighed måtte blive bekendt med, at der kan være sket en strafbar overtrædelse af loven eller regler udstedt i medfør af loven, vil myndigheden efter Ministeriet for Samfundssikkerhed og Beredskabs opfattelse skulle foretage en konkret vurdering – under hensyntagen til omstændighederne i hver enkelt sag og sanktionsregimets effektivitet, forholdsmæssighed og afskrækkende virkning – og på den baggrund beslutte, om forholdet skal politianmeldes.

NIS 2-direktivets artikel 34, stk. 3-5, 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 iværksætte håndhævelsesforanstaltninger efter artikel 32, stk. 7, jf. afsnit 3.4.2 ovenfor.

Henset til, at der ikke i almindelighed anvendes administrative bøder i dansk ret, jf. ovenfor, forudsættes det, at de pågældende hensyn indgår i de kompetente myndigheders beslutning om politianmeldelse af et forhold, samt i politi- og anklagemyndighedens og domstolenes vurdering af sagen, herunder ved udmålingen af en eventuel bøde.

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 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 endvidere af NIS 2-direktivets artikel 34, stk. 5, at vigtige enheders overtrædelse af direktivets artikel 21 (foranstaltninger til styring af cybersikkerhedsrisici) eller artikel 23 (rapporteringsforpligtelser) skal straffes 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.

Ministeriet for Samfundssikkerhed og Beredskab finder, at det i overensstemmelse med det grundlæggende princip i dansk retspleje om strafferetlige sanktioner og som følge af muligheden i direktivets artikel 34, stk. 8, bør fastsættes i lovforslaget, at overtrædelser af de pågældende bestemmelser i loven skal kunne straffes med bøde.

3.5.3.1. Særligt om ansvar og sanktioner for den offentlige forvaltning

Det følger af NIS 2-direktivets artikel 34, stk. 7, at den enkelte medlemsstat kan fastsætte regler om, hvorvidt og i hvilket omfang (administrative) bøder skal kunne pålægges offentlige forvaltningsorganer.

Det er i dansk ret et generelt princip, at staten, regioner og kommuner alene kan straffes for overtrædelser, der begås ved udøvelse af virksomhed, som svarer til eller kan sidestilles med virksomhed udøvet af private, jf. straffelovens § 27, stk. 2.

En anvendelse af dette princip ved gennemførelsen af NIS 2-direktivet vil betyde, at offentlige myndigheder kun vil kunne straffes for tilsidesættelse af deres forpligtelser efter denne lov og regler udstedt i medfør af loven, når deres aktiviteter ikke har karakter af myndighedsudøvelse, dvs. hvis de leverer tjenester eller udøver virksomhed, der i øvrigt måtte være omfattet af direktivet, eksempelvis inden for sundhedssektoren eller spildevandshåndtering.

3.5.2.2. Særligt om tvangsbøder

Det følger af NIS 2-direktivets artikel 34, stk. 6, at medlemsstaterne kan fastsætte beføjelser til at pålægge tvangsbøder for at tvinge en væsentlig eller vigtig enhed til at bringe en overtrædelse af direktivet til ophør i overensstemmelse med en forudgående afgørelse truffet af den kompetente myndighed.

På denne baggrund er det Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at der ikke bør skabes hjemmel til administrative tvangsbøder på dette område. Det skal bl.a. ses i lyset af, at det på nuværende tidspunkt er usikkert, om de forhold, der i givet fald vil kunne begrunde tvangsbøder, er så tilstrækkeligt objektivt konstaterbare, at det vil være ubetænkeligt at skabe en sådan hjemmel.

Ministeriet for Samfundssikkerhed og Beredskab vurderer således som udgangspunkt, at de retsmidler, der foreslås med denne lov, herunder tilsyns- og håndhævelsesforanstaltningerne samt muligheden for at offentliggøre afgørelser mv., er tilstrækkelige til at sikre, at reglerne efterleves. Dette skal også ses i lyset af de eksisterende muligheder i retsplejeloven for at anvende tvangsbøder.

3.5.2.3. Særligt om fysiske personers strafansvar og ansvarssubjekt

Artikel 34 i NIS 2-direktivet indeholder generelle betingelser for at pålægge 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 direktivets artikel 32, stk. 6, at medlemsstaterne skal sikre, 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 skal sikre, at det er muligt at drage sådanne fysiske personer til ansvar for tilsidesættelse af deres forpligtelser til at sikre overholdelsen af NIS 2-direktivet. Dette berører dog efter direktivet ikke national ret for så vidt angår ansvaret for embedsmænd og personer valgt eller udnævnt til offentlige hverv.

Det er i 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.

Efter rigsadvokatmeddelelse om strafansvar for juridiske personer, er udgangspunktet ved valg af ansvarssubjekt i særlovgivningen, 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 afgørelse 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.

3.5.2.4. Særligt om brud på persondatasikkerheden

Artikel 35, stk. 2, i NIS 2-direktivet indeholder særlige bestemmelser for så vidt angår overtrædelser af forpligtelserne i direktivets artikel 21 (om foranstaltninger til styring af cybersikkerhedsrisici) og artikel 23 (om rapporteringsfor-

pligtelser), der (også) kan medføre et brud på persondatasikkerheden i medfør af databeskyttelsesforordningen.

Det følger således 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 også efter omstændighederne kan udgøre et brud på databeskyttelsesreglerne, 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 – i dansk ret 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.

Det bemærkes, at loven ikke ændrer på de dataansvarliges forpligtelser til anmeldelse af overtrædelser af brud på persondatasikkerheden efter de databeskyttelsesretlige regler.

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 uden unødig forsinkelse og om muligt senest 72 timer efter, at denne er blevet bekendt med bruddet på persondatasikkerheden, »medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder«.

De kompetente myndigheder vil derfor skulle foretage underretning af Datatilsynet på baggrund af NIS 2-direktivets artikel 35, stk. 1, om forhold der kan medføre et brud på persondatasikkerheden, medmindre det er usandsynligt, at et eventuelt brud på persondatasikkerheden vil indebære en risiko for fysiske personers rettigheder eller frihedsrettigheder. Der må overlades de kompetente myndigheder et bredt skøn ved foretagelsen af denne vurdering. Det bemærkes dog i den forbindelse, at en underretning til den relevante kompetente myndighed og CSIRT'en efter de forslåede regler i §§ 12 og 13 efter omstændighederne vil kunne udgøre et brud på persondatasikkerheden.

Det forudsættes, at den kompetente myndighed i relevant omfang hører Datatilsynet 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.

3.5.3. Den foreslåede ordning

Det foreslås, at der som led i gennemførelsen af NIS 2-direktivet indsættes sanktionsbestemmelser i loven med det formål, at overtrædelse af alle materielle og processuelle krav i loven eller regler udstedt til væsentlige og vigtige enheder i medfør af loven kan straffes med bøde.

Det foreslås således, at den der overtræder § 6, stk. 1 eller 2, §§ 9 eller 10, § 11, stk. 1-6, § 12, stk. 1, § 13, stk. 1 eller 2, eller § 15, undlader at efterkomme en kompetent myndigheds afgørelse efter § 23, stk. 1, nr. 1 eller 2, undlader at efterkomme påbud og forbud efter §§ 22, stk. 1, nr. 3-6 eller 25, stk. 1, nr. 3-6, undlader at efterkomme afgørelse efter § 16, stk. 2, § 21, stk. 1, nr. 2 eller nr. 5-7, eller § 24, stk. 1, nr. 2 eller nr. 4-6, eller hindrer de kompetente myndigheder i at føre tilsyn efter bestemmelserne i § 21, stk. 1, nr. 1-4, eller § 24, stk. 1, nr. 1-3, straffes med bøde. Det foreslås i den forbindelse, at der ikke anvendes administrative bøder, men at bøder udstedes og udmåles i det almindelige straffeprocessuelle system.

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

Det forudsættes i overensstemmelse med en minimumsimplementering af direktivets artikel 34, stk. 4 og 5, at bødens størrelse for væsentlige enheder for så vidt angår overtrædelse af bestemmelserne i § 6, stk. 1, §§ 12, 13 og 15, § 16, stk. 2, og regler udstedt i medfør af § 6, stk. 3, maksimalt vil udgøre et beløb svarende til 10.000.000 euro eller 2 pct.

af enhedens samlede globale årsomsætning i det foregående regnskabsår, alt efter hvad der er højest. Det forudsættes desuden, at bødens størrelse for vigtige enheder for så vidt angår overtrædelse af de samme bestemmelser maksimalt vil udgøre et beløb svarende til 7.000.000 euro eller 1,4 pct. af enhedens samlede globale årsomsætning i det foregående regnskabsår, alt efter hvad der er højest.

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 §§ 22, 23 og 25.

Ved afgørelse om at politianmelde et forhold, ved pålæg af en bøde og ved udmåling af bødens størrelse forudsættes det, at der lægges vægt på de hensyn, der er beskrevet i pkt. 3.5.2 ovenfor.

Der henvises i øvrigt til bemærkningerne til den foreslåede § 32.

4. Forholdet til databeskyttelsesreglerne

Med lovforslaget gennemføres NIS 2-direktivet på tværs af en lang række sektorer.

Lovforslaget indebærer en række forpligtelser for omfattede enheder samt myndighedsopgaver for de relevante myndigheder, der i et vist omfang vil indebære behandling af personoplysninger.

Efter de foreslåede bestemmelser i §§ 9 og 10, skal enhederne som led i overholdelsen af registreringsforpligtelserne indgive en række oplysninger til de kompetente myndigheder. Oplysningerne kan indeholde almindelige personoplysninger eksempelvis i form af navn og visse kontaktoplysninger på medarbejdere hos enheden. Det kan endvidere ikke udelukkes, at en enkeltmandsvirksomhed vil være omfattet af loven. Der vil derfor blive behandlet almindelige personoplysninger i form af navn på virksomheden.

Der er desuden i den foreslåede § 11 en forpligtelse for topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringsdata til at skulle føre en database, der indeholder domænenavnsregistreringsdata. Blandt disse data er bl.a. almindelige personoplysninger såsom den registreredes navn, e-mailadresse og telefonnummer. Det følger af den foreslåede ordning, at legitime adgangssøgende – hvilket omfatter de kompetente myndigheder, CSIRT'en og myndigheder, som i henhold til EU-retten eller dansk ret arbejder med at forebygge, efterforske eller retsforfølge strafbare handlinger – efter anmodning skal kunne få adgang til specifikke domænenavnsregistreringsdata, herunder personoplysninger.

Det følger af de foreslåede bestemmelser i §§ 12 og 13, at væsentlige og vigtige enheder skal underrette den relevante kompetente myndighed og CSIRT'en om enhver væsentlig hændelse. En enheds hændelsesunderretning til myndighederne vil kunne indeholde almindelige personoplysninger. 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 §§ 21-23 og §§ 24 og 25 vil blive behandlet almindelige personoplysninger. F.eks. kan den kompetente myndighed i forbindelse med udførelsen af tilsyn, jf. § 21, stk. 1, nr. 5 og 6 og § 24, stk. 1, nr. 4 og 5, kræve at få udleveret oplysninger, der er nødvendige for efterfølgende at vurdere de foranstaltninger til styring af cybersikkerhedsrisici, som den berørte enhed har indført, samt kræve adgang til data, dokumenter og oplysninger, der er nødvendige for udførelsen af tilsynsopgaven. Det er Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at de oplysninger, der måtte blive behandlet i denne forbindelse, vil udgøre oplysninger om enhedens medarbejdere. Disse oplysninger vil primært udgøre kontaktoplysninger på enhedens kontaktpersoner, ligesom der eksempelvis kan være tale om oplysninger om hvilke medarbejdere, der har adgang til enhedens net- og informationssystemer.

Det bemærkes, at der med den foreslåede § 20, stk. 3, lægges op til, at ministeren for samfundssikkerhed og beredskab kan fastsætte regler om koordinering, ansvar, fordeling af opgaver og udveksling af oplysninger mellem de kompetente myndigheder, samt de kompetente myndigheder og CSIRT'en, herunder i forhold til hændelsesunderretninger efter kapitel 3, tilsyn samt håndhævelse efter kapitel 6. Der forventes i den forbindelse bl.a. fastsat regler, der vil indebære udveksling af almindelige personoplysninger til brug for de kompetente myndigheders koordinering af tilsyn, håndtering af hændelser mv.

Det følger af det foreslåede § 22, stk. 1, nr. 8, og § 25, nr. 6, at den kompetente myndighed kan påbyde en enhed i ikke-anonymiseret form og på en nærmere angiven måde at offentliggøre afgørelser om håndhævelsesforanstaltninger samt resumeer af domme eller bødevedtagelser, hvor der idømmes eller vedtages en bøde. Bestemmelserne indebærer, at der vil kunne blive behandlet almindelige personoplysninger, da det ikke kan udelukkes, at enkeltmandsvirksomheder vil være omfattet af loven.

I medfør af den foreslåede § 28 kan relevante myndigheder videregive oplysninger til andre medlemsstaters myndigheder og institutioner i Den Europæiske Union for at varetage de opgaver, som følger af denne lov eller udstedt i medfør af loven. Myndighederne vil i den forbindelse kunne videregive almindelige personoplysninger. Der kan f.eks. være tale om oplysninger om navn på den væsentlige eller vigtige enhed. Det kan i den forbindelse ikke udelukkes, at en

enkeltmandsvirksomhed vil være omfattet af loven. Der vil endvidere kunne videregives oplysninger om f.eks. navn på medarbejdere mv.

Det er vurderingen, at behandlingen af almindelige personoplysninger i forbindelse med overholdelsen af registreringsforpligtelserne i §§ 9 og 10, pligten til at føre én særskilt database, efter § 11 og underretningsforpligtelserne i §§ 12 og 13 samt myndighedernes anvendelse af tilsyns- og håndhævelsesforanstaltninger efter reglerne i kapitel 6 for private virksomheder vil kunne ske i medfør af databeskyttelsesforordningens artikel 6, stk. 1, litra c og e, jf. stk. 2 og 3.

Det følger således 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. Danmark har en EU-retlig forpligtelse til at gennemføre NIS 2-dikretivets regler i dansk ret.

Herudover følger af litra e, at behandling er lovlig, hvis den er nødvendig af hensyn til udførelse af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlig har fået pålagt.

For så vidt angår offentlige myndigheder behandling af personoplysninger følger det af NIS 2-direktivet, at myndighederne pålægges en række nye myndighedsopgaver. Det skyldes, at lovforslaget har til formål at sikre et højt sikkerhedsniveau for net- og informationssystemer. Direktivet stiller således bl.a. cybersikkerhedskrav til virksomheder, myndigheder og organisationer inden for en lang række samfundskritiske sektorer. Det er Ministeriet for Samfundssikkerhed og Beredskabs vurdering, at der dermed er tale om myndighedsudøvelse omfattet af databeskyttelsesforordningens artikel 6, stk. 1, litra e, jf. stk. 2 og 3.

For så vidt angår privates behandling af personoplysninger sker dette, da NIS 2-direktivet medfører forpligtelser for de udpegede enheder med henblik på at sikre et højt niveau af cybersikkerhed i net- og informationssystemer. Det skal bl.a. ses i lyset af, at Danmark står over for et mere sammensat og komplekst trusselsbillede end for blot få år siden, hvilket ikke mindst gælder på cybersikkerhedsområdet. Net- og informationssystemer spiller i dag en afgørende rolle i samfundet, både for virksomheder, myndigheder og borgere, som alle i stigende grad er afhængige af velfungerende digitale systemer i hverdagen. Behandlingen af personoplysninger vurderes på den baggrund at være en opgave i samfundets interesse, jf. databeskyttelsesforordningens artikel 6, stk. 1, litra e, jf. stk. 2 og 3.

For så vidt angår de kompetente myndigheders adgang til at pålægge en enhed i ikke-anonymiseret form at offentliggøre resumeer af domme eller bødevedtagelser, hvor der idømmes eller vedtages en bøde, jf. de foreslåede bestemmelser i § 22, stk. 1, nr. 8, og § 25, nr. 6, er det Ministeriet for Samfundssikkerhed og Beredskabs vurdering, at de foreslåede bestemmelser giver passende garantier for de registreredes rettigheder og friheder. Der lægges i den forbindelse vægt på, at der ikke er tale om en systematisk offentliggørelsesordning, men en adgang, hvor den kompetente myndighed kun kan påbyde enheden at offentliggøre afgørelser mv. efter en konkret vurdering af omstændighederne i sagen. Ministeriet for Samfundssikkerhed og Beredskab har herved lagt vægt på, at en enhed alene vil blive påbudt at offentliggøre en afgørelse mv. hvis hensynet til de samfundsmæssige interesser ved offentliggørelsen vejer tungere end hensynet til enheden, som er omfattet af afgørelsen mv.

Det er endelig vurderingen, at den foreslåede bestemmelse kan rummes inden for rammerne af databeskyttelsesforordningens artikel 10, 1. pkt, jf. artikel 6, stk. 1, litra c og e. For en nærmere gennemgang af artikel 6, stk. 1, litra c og e, som hjemmelsgrundlag, henvises til ovenfor.

Det er Ministeriet for Samfundssikkerhed og Beredskabs vurdering, at behandlingen af personoplysninger i medfør af de foreslåede bestemmelser i lovforslaget er proportional og ikke går videre, end hvad der er nødvendigt for at opfylde Danmarks EU-retlige forpligtelser til implementering af NIS 2-direktivet.

Ministeriet for Samfundssikkerhed og Beredskab skal afslutningsvis bemærke, at det forudsættes, at de øvrige bestemmelser i databeskyttelsesforordningen og databeskyttelsesloven, herunder de grundlæggende principper i databeskyttelsesforordning artikel 5 også iagttages, når der behandles personoplysninger i medfør af de foreslåede bestemmelser. Det betyder, at personoplysninger skal være tilstrækkelige, relevante og begrænset til, hvad der nødvendigt i forhold til de formål, hvortil de behandles.

4.1. Videregivelse af oplysninger til CSIRT'en og det centrale kontaktpunkt

Styrelsen for Samfundssikkerhed (tidligere Center for Cybersikkerhed) forventes at varetage opgaven som centralt kontaktpunkt.

Navnlig vil opgaven som national CSIRT indebære, at netsikkerhedstjenesten vil kunne behandle personoplysninger hos de berørte enheder. Det følger således af den foreslåede § 17, at CSIRT'en efter anmodning fra en enhed skal kunne yde bistand vedrørende monitorering af enhedens net- og informationssystemer, reagere på hændelser og yde bistand til de berørte enheder samt efter anmodning fra en enhed foretage en proaktiv scanning af enhedens net- og informationssystemer. I forbindelse med løsningen af disse opgaver vil CSIRT'en kunne få adgang til enhedens it-systemer. Såfremt disse it-systemer indeholder personoplysninger, herunder følsomme personoplysninger og personoplysninger vedrørende straffedomme og lovovertrædelser, vil det ikke helt kunne udelukkes, at CSIRT'en vil få adgang til disse oplysninger. Det bemærkes i den forbindelse, at CSIRT'ens medarbejdere ikke vil have til formål at bruge de konkrete oplysninger om eksempelvis strafbare forhold, men derimod

alene undersøge data med henblik på at afdække sikkerhedshændelser eller sårbarheder.

Det følger af § 8 i lov om Center for Cybersikkerhed, jf. lovbekendtgørelse nr. 836 af 7. august 2019, at centerets virksomhed er undtaget databeskyttelsesloven og databeskyttelsesforordningen. Uanset at virksomheden er undtaget fra databeskyttelseslovgivningen, finder størstedelen af de centrale principper i databeskyttelseslovgivningen anvendelse for netsikkerhedstjenesten i medfør af kapitel 6 i lov om Center for Cybersikkerhed.

Databeskyttelsesforordningen og databeskyttelsesloven vil imidlertid finde anvendelse for de væsentlige og vigtige enheder, som anmoder om CSIRT'ens bistand i medfør af den foreslåede § 17.

CSIRT'en er, jf. ovenfor heller ikke omfattet af begrebet "dataansvarlig" i databeskyttelsesforordningen og databeskyttelsesloven. CSIRT'en vil dog i relation til de væsentlige og vigtige enheder være at betragte som en selvstændig dataansvarlig for den behandling af personoplysninger, som CSIRT'en udfører. I tilfælde af, at CSIRT'en får adgang til oplysninger hos væsentlige og vigtige enheder, er det dermed at betragte som en videregivelse mellem to selvstændige dataansvarlige. Denne videregivelse sker inden for rammerne af databeskyttelsesforordningen og databeskyttelsesloven.

For så vidt angår en situation, hvor de offentlige myndigheder, der er omfattet af direktivet, herunder de kompetente myndigheder, videregiver oplysninger til CSIRT'en, henvises der til forordningens artikel 6, stk. 1, litra e, jf. stk. 2 og 3, hvorefter behandling bl.a. er lovlig, hvis behandlingen er nødvendig af hensyn til udførelse af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse. Henset til at videregivelsen er nødvendig af hensyn til udførelsen af opgaven som CSIRT og centralt kontaktpunkt, vurderer Ministeriet for Samfundssikkerhed og Beredskab, at videregivelse af almindelige personoplysninger til CSIRT'en er omfattet af forordningens artikel 6, stk. 1, litra e, jf. stk. 2 og 3.

Det vurderes på den baggrund, at væsentlige og vigtige enheder samt de kompetente myndigheder med hjemmel i databeskyttelsesforordningens artikel 6 kan videregive almindelige personoplysninger til CSIRT'en.

I relation til behandling af eventuelle oplysninger om strafbare forhold henvises der til § 8 i databeskyttelsesloven. Private virksomheders videregivelse af oplysninger om strafbare forhold vurderes at være omfattet af databeskyttelseslovens § 8, stk. 4, 2. pkt., hvorefter videregivelse bl.a. kan ske, når det sker til varetagelse af offentlige interesser, der klart overstiger hensynet til de interesser, der begrunder hemmeligholdelse. Som nævnt ovenfor vurderes formålet med videregivelsen at varetage væsentlige offentlige interesser, som klart overstiger hensynet til den enkelte. Ministeriet for Samfundssikkerhed og Beredskab har ved vurderingen lagt vægt på, at CSIRT'en bl.a. har til opgave at overvåge og analysere cybertrusler, sårbarheder og hændelser på nationalt plan, samt at reagere på hændelser. Ministeriet for Samfundssikkerhed og Beredskab har endvidere lagt vægt på, at CSIRT'ens analytikere ikke vil have til formål at bruge den konkrete oplysning om et strafbart forhold, men derimod alene undersøger data med henblik på at afdække sikkerhedshændelser.

Offentlige myndigheders videregivelse af oplysninger om strafbare forhold vurderes at være omfattet af databeskyttelseslovens § 8, stk. 2, nr. 2 og 3, hvorefter videregivelse af sådanne oplysninger bl.a. kan ske, hvis videregivelsen sker til varetagelse af offentlige interesser, der klart overstiger hensynet til de interesser, der begrunder hemmeligholdelse, eller hvis videregivelsen er nødvendig for udførelsen af en myndigheds virksomhed. Ministeriet for Samfundssikkerhed og Beredskab henviser i den forbindelse til overvejelserne i forhold til private virksomheders videregivelse af sådanne oplysninger, jf. ovenfor, idet der tillige lægges vægt på, at videregivelsen af oplysningerne vil være nødvendig for udførelsen af opgaverne som CSIRT og centralt kontaktpunkt.

Det vurderes på den baggrund, at myndigheder og virksomheder med hjemmel i databeskyttelseslovens § 8 kan videregive oplysninger om strafbare forhold til CSIRT'en.

I relation til behandling af særlige kategorier af personoplysninger omfattet af databeskyttelsesforordningens artikel 9, henvises til bestemmelsens stk. 2, litra g, hvorefter forbuddet mod behandling af sådanne personoplysninger ikke finder anvendelse, når behandlingen er nødvendig af hensyn til væsentlige samfundsinteresser på grundlag af EU-retten eller medlemsstaternes nationale ret og står i et rimeligt forhold til det mål, der forfølges, respekterer det væsentligste indhold af retten til databeskyttelse og sikrer passende og specifikke foranstaltninger til beskyttelse af den registreredes grundlæggende rettigheder og interesser.

Henvisningen til EU-retten eller medlemsstaternes nationale ret i artikel 9, stk. 2, litra g, forudsætter, at behandlingen er forankret i f.eks. national ret, for at udgangspunktet i artikel 9, stk. 1, om forbud mod behandling kan fraviges. Forordningens artikel 9, stk. 2, litra g, stiller således krav om udfyldning i national ret og kan ikke uden videre anvendes som behandlingshjemmel. Der stilles imidlertid ikke krav om, at den nationale ret skal indeholde en udtrykkelig hjemmel til behandling af sådanne personoplysninger. Det vurderes på den baggrund at være tilstrækkeligt, at myndigheders og virksomheders videregivelse af personoplysninger er forudsat i nærværende lov, som gennemfører NIS 2-direktivet. Ministeriet for Samfundssikkerhed og Beredskab har i den forbindelse foretaget en vurdering i henhold til den tjekliste om udarbejdelse af nye nationale særregler for behandling af følsomme personoplysninger, som fremgår af betænkning nr. 1565 om databeskyttelsesforordningen.

5. Økonomiske konsekvenser og implementeringskonsekvenser for det offentlige

Efter lovforslaget vil statslige myndigheder og regionerne samt kommuner blive omfattet af lovens anvendelsesområde. Lovforslaget forventes på denne baggrund at medføre merudgifter og negative implementeringskonsekvenser til statslige og regionale myndigheder, da de – i lighed med private enheder – skal overholde lovens forpligtelser. Disse forpligtelser vil bl.a. omfatte registrerings- og underretningsforpligtelserne i lovens §§ 9, 10 og 12.

Lovforslaget stiller derudover i § 6 krav om, at enheder 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 operation eller til at levere deres tjenester. Dette vil også gælde for de myndigheder, der er omfattet af loven.

Det bemærkes, at der med lovforslagets § 6, stk. 3, lægges op til, at vedkommende minister inden for sit område efter forhandling med ministeren for samfundssikkerhed og beredskab fastsætter nærmere regler om krav til foranstaltninger efter stk. 1. Som nærmere beskrevet i lovforslagets pkt. 2.2.1. vil en sådan konkretisering i bekendtgørelse alene ske, hvis særlige sektorspecifikke hensyn tilsiger det.

Da de nærmere økonomiske konsekvenser ved foranstaltningerne til styring af cybersikkerhedsrisici vil afhænge af det nærmere indhold af eventuelle sektorspecifikke bekendtgørelser, vil de økonomiske konsekvenser heraf først kunne opgøres endeligt i forbindelse med udstedelsen af de forskellige bekendtgørelser. De økonomiske og administrative konsekvenser vil desuden afhænge af myndighedernes eksisterende sikkerhedsniveau og udviklingen i trusselsbilledet i samfundet.

Ud over konsekvenserne forbundet med, at statslige myndigheder vil være omfattet af lovforslaget, vil der være konsekvenser forbundet med løsningen af de myndighedsopgaver, der følger af direktivet.

Efter lovforslaget vil en række myndigheder i de sektorer, der fremgår af lovens bilag skulle udføre rollen som kompetente myndigheder og som følge heraf varetage opgaven med bl.a. at føre tilsyn med lovens overholdelse. Der er allerede i dag myndigheder, der varetager opgaven som kompetente myndigheder i medfør af den danske gennemførelse af NIS 1-direktivet. Med NIS 2-direktivet udvides antallet af sektorer, hvilket vil medføre, at der vil blive udpeget yderligere kompetente myndigheder, hvilket vil indebære administrative implementeringsmæssige konsekvenser. Lovforslaget forventes derfor i varierende omfang at medføre merudgifter for de ministerområder, der har ressortansvar for de sektorer, der fremgår af lovens bilag.

De statsfinansielle konsekvenser til øgede aktiviteter afstedkommet af lovforslaget estimeres med betydelig usikkerhed at udgøre ca. 105-147 mio. kr. årligt.

Derudover estimeres der med betydelig usikkerhed at være udgifter i regionerne på 63-100 mio. kr. årligt.

Der estimeres endvidere med betydelig usikkerhed at være udgifter i kommunerne på 95-280 mio. kr. årligt. Der vurderes desuden at være negative implementeringskonsekvenser.

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

Det Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at princip nr. 1 er iagttaget, idet det i lovforslaget – inden for direktivets rammer – klart fremgår, hvilke forpligtelser der påhviler omfattede enheder, og hvilke beføjelser en kompetent myndighed har i sit tilsyn med enhedernes efterlevelse af deres forpligtelser.

Det er desuden Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at lovforslaget er udarbejdet i overensstemmelse med princip nr. 2, da lovforslagets § 31 indfører hjemmel til at fastsætte regler om digital kommunikation.

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

Det bemærkes navnlig i relation til registrerings- og underretningspligterne i §§ 9, 10 og 12, at der med lovforslaget forudsættes anvendt digitale selvbetjeningsløsninger såsom Virk.dk. Dermed anvendes eksisterende offentlig it-infrastruktur til digital kommunikation mellem enhederne og myndighederne, hvilket er i overensstemmelse med princip nr. 6.

Det er Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at de øvrige principper ikke er relevante for lovforslaget.

6. Økonomiske og administrative konsekvenser for erhvervslivet mv.

Lovforslaget forventes at medføre væsentlige negative erhvervsøkonomiske konsekvenser for ca. 3.255 virksomheder i Danmark. Bl.a. vil virksomheder skulle overholde registrerings- og underretningsforpligtelserne i de foreslåede §§ 9, 10, 12 og 13 i lovforslaget.

Lovforslaget stiller derudover i § 6 krav om, at enheder 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 operation eller til at levere deres tjenester.

NIS 2-hovedloven medfører en række administrative krav for private virksomheder. Med afsæt i data fra Klima-, Energi- og Forsyningsministeriets' AMVAB-undersøgelse for bekendtgørelse om modstandsdygtighed og beredskab i

energisektoren skønnes de *administrative omkostninger* ved nærværende lovforslag med stor usikkerhed at udgøre ca. 2,8-3,3 mia. kr. i omstillingsomkostninger og ca. 0,7-1,2 mia. kr. årligt i løbende udgifter.

Ligeledes medfører lovforslaget en række øvrige efterlevelseskonsekvenser for private virksomheder. Med afsæt i Klima-, Energi- og Forsyningsministeriets erhvervsøkonomiske konsekvenser for bekendtgørelse om modstandsdygtighed og beredskab i energisektoren skønnes de *øvrige efterlevelsesomkostninger* ved nærværende lovforslag med stor usikkerhed at udgøre 1,6-2,4 mia. kr. i omstillingsomkostninger og 2,0-2,6 mia. kr. i løbende udgifter

I alt skønnes således omstillingsomkostninger for 4,4 – 5,7 mia. kr. og årlige løbende omkostninger på 2,7 – 3,8 mia. kr. *jf. tabel 1.*

Tabel 1

Kvantificering af de erhvervsøkonomiske konsekvenser[1)]

Mia. kr.	Administrative konsekvenser	Øvrige efterlevelseskonsekvenser	I alt
Omstillingsomkostninger	2,8-3,3	1,6-2,4	4,4-5,7
Løbende omkostninger	0,7-1,2	2,0-2,6	2,7-3,8

1) Kilde: Ministeriet for Samfundssikkerhed og Beredskab og Erhversstyrelsen.

Efter lovens ikrafttræden vil der blive gennemført en AMVAB-måling af de administrative konsekvenser ligesom at de øvrige efterlevelseskonsekvenser genberegnes. Det bemærkes, at der udestår en kvantificering af de samlede erhvervsøkonomiske konsekvenser for leverandører til de virksomheder, der er omfattet af loven. Disse vil indgå i målingen 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 konsekvenser for 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 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).

Det følger af artikel 41, stk. 1, i NIS 2-direktivet, at direktivet skulle være gennemført i dansk ret senest den 17. oktober 2024 og træde i kraft senest den 18. oktober 2024. Med den foreslåede bestemmelse i § 33 vil loven dermed træde i kraft den 1. juli 2025, og således lidt over ni måneder efter direktivets implementeringsfrist. Den 28. november 2024 indledte EU-Kommissionen traktatbrudssager mod 23 medlemsstater, herunder Danmark for ikke at have gennemført NIS 2-direktivet.

11. Hørte myndigheder og organisationer mv.

Et udkast til lovforslag har i perioden fra den 5. juli 2024 til den 22. august 2024 (48 dage) været sendt i høring hos følgende myndigheder og organisationer mv.:

Advokatrådet, Amnesty International, ATP, Bestyrelsesforeningen, Danish Care, Danish Cloud Community, Danish Seafood Association, Danmarks Apotekerforening, Dansk Arbejdsgiverforening, Dansk Erhverv, Dansk Industri, Dansk IT, Dansk Kollektiv Trafik, Dansk Luftfart, Dansk Selskab for Patientsikkerhed, Dansk Standard, Danske Advokater, Danske Havne, Danske Maritime, Danske Rederier, Danske Regioner, Danske Shipping- og Havnevirksomheder, Danske Universiteter, Danske Vandværker, DANVA

Dataetisk Råd, Datatilsynet, Danish e-infrastructure consortium, De Samvirkende Købmænd, Den Danske Dommerforening, Den Danske Søretsforening, Dansk Internet Forum, DJØF, DKCERT, D-mærket, Domstolsstyrelsen, Erhvervsflyvningens sammenslutning, Fagbevægelsens Hovedorganisation, Finans Danmark, Færøernes Landsstyre via Rigsombudsmanden på Færøerne, GTS-foreningen, Ingeniørforeningen i Danmark, Industriens Fond, Industriforeningen for Generiske og Biosimilære Lægemidler, Institut for Menneskerettigheder, IT-Branchen, IT-politisk forening, IT-Universitetet, Justitia, KOMBIT, Kommunale Velfærdschefer, Kommunernes Landsforening, Landbrug og Fødevarer, Lederne, Lægemiddelindustriforeningen, MEDCOM, Medicoindustrien, NORDUnet A/S, Naalakkersuisut via Rigsombudsmanden på Grønland, Pharmadanmark, Præsidenten for Vestre Landsret, Præsidenten for Østre Landsret, Punktum

dk, Retspolitisk Forening, Rådet for Digital Sikkerhed, Samtlige byretspræsidenter, SMVdanmark, Statsadvokaten i København og Statsadvokaten i Viborg.

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 estimeres med betydelig usikkerhed at udgøre ca. 105-147 mio. kr. årligt. Derudover estimeres der med betydelig usikkerhed at være udgifter i regionerne på 63-100 mio. kr. årligt. Der estimeres med usikkerhed at være udgifter i kommunerne på 95-280 mio. kr. årligt.
Implementeringskonsekvenser for stat, kommuner og regioner	Ingen.	Lovforslaget forventes at medføre negative implementeringskonsekvenser for staten, regionerne og i et vist omfang kommunerne, da de skal overholde lovens forpligtelser. Disse forpligtelser vil bl.a. omfatte registrerings- og underretningsforpligtelserne i lovens §§ 9, 10 og 12.
Økonomiske konsekvenser for erhvervslivet m.v.	Ingen.	Det er vanskeligt at estimere de erhvervsøkonomiske konsekvenser på nuværende tidspunkt. De erhvervsøkonomiske konsekvenser ved NIS 2-hovedloven er i lovforslaget med stor usikkerhed opgjort til ca. 4,4-5,7 mia. kr. i omstillingsomkostninger og ca. 2,7-3,8 mia. kr. årligt i løbende udgifter.
Administrative konsekvenser for erhvervslivet m.v.	Ingen.	Lovforslaget forventes at medføre negative implementeringskonsekvenser for erhvervslivet, da virksomheder, organisationer mv. (i det omfang de er omfattet af lovens anvendelsesområde), skal overholde lovens forpligtelser. Disse forpligtelser vil bl.a. omfatte registrerings- og underretningsforpligtelserne i lovens §§ 9, 10, 12 og 13.
Administrative konsekvenser for borgerne	Ingen.	Ingen.
Klimamæssige konsekvenser	Ingen.	Ingen.
Miljø- og naturmæssige konsekvenser	Ingen.	Ingen.
Forholdet til EU-retten	(Beskriv forholdet til EU-retten/anfør »Lovforslaget indeholder ingen EU-retlige aspekter.«)	
Er i strid med de fem principper for implementering af	Ja	Nej

erhvervsrettet EU-regulering (der i relevant omfang også gælder ved implementering af ikke-erhvervsrettet EU-regulering) (sæt X)	X

Bemærkninger til lovforslagets enkelte bestemmelser

Til § 1

Net- og informationssikkerhed var tidligere reguleret i NIS 1-direktivet. NIS 1-direktivet omfattede operatører af væsentlige tjenester og udbydere af digitale tjenester inden for sektorerne: 1) energi, 2) transport, 3) bankvæsen, 4) finansielle markedsinfrastrukturer, 5) sundhedssektoren, 6) drikkevandsforsyning og 7) digital infrastruktur.

NIS 1-direktivet er i dansk ret gennemført sektorvist i regulering under de respektive ressortministerier, hvor direktivet finder anvendelse. For en nærmere gennemgang af den sektorvise implementering af NIS 1-direktivet henvises til afsnit 2.4 i lovforslagets almindelige bemærkninger.

Det følger af det foreslåede *stk. 1,* at loven finder anvendelse på offentlige og private enheder, der er omfattet NIS 2-direktivet, jf. dog stk. 2-4 og 6.

Den foreslåede bestemmelse vil indebære, at enheder, der er omfattet af NIS 2-direktivets anvendelsesområde, vil være omfattet af lovens anvendelsesområde med de modifikationer, der følger af de foreslåede bestemmelser § 1, stk. 2-4 og 6. Bestemmelsen vil gennemføre NIS 2-direktivets artikel 2, stk. 1-4, 7 og 9.

Det følger af NIS 2-direktivets artikel 2, stk. 1, at direktivet finder anvendelse på offentlige eller private enheder af den type, der er omhandlet i direktivets bilag I eller II, som udgør mellemstore virksomheder i henhold til artikel 2 i bilaget til Europa-Kommissionens henstilling 2003/361/EF af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder, eller som overskrider tærsklerne for mellemstore virksomheder fastsat i nævnte artikels stk. 1, og som leverer deres tjenester eller udfører deres aktiviteter inden for Den Europæiske Union.

Af direktivets bilag I fremgår en oversigt over sektorer af særlig kritisk betydning, herunder en række delsektorer og typer af enheder, som indgår i de enkelte sektorer. Der henvises til lovens bilag 1. Af direktivets bilag II fremgår en oversigt over andre kritiske sektorer, herunder en række delsektorer og typer af enheder, som indgår i de enkelte sektorer. Der henvises til lovens bilag 2.

Med NIS 2-direktivet omfattes en række yderligere sektorer end dem, der var omfattet af NIS 1-direktivets regulering. Ud over de tidligere nævnte sektorer, som er omfattet af NIS 1-direktivets anvendelsesområde, er følgende sektorer således også omfattet af NIS 2-direktivet: 1) spildevand, 2) forvaltning af informations- og kommunikationstjenester (IKT-tjenester) (business-to-business), 3) offentlig forvaltning, 4) rummet, 5) post- og kurertjenester, 6) affaldshåndtering, 7) fremstilling, produktion og distribution af kemikalier, 8) produktion, tilvirkning og distribution af fødevarer, 9) forskning og 10) fremstilling med delsektorerne: a) fremstilling af medicinsk udstyr og medicinsk udstyr til vitro-diagnostik, b) fremstilling af computere og elektroniske og optiske produkter, c) fremstilling af elektrisk udstyr, d) fremstilling af maskiner og udstyr ikke andetsteds nævnt, e) fremstilling af motorkøretøjer, påhængsvogne og sættevogne og f) fremstilling af andre transportmidler.

Det fremgår af direktivets bilag II, pkt. 3, at direktivet finder anvendelse for sektoren for fremstilling, produktion og distribution af kemikalier. Af bilagets pkt. 3, at denne sektor omfatter typer af enheder, der beskæftiger sig med fremstilling af stoffer og distribution af stoffer eller blandinger som omhandlet i artikel 3, nr. 9) og 14), i Europa-Parlamentets og Rådets forordning (EF) nr. 1907/2006 (2) (REACH-forordningen) og virksomheder, der beskæftiger sig med produktion af artikler som defineret i artikel 3, nr. 3), i nævnte forordning ud af stoffer eller blandinger.

I juli 2024 offentliggjorde Kommissionen sine besvarelser af udvalgte spørgsmål stillet af medlemsstaterne i forbindelse med implementeringen af NIS 2-direktivet. Ét af de besvarede spørgsmål vedrører direktivets anvendelsesområde inden for sektoren for fremstilling, produktion og distribution af kemikalier.

Det fremgår i den forbindelse bl.a. af Kommissionens besvarelse af spørgsmålet, at ”By referring to undertakings carrying out the manufacture of substances and the distribution of substances or mixtures under the sector “manufacture, production and distribution of chemicals”, the NIS 2 Directive seems to refer to all chemical substances, regardless of whether they are potentially hazardous industrial chemicals or used in day-to-day products. ”

I forlængelse heraf fremgår af besvarelsen, at Kommissionen i forbindelse med vurderingen af medlemsstaters implementering af NIS 2-direktivet for sektoren for fremstilling, produktion og distribution af kemikalier i første omgang alene vil fokusere på enheder, der er omfattet af registreringsforpligtelsen under REACH-forordningen, som alene omfatter ”hazardous industrial chemicals”, jf. ovenfor.

Det er Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at afgrænsningen af anvendelsesområdet for sektoren for fremstilling, produktion og distribution af kemika-

lier, skal fortolkes i overensstemmelse med Kommissionens vejledende udtalelse.

NIS 2-direktivets artikel 2, stk. 1, indebærer, at enhederne som udgangspunkt mindst skal udgøre mellemstore virksomheder, som defineret i Europa-Kommissionens henstilling 2003/361/EF af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder, for at være omfattet af NIS 2-direktivet.

Det fremgår af artikel 2 i den nævnte henstilling, at kategorien mikrovirksomheder, små og mellemstore virksomheder (SMV'er) omfatter virksomheder, som beskæftiger under 250 personer, og som har en årlig omsætning på ikke over 50 mio. euro eller en årlig samlet balance på ikke over 43 mio. euro.

Efter henstillingens artikel 2, stk. 2, forstås der ved små virksomheder i kategorien SMV'er, virksomheder som beskæftiger under 50 personer, og som har en årlig omsætning eller en samlet årlig balance på ikke over 10 mio. euro.

For at falde ind under henstillingens definition af små virksomheder skal enheden således både opfylde 1) beskæftigelseskravet om under 50 ansatte og 2) den finansielle tærskel om en årlig omsætning eller en årlig balance på ikke over 10 mio. euro.

På den baggrund er det Ministeriet for Samfundssikkerhed og Beredskabs vurdering, at en enhed er omfattet af NIS 2-direktivet, hvis enheden har 50 ansatte eller derover eller en årlig omsætning og en årlig balance, der overstiger 10 mio. euro.

Den nævnte henstilling fastsætter i artiklerne 3-6, nærmere regler om typer af virksomheder, som tages i betragtning ved beregningen af antal beskæftigede og beløbsstørrelser, om data, der skal anvendes ved beregningen af antal beskæftigede og beløbsstørrelser og referenceperiode, om antal beskæftigede og om fastlæggelse af oplysninger om virksomheden.

Det følger af præambelbetragtning nr. 16 til NIS 2-direktivet, at for at undgå, at enheder, der har partnervirksomheder eller er tilknyttede virksomheder, betragtes som væsentlige eller vigtige enheder, hvor dette ville være uforholdsmæssigt, kan der tages hensyn til den grad af uafhængighed, som en enhed har i forhold til sine partnervirksomheder eller tilknyttede virksomheder, ved at henstillingens artikel 6, stk. 2, om fastlæggelse af oplysninger om virksomheden, anvendes ved vurderingen af, om en enhed er omfattet af NIS 2-direktivet eller ej.

Det fremgår endvidere af præambelbetragtningen, at der navnlig kan 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.

I overensstemmelse med principperne i den nævnte præambelbetragtning vil visse enheder efter omstændighederne, kunne anses for *ikke* at opfylde NIS 2-direktivets kriterium om 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 henstilling, hvis den pågældende enhed i betragtning af dens grad af uafhængighed ikke ville være blevet anset for at udgøre en mellemstor virksomhed eller overskride tærsklerne, hvis kun enhedens egne data var blevet taget i betragtning. Dette vil således medføre, at enheden ikke er omfattet af lovens anvendelsesområde.

Der er desuden visse typer af enheder, som vil være omfattet af direktivet uanset størrelse.

Det følger således af NIS 2-direktivets artikel 2, stk. 2, at direktivet finder anvendelse på enheder omhandlet i direktivets bilag I eller II, uanset enhedernes størrelse, hvor: a) tjenester leveres af i) udbydere af offentlige elektroniske kommunikationsnet eller af offentligt tilgængelige elektroniske kommunikationstjenester, ii) tillidstjenesteudbydere eller iii) topdomænenavneadministratorer og udbydere af domænenavnesystemer, b) enheden er den eneste udbyder i en medlemsstat af en tjeneste, der er væsentlig for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter, c) en forstyrrelse af den tjeneste, enheden leverer, vil kunne have væsentlig indvirkning på den offentlige sikkerhed eller folkesundheden, d) en forstyrrelse af den tjeneste, enheden leverer, vil kunne medføre en væsentlig systemisk risiko, navnlig for sektorer, hvor en sådan forstyrrelse kan have en grænseoverskridende virkning, e) 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 og f) enheden er en offentlig forvaltningsenhed i) under den centrale forvaltning som defineret af en medlemsstat i overensstemmelse med national ret eller ii) på regionalt plan som defineret af en medlemsstat i overensstemmelse med national ret, som efter en risikobaseret vurdering leverer tjenester, hvis forstyrrelse vil kunne have væsentlig indvirkning på kritiske samfundsmæssige eller økonomiske aktiviteter.

Vedrørende afgrænsningen af offentlig forvaltningsenhed under den centrale forvaltning som defineret af en medlemsstat i overensstemmelse med national ret, jf. den nævnte litra f, 1) ovenfor, bemærkes, at det følger af NIS 2-direktivets artikel 6, nr. 35, at en offentlig forvaltningsenhed er en enhed, der er anerkendt som sådan i en medlemsstat i overensstemmelse med national ret, med undtagelse af retsvæsenet, parlamenter og centralbanker, som a) er oprettet med henblik på at opfylde almennyttige formål og ikke har industriel eller kommerciel karakter, b) har status som juridisk person, eller ved lov er berettiget til at handle på vegne af en anden enhed med status som juridisk person, c) overvejende finansieres af staten, regionale myndigheder eller af andre offentligretlige organer, er underlagt ledelsesmæssig kontrol af disse myndigheder eller organer, eller har et administrations-, ledelses- eller tilsynsorgan, hvor mere

end halvdelen af medlemmerne udpeges af staten, regionale myndigheder eller andre offentligretlige organer og d) har beføjelse til at rette administrative eller lovgivningsmæssige afgørelser til fysiske eller juridiske personer, der påvirker deres rettigheder i forbindelse med grænseoverskridende bevægelighed for personer, varer, tjenester eller kapital.

De fire kriterier i a-d er kumulative, mens kriterie c indeholder tre alternative betingelser, hvoraf mindst én skal være opfyldt.

Det følger som nævnt ovenfor af NIS 2-direktivets artikel 2, litra f, i), at omfattet af direktivet er enheder, som er en offentlig forvaltningsenhed under den centrale forvaltning som defineret i overensstemmelse med national ret.

Offentlige forvaltningsmyndigheder under den centrale forvaltning er ikke et fast defineret begreb i dansk forvaltningsret. Det bemærkes dog, at bl.a. forvaltningsloven, offentlighedsloven, retssikkerhedsloven og ombudsmandsloven anvender begrebet "den offentlige forvaltning".

Efter disse fire tværgående forvaltningslove er det afgørende for, om lovene finder anvendelse på det pågældende organ, om organet kan karakteriseres som en forvaltningsmyndighed i organisatorisk og formel forstand. Væsentlige kriterier vil i denne forbindelse være, jf. Niels Fenger, Forvaltningsret (2018), 1. udgave, s. 113: 1) om organet er oprettet ved lov eller på privat initiativ, 2) om organet er placeret i et over-/underordnelsesforhold til en forvaltningsmyndighed, 3) om organets drift finansieres ved offentlig bevilling eller private midler og 4) om der ved lov er fastsat regler med hensyn til anvendelse af bevilgede midler.

I særlige tilfælde, hvor anvendelse af ovenstående organisatoriske kriterier giver anledning til tvivl om organets karakter som en forvaltningsmyndighed, kan der desuden tages hensyn til, om organet udøver offentligretlige funktioner. Organets eventuelle benævnelse som "råd", "institut" eller lignende vil derimod ikke være afgørende for, om det omfattes af begrebet den offentlige forvaltning og de fire love, jf. Niels Fenger, Forvaltningsret (2018), 1. udgave, s. 113.

Uden for den forvaltningsretlige definition af "den offentlige forvaltning" falder bl.a. Folketinget og visse organer med organisatorisk tilknytning til Folketinget, Rigsrevisionen, Folketingets Ombudsmand, domstolene, udenlandske myndigheder og internationale organisationer. Institutioner, foreninger og selskaber mv. oprettet på privatretligt grundlag vil ligeledes som det klare udgangspunkt ikke være omfattet af begrebet "den offentlige forvaltning". Statslige (og kommunale) institutioner, der er organiseret i selskabsform, vil heller ikke umiddelbart være en del af den offentlige forvaltning, jf. Niels Fenger, Forvaltningsret (2018), 1. udgave, s. 113 f.

Ved den centrale forvaltning forstås herefter organer på statsligt niveau, der opfylder ovenstående afgrænsninger.

Omfattet af lovens anvendelsesområde vil være enheder, som er statslige myndigheder, og som opfylder betingelserne for at blive anset som offentlige forvaltningsenheder. Dette betyder, at f.eks. departementer, styrelser og institutioner som f.eks. Udbetaling Danmark må anses som omfattet af loven. Det bemærkes i den forbindelse, at Udbetaling Danmark har organisatorisk tilknytning til Beskæftigelsesministeriet, træffer afgørelser i forhold til borgere og virksomheder, er oprettet ved lov og omfattet af forvaltningsloven.

Derimod vil en række uddannelses- og kulturinstitutioner næppe være tilstrækkeligt myndighedsudøvende til at udgøre offentlige forvaltningsenheder, jf. afgrænsningen ovenfor, idet de ikke vil opfylde kravet i NIS 2-direktivets artikel 6, nr. 35, litra c, eller er uden statslig organisatorisk placering. Heller ikke a-kasser vil være omfattet, idet de ikke er en del af den offentlige forvaltning og derfor deres virksomhed ikke er omfattet af forvaltningsloven.

Efter NIS 2-direktivets artikel 2, stk. 3, finder direktivet anvendelse på enheder uanset deres størrelse, der er identificeret som kritiske enheder i henhold til 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).

Efter NIS 2-direktivets artikel 2, stk. 4, finder direktivet anvendelse på enheder uanset deres størrelse, der leverer domænenavnsregistreringstjenester.

Det følger af NIS 2-direktivets artikel 2, stk. 7, at direktivet ikke finder anvendelse på offentlige forvaltningsenheder, der udfører deres aktiviteter inden for national sikkerhed, offentlig sikkerhed, forsvar eller retshåndhævelse, herunder forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger.

Det bemærkes, at det bl.a. fremgår af NIS 2-direktivets præambelbetragtning nr. 8, at, »udelukkelsen af offentlige forvaltningsenheder fra dette direktivs anvendelsesområde bør gælde for enheder, hvis aktiviteter hovedsagelig udføres inden for national sikkerhed, offentlig sikkerhed, forsvar eller retshåndhævelse, herunder forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger. Offentlige forvaltningsenheder, hvis aktiviteter kun er marginalt forbundet med disse områder, bør dog ikke udelukkes fra dette direktivs anvendelsesområde. Med henblik på dette direktiv anses enheder med reguleringsbeføjelser ikke for at udføre aktiviteter inden for retshåndhævelse, og de er derfor ikke på dette grundlag udelukket fra dette direktivs anvendelsesområde. Offentlige forvaltningsenheder, der er etableret i fællesskab med et tredjeland i overensstemmelse med en international aftale, er udelukket fra dette direktivs anvendelsesområde. Dette direktiv finder ikke anvendelse på medlemsstaternes diplomatiske og konsulære missioner i tredjelande eller på deres net- og informationssystemer, for så vidt sådanne systemer befinder sig i missionens lokaler eller drives for brugere i et tredjeland.«

Efter NIS 2-direktivets artikel 2, stk. 9, finder artikel 2, stk. 7 og 8, ikke anvendelse, hvor en enhed fungerer som tillidstjenesteudbyder.

Det vil efter den foreslåede bestemmelse i stk. 1 være enhedernes ansvar at vurdere, om de er omfattet af lovens anvendelsesområde, idet enheder, der er omfattet af anvendelsesområdet i artikel 2 i NIS 2-direktivet, vil være umiddelbart omfattet af lovens anvendelsesområde. Enheder vil i overensstemmelse med forvaltningslovens § 7 i fornødent omfang kunne få vejledning og bistand fra de kompetente myndigheder.

I en situation, hvor en enhed fejlagtigt måtte vurdere, at denne er eller ikke er omfattet af lovens anvendelsesområde, vil de kompetente myndigheder kunne træffe afgørelse om, hvorvidt enheden er omfattet af lovens anvendelsesområde. Det bemærkes i den forbindelse, at en kompetent myndighed i medfør af de foreslåede bestemmelser i § 21, stk. 1, nr. 6, og § 24, stk. 1, nr. 5, 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 loven eller regler udstedt i medfør af loven. Sådanne oplysninger kan eksempelvis være oplysninger, der er nødvendige for at vurdere, om forhold falder ind under loven eller regler, der er udstedt i medfør af denne lov.

Det følger af det foreslåede *stk. 2,* at loven ikke anvendelse på enheder i det omfang, de er omfattet af lov om styrket beredskab i energisektoren. Loven finder ikke anvendelse på enheder i det omfang, de er omfattet af lov om sikkerhed og beredskab i telesektoren, jf. dog § 1, stk. 2, i denne lov. Loven finder endvidere ikke anvendelse for enheder, der er udpeget i medfør af § 333, stk. 1, i lov om finansiel virksomhed.

I det omfang kommuner og regioner måtte udbyde offentlige elektroniske kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester, vil de imidlertid være omfattet af nærværende lov, uanset at sådanne udbydere i øvrigt er omfattet af det samtidigt fremsatte forslag til lov om sikkerhed og beredskab i telesektoren.

Det følger af det foreslåede *stk. 3,* at loven ikke finder anvendelse på enheder, hvor sektorspecifikke EU-retsakter og eventuel national gennemførelse heraf har mindst samme virkning som bestemmelserne i §§ 6, 12, 13 og 15.

Bestemmelsen vil gennemføre NIS 2-direktivets artikel 4, stk. 1, hvoraf det følger, at i tilfælde, hvor sektorspecifikke EU-retsakter kræver, at væsentlige eller vigtige enheder træffer foranstaltninger til styring af cybersikkerhedsrisici eller underretter om væsentlige hændelser, og hvor disse krav har en virkning, der mindst svarer til de forpligtelser, der er fastsat i NIS 2- direktivet, finder de relevante bestemmelser i direktivet, herunder bestemmelserne om tilsyn og håndhævelse, der er fastsat i direktivets kapitel VII, ikke anvendelse på sådanne enheder. I tilfælde, hvor sektorspecifikke EU-retsakter ikke omfatter alle enheder i en specifik sektor, der er omfattet af direktivets anvendelsesområde, finder de relevante bestemmelser i direktivet fortsat anvendelse på de enheder, der ikke er omfattet af de nævnte sektorspecifikke EU-retsakter.

I overensstemmelse med direktivets artikel 4, stk. 2, vil der under vurderingen af, om sektorspecifikke EU-retsakter og eventuel national gennemførelse heraf har mindst samme virkning som bestemmelserne i §§ 6, 12, 13 og 15, skulle lægges vægt på om a) foranstaltningerne til styring af cybersikkerhedsrisici har mindst samme virkning som dem, der er fastsat i direktivets artikel 21, stk. 1 og 2, eller b) den sektorspecifikke EU-retsakt giver CSIRT'erne, de kompetente myndigheder eller de centrale kontaktpunkter i henhold til NIS 2-direktivet øjeblikkelig, hvor relevant automatisk og direkte, adgang til underretninger om hændelser, og hvor kravene om at give underretning om væsentlige hændelser mindst har samme virkning som kravene fastsat i direktivets artikel 23, stk. 1-6.

Det bemærkes, at Europa-Kommissionen ved meddelelse af 18. september 2023 har fastsat nærmere retningslinjer for anvendelsen af artikel 4, stk. 1 og 2, i NIS 2-direktivet. Der henvises til EU-tidende 2023, L nr. 328, side 2. Anvendelse af den foreslåede bestemmelse forudsættes at ske i overensstemmelse med disse retningslinjer.

I tilfælde, hvor en enhed indgår i flere sektorer i lovens bilag, og det alene er den ene sektor, hvor der er udstedt sektorspecifikke EU-retsakter, og den nationale gennemførelse heraf har mindst samme virkning som bestemmelserne i §§ 6, 12, 13 og 15, vil enhedens aktiviteter i de øvrige sektorer ikke kunne undtages fra denne lovs bestemmelser.

Det følger af det foreslåede *stk. 4,* at vedkommende minister inden for sit område kan træffe afgørelse om at undtage specifikke enheder, såfremt enhederne udfører aktiviteter inden for national sikkerhed, offentlig sikkerhed, forsvar eller retshåndhævelse, herunder forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger, eller som udelukkende leverer tjenester til offentlige forvaltningsenheder, der udfører disse aktiviteter, fra forpligtelserne i §§ 6, 8, 12, 13, 15 og 16 for så vidt angår disse aktiviteter eller tjenester. Hvis enhederne udelukkende udfører aktiviteter eller leverer tjenester af den type, der er omhandlet i dette stykke, kan vedkommende minister endvidere træffe afgørelse om at fritage disse enheder for forpligtelserne i medfør af §§ 9 og 10.

Den foreslåede bestemmelse vil gennemføre NIS 2-direktivets artikel 2, stk. 8, som fastsætter, at medlemsstaterne kan undtage specifikke enheder, der udfører aktiviteter inden for national sikkerhed, offentlig sikkerhed, forsvar eller retshåndhævelse, herunder forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger, eller som udelukkende leverer tjenester til de offentlige forvaltningsenheder, der er omhandlet i artikel 2, stk. 7, fra forpligtelserne i artikel 21 (foranstaltninger til styring af cybersikkerheden) eller 23 (rapporteringsforpligtelser) for så vidt angår

disse aktiviteter eller tjenester. I så fald finder de i direktivets kapitel VII omhandlede tilsyns- og håndhævelsesforanstaltninger ikke anvendelse i forbindelse med disse specifikke aktiviteter eller tjenester. Hvor enhederne udelukkende udfører aktiviteter eller leverer tjenester af den type, der er omhandlet i dette stykke, kan medlemsstater beslutte også at fritage disse enheder for forpligtelserne i artikel 3 og 27 (registreringsforpligtelser).

Efter bestemmelsen vil specifikke enheder, der udfører aktiviteter inden for national sikkerhed, offentlig sikkerhed, forsvar eller retshåndhævelse, herunder forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger, kunne undtages fra forpligtelserne i de foreslåede § 6 (foranstaltninger til styring af cybersikkerheden) og § 8, 12, 13, 15 og 16 (oplysnings- og underretningspligter).

Bestemmelsen tager sigte på enheder, der ikke allerede er udelukket fra lovens anvendelsesområde, jf. den foreslåede bestemmelse i § 1, stk. 1, jf. NIS 2-direktivets artikel 2, stk. 7, som undtager offentlige forvaltningsenheder, der udfører aktiviteter inden for national sikkerhed, offentlig sikkerhed, forsvar eller retshåndhævelse, herunder forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger. Der vil således typisk være tale om private virksomheder, der selvstændigt udfører aktiviteter inden for national sikkerhed, offentlig sikkerhed, forsvar eller retshåndhævelse. I Danmark er der ikke generelt tradition for, at private virksomheder selvstændigt udfører aktiviteter inden for national sikkerhed mv., og derfor vil 1. pkt. i praksis have et begrænset anvendelsesområde.

Bestemmelsen vil også omfatte enheder, der udelukkende leverer tjenester til offentlige forvaltningsenheder, som udfører aktiviteter inden for national sikkerhed, offentlig sikkerhed, forsvar eller retshåndhævelse, herunder forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger, der derfor vil kunne undtages fra forpligtelserne i §§ 6 (foranstaltninger til styring af cybersikkerheden) og §§ 8, 12, 13, 15 og 16 (oplysnings- og underretningspligter).

At en enhed »udelukkende leverer tjenester« til forvaltningsenheder, der udfører ovenfor nævnte aktiviteter, indebærer i overensstemmelse med præambelbetragtning nr. 9, at tjenester, som enheden leverer, eksklusivt skal leveres til offentlige forvaltningsenheder, der udfører disse aktiviteter. Såfremt en enhed både leverer tjenester til offentlige forvaltningsenheder, der udfører de nævnte aktiviteter, og til andre aktører, eksempelvis private virksomheder eller offentlige forvaltningsenheder, der ikke udfører aktiviteter inden for national sikkerhed, offentlig sikkerhed, forsvar eller retshåndhævelse, herunder forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger, vil enheden således ikke kunne undtages fra forpligtelserne i §§ 6, 8, 12, 13, 15 og 16 for så vidt angår disse tjenester.

Efter bestemmelsen vil vedkommende minister endvidere kunne træffe afgørelse om at undtage en specifik enhed fra registreringsforpligtelserne i de foreslåede §§ 9 og 10, såfremt enheden alene udfører aktiviteter inden for national sikkerhed, offentlig sikkerhed, forsvar eller retshåndhævelse, herunder forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger, eller som udelukkende leverer tjenester til offentlige forvaltningsenheder, der udfører de ovenfor nævnte aktiviteter.

Det forudsættes, at de relevante kompetente myndigheder og CSIRT'en underrettes om en ministers afgørelse om at undtage en specifik enhed i medfør af den foreslåede bestemmelse.

Det følger af det foreslåede *stk. 5,* at der ikke kan fastsættes regler efter stk. 4, hvor en enhed fungerer som tillidstjenesteudbyder.

Den foreslåede bestemmelse vil gennemføre NIS 2-direktivets artikel 2, stk. 9. Den foreslåede bestemmelse svarer indholdsmæssigt til NIS 2-direktivets artikel 2, stk. 9, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Ved en tillidstjenesteudbyder forstås en fysisk eller juridisk person, der udbyder en eller flere tillidstjenester, som enten en kvalificeret eller ikkekvalificeret tillidstjenesteudbyder, jf. 3, nr. 19 i Europa-Parlamentets og Rådets forordning (eu) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF.

Det følger af det foreslåede *stk. 6,* at vedkommende minister efter forhandling med ministeren for samfundssikkerhed og beredskab kan fastsætte regler om, at loven helt eller delvist også finder anvendelse på henholdsvis offentlige forvaltningsenheder på lokalt plan og uddannelsesinstitutioner.

Bestemmelsen skal læses i lyset af NIS 2-direktivets artikel 2, stk. 5, hvorefter medlemsstaterne kan fastsætte, at direktivet finder anvendelse på: a) forvaltningsenheder på lokalt plan og b) uddannelsesinstitutioner, navnlig hvor de udfører kritiske forskningsaktiviteter.

Det er Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at forvaltningsenheder på lokalt plan i Danmark hovedsageligt skal forstås som kommuner og lokale folkekirkelige myndigheder, dvs. menighedsråd og provstiudvalg.

For så vidt angår uddannelsesinstitutioner forventes det primært at være aktuelt at sætte reglerne i kraft for universiteter omfattet af universitetsloven, jf. lovbekendtgørelse 391 af 10. april 2024, bl.a. henset til universiteternes udførelse af kritiske forskningsaktiviteter. Det kan dog ikke udelukkes, at loven også vil blive sat i kraft for andre videregående uddannelsesinstitutioner, bl.a. hvis disse vurderes at udføre kritiske forskningsaktiviteter.

Det bemærkes, at en offentlig forvaltningsenhed på lokalt plan eller en uddannelsesinstitution efter omstændighederne kan være omfattet af lovens anvendelsesområde, selvom bemyndigelsen i det foreslåede stk. 6 ikke er udnyttet. Dette

vil eksempelvis være tilfældet i en situation, hvor en kommune agerer som sundhedstjenesteyder i overensstemmelse med lovens bilag 1 eller 2. I denne situation vil kommunen være omfattet af lovens anvendelsesområde på baggrund af disse aktiviteter, også selvom bemyndigelsen i det foreslåede stk. 6 ikke er udnyttet. I sådanne tilfælde vil eksempelvis en kommune og en uddannelsesinstitution som en helhed være omfattet af lovens krav. Der henvises i den forbindelse til lovforslagets pkt. 3.1.3, hvoraf det bl.a. fremgår, at i tilfælde, hvor en enhed leverer flere forskellige typer af net- og informationssystemer, og hvor kun nogle af disse systemer er omfattet af lovens bilag, vil samtlige af de net- og informationssystemer, som enheden anvender til sine operationer, eller til at levere sine tjenester, blive underlagt direktivets krav.

Den foreslåede bestemmelse i stk. 6 vil således alene være relevant, hvis man måtte ønske at omfatte offentlige forvaltningsenheder på lokalt plan eller uddannelsesinstitutioner, der ikke allerede er omfattet af direktivets anvendelsesområde.

For at sikre ensartethed blandt sektorerne, er det Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at sådanne regler bør fastsættes efter forhandling med ministeren for samfundssikkerhed og beredskab.

Der henvises i øvrigt til lovforslagets pkt. 3.1.

Til § 2

Det følger af artikel 18, stk. 1, i NIS 1-direktivet at en udbyder af digitale tjenester anses for at høre under den medlemsstats jurisdiktion, hvor den har sit hjemsted. En udbyder af digitale tjenester anses for at have sit hjemsted i en medlemsstat, hvis dens hovedkontor er placeret i den pågældende medlemsstat. Det følger endvidere af artikel 18, stk. 2, at en udbyder af digitale tjenester, som ikke er etableret i Unionen, men som tilbyder tjenester som omhandlet i direktivets bilag I eller II i Unionen, udpeger en repræsentant i Unionen. Repræsentanten skal være etableret i en af de medlemsstater, hvor tjenesterne tilbydes. En udbyder af digitale tjenester anses for at høre under den medlemsstats jurisdiktion, hvor repræsentanten er etableret.

NIS 1-direktivet blev gennemført sektorvist i dansk ret gennem regulering gældende for de specifikke sektorer, hvor direktivet finder anvendelse. For en nærmere gennemgang af den sektorvise implementering af NIS 1-direktivet, henvises til afsnit 2.4 i lovforslagets almindelige bemærkninger.

Det følger af den foreslåede *stk. 1,* at under dansk jurisdiktion hører enheder, der er omfattet af lovens anvendelsesområde, og som er etableret i Danmark, jf. dog stk. 2.

Bestemmelsen vil delvist gennemføre artikel 26, stk. 1, i NIS 2-direktivet. Det fremgår heraf, at enheder, der er omfattet af direktivets anvendelsesområde, anses for at henhøre under jurisdiktionen i den medlemsstat, hvor de er etableret.

Den foreslåede bestemmelse svarer indholdsmæssigt til dele af NIS 2-direktivets artikel 26, stk. 1, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Den foreslåede bestemmelse indeholder to kumulative betingelser for, at en enhed hører under dansk jurisdiktion: 1) enheden skal være omfattet af lovens anvendelsesområde, og 2) enheden skal være etableret i Danmark. Dette udgangspunkt er dog modificeret i det foreslåede stk. 2, jf. nedenfor.

Det bemærkes, at det fremgår af NIS 2-direktivets præambelbetragtning nr. 113, at hvis enheden leverer tjenester eller er etableret i mere end én medlemsstat, bør den henhøre under hver af disse medlemsstaters særskilte og parallelle jurisdiktion.

Efter samme præambelbetragtning hører offentlige forvaltningsenheder under jurisdiktionen i den medlemsstat, der har oprettet dem.

Det følger af det foreslåede *stk. 2,* at DNS-tjenesteudbydere, topdomænenavneadministratorer, enheder, der leverer domænenavnsregistreringstjenester, og udbydere af henholdsvis cloudcomputingtjenester, datacentertjenester, indholdsleveringsnetværk, administrerede tjenester, administrerede sikkerhedstjenester, onlinemarkedspladser, onlinesøgemaskiner og platforme for sociale netværkstjenester, der har deres hovedforretningssted i Danmark, jf. stk. 3, hører under dansk jurisdiktion.

Bestemmelsen vil gennemføre NIS 2-direktivets artikel 26, stk. 1, litra b, som bl.a. fastsætter, at DNS-tjenesteudbydere, topdomænenavneadministratorer, enheder, der leverer domænenavnsregistreringstjenester, og udbydere af cloudcomputingtjenester, af datacentertjenester, af indholdsleveringsnetværk, af administrerede tjenester, af administrerede sikkerhedstjenester, af onlinemarkedspladser, af onlinesøgemaskiner eller af platforme for sociale netværkstjenester anses for at henhøre under jurisdiktionen i den medlemsstat, hvor de har deres hovedforretningssted i Unionen.

Den foreslåede bestemmelse svarer indholdsmæssigt til NIS 2-direktivets artikel 26, stk. 1, litra b, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

For så vidt angår fastlæggelsen af en enheds hovedforretningssted, henvises der til bemærkningerne til det foreslåede stk. 3.

Det følger af det foreslåede *stk. 3,* at en enhed omfattet af stk. 2 anses for at have sit hovedforretningssted i Den Europæiske Union i den medlemsstat, hvor beslutningerne vedrørende foranstaltningerne til styring af cybersikkerhedsrisici overvejende træffes. Hvis en sådan medlemsstat ikke kan fastslås, eller hvis sådanne beslutninger ikke træffes i Den Europæiske Union, anses hovedforretningsstedet for at være i den medlemsstat, hvor der udføres cybersikkerhedsoperationer. Hvis en sådan medlemsstat ikke kan fastslås, anses hovedforretningsstedet for at være i den medlemsstat,

hvor den pågældende enheds forretningssted med det største antal ansatte i Den Europæiske Union er beliggende.

Bestemmelsen vil gennemføre NIS 2-direktivets artikel 26, stk. 2, hvorefter enheder, der er omhandlet i stk. 1, litra b, anses for at have deres hovedforretningssted i Den Europæiske Union i den medlemsstat, hvor beslutningerne vedrørende foranstaltningerne til styring af cybersikkerhedsrisici overvejende træffes. Hvis en sådan medlemsstat ikke kan fastslås, eller hvis sådanne beslutninger ikke træffes i Unionen, anses hovedforretningsstedet for at være i den medlemsstat, hvor der udføres cybersikkerhedsoperationer. Såfremt en sådan medlemsstat ikke kan fastslås, anses hovedforretningsstedet for at være i den medlemsstat, hvor den pågældende enheds forretningssted med det største antal ansatte i Unionen er beliggende.

Den foreslåede bestemmelse svarer med sproglige tilpasninger uden indholdsmæssig betydning til NIS 2-direktivets artikel 26, stk. 2, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Det fremgår af NIS 2-direktivets præambelbetragtning nr. 114, at for at tage hensyn til den grænseoverskridende karakter af de tjenester og operationer, der henholdsvis leveres og udføres af DNS-tjenesteudbydere, topdomænenavneadministratorer, enheder, der leverer domænenavnsregistreringstjenester, og udbydere af cloudcomputingtjenester, af datacentertjenester, af indholdsleveringsnetværk, af administrerede tjenester, af administrerede sikkerhedstjenester, af onlinemarkedspladser, af onlinesøgemaskiner og af platforme for sociale netværkstjenester, bør kun én medlemsstat have jurisdiktion over disse enheder. Det fremgår endvidere, at jurisdiktionen bør tillægges den medlemsstat, hvor den pågældende enhed har sit hovedforretningssted i Unionen.

For så vidt angår forretningsstedskriteriet indebærer dette ifølge præambelbetragtning 114 en faktisk udøvelse af virksomhed gennem faste ordninger. De pågældende ordningers juridiske form, herunder hvorvidt der er tale om en filial eller et datterselskab med status som juridisk person, er i den forbindelse ikke den afgørende faktor. Det fremgår endvidere af præambelbetragtningen, at det nævnte kriterium ikke bør afhænge af, om net- og informationssystemerne fysisk befinder sig på et givent sted. Tilstedeværelsen og anvendelsen af sådanne systemer udgør ikke i sig selv et sådant hovedforretningssted og er derfor ikke afgørende for fastlæggelsen af samme. Hovedforretningsstedet bør ifølge præambelbetragtningen anses som værende i den medlemsstat, hvor beslutningerne vedrørende foranstaltninger til styring af cybersikkerhedsrisici overvejende træffes i Unionen. Det vil typisk være det sted, hvor enhedernes centrale administration i Unionen er placeret. Hvis en sådan medlemsstat ikke kan fastslås, eller hvis sådanne beslutninger ikke træffes i Unionen, bør hovedforretningsstedet anses for at være i den medlemsstat, hvor der udføres cybersikkerhedsoperationer. Hvis en sådan medlemsstat ikke kan fastslås, bør hovedforretningsstedet anses for at være i den medlemsstat, hvor enhedens forretningssted med det største antal ansatte i Unionen er beliggende. Hvor tjenesterne udføres af en gruppe af virksomheder, bør den kontrollerende virksomheds hovedforretningssted anses for at være hele gruppens hovedforretningssted.

Den foreslåede bestemmelse svarer med sproglige tilpasninger uden indholdsmæssig betydning til NIS 2-direktivets artikel 26, stk. 2, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Det følger af det foreslåede *stk. 4,* at er en enhed som nævnt i stk. 2 ikke etableret i Den Europæiske Union, men udbyder tjenester inden for Unionen, herunder i Danmark skal enheden udpege en repræsentant, der er etableret i en af de medlemsstater i Unionen, hvor enhedens tjenester udbydes. Er repræsentanten etableret i Danmark, hører enheden under dansk jurisdiktion. Er der ikke er udpeget en repræsentant efter 1. pkt., anses enheden for at høre under jurisdiktionen i de medlemsstater, hvor tjenesterne udbydes.

Bestemmelsen vil gennemføre NIS 2-direktivets artikel 26, stk. 3, hvoraf det følger, at en enhed som omhandlet i stk. 1, litra b, som ikke er etableret i Unionen, men som udbyder tjenester inden for Unionen, skal udpege en repræsentant i Unionen. Repræsentanten skal være etableret i en af de medlemsstater, hvor tjenesterne tilbydes. Enheden vil skulle anses for at høre under den medlemsstats jurisdiktion, hvor repræsentanten er etableret. Hvis der ikke er udpeget en repræsentant i Unionen, kan enhver medlemsstat, hvor enheden leverer tjenester, tage retlige skridt mod enheden for overtrædelse af dette direktiv.

Den foreslåede bestemmelse svarer indholdsmæssigt til dele af NIS 2-direktivets artikel 26, stk. 3, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Udpegelsen af en repræsentant sikrer, at enheden kun omfattes af NIS 2-reguleringen i én medlemsstat, herunder at det kun vil være én medlemsstats kompetente myndigheder, der fører tilsyn med efterlevelsen af kravene og håndhæver manglende overholdelse heraf.

I overensstemmelse med NIS 2-direktivets artikel 26, stk. 4, vil det forhold, at en enhed har udpeget en repræsentant, ikke forhindre, at der kan tages retlige skridt mod enheden selv.

Til § 3

Den foreslåede bestemmelse i *§ 3* indeholder definitioner af lovens centrale begreber.

Definitionerne bygger på de relevante tilsvarende definitioner i artikel 6 og det definitoriske indhold i artikel 8, stk. 4, i NIS 2-direktivet.

Den foreslåede bestemmelse i § 3 svarer indholdsmæssigt til de relevante dele af NIS 2-direktivets artikel 6 og artikel 8, stk. 2 og 4, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Det foreslås i *nr. 1,* at »centralt kontaktpunkt« defineres som den myndighed, der udøver forbindelsesfunktionen for at sikre grænseoverskridende samarbejde mellem de danske myndigheder, myndigheder i andre medlemsstater i Den Europæiske Union og Den Europæiske Unions institutioner, samt for at sikre tværsektorielt samarbejde mellem de nationale kompetente myndigheder.

Definitionen af det centrale kontaktpunkt bygger på beskrivelsen heraf i NIS 2-direktivets artikel 8, stk. 4. Det henvises i øvrigt til afsnit 2.2.2 i lovforslagets almindelige bemærkninger om nationale myndigheder og samarbejde.

Det foreslås i *nr. 2,* at »cloudcomputingtjeneste« defineres som en digital tjeneste, som muliggør on demand-administration og giver bred fjernadgang til en skalerbar og fleksibel pulje af delbare computerressourcer, herunder hvor disse ressourcer er fordelt mellem flere lokaliteter.

Den foreslåede bestemmelse svarer til definitionen i NIS 2-direktivets artikel 6, nr. 30, med en mindre, rent sproglig justering. Det forudsættes, at bestemmelsen fortolkes i overensstemmelse med direktivets definition.

Det foreslås i *nr. 3,* at »cybersikkerhed« defineres som de aktiviteter, der er nødvendige for at beskytte net- og informationssystemer, brugerne af sådanne systemer og andre personer berørt af cybertrusler.

Efter NIS 2-direktivets artikel 6, nr. 3, skal cybersikkerhed forstås på samme måde som definitionen i artikel 2, nr. 1, 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 i *nr. 4,* at »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 i *nr. 5,* at »datacentertjeneste« defineres som en tjeneste, der omfatter strukturer eller grupper af strukturer, som er beregnet til central opbevaring, sammenkobling og drift af it- og netværksudstyr, der leverer datalagrings-, databehandlings- og datatransporttjenester, samt alle faciliteter og infrastrukturer til energidistribution og miljøkontrol.

Den foreslåede bestemmelse svarer til definitionen i NIS 2-direktivets artikel 6, nr. 31. Det forudsættes, at bestemmelsen fortolkes i overensstemmelse med direktivets definition.

Det foreslås i *nr. 6,* at »digital tjeneste« defineres som enhver tjeneste i informationssamfundet, dvs. enhver tjeneste, der normalt ydes mod betaling, og som teleformidles ad elektronisk vej på individuel anmodning fra en tjenestemodtager.

Efter NIS 2-direktivets artikel 6, nr. 23, skal digital tjeneste forstås på samme måde som definitionen i artikel 1, stk. 1, litra b, Europa-Parlamentets og Rådets direktiv (EU) 2015/1535 af 9. september 2015 om en informationsprocedure med hensyn til tekniske forskrifter samt forskrifter for informationssamfundets tjenester.

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

Det foreslås i *nr. 7,* at »DNS-tjenesteudbyder« defineres som en enhed, der leverer: a) Offentligt tilgængelige rekursive domænenavnsoversættelsestjenester til internetslutbrugere, eller b) autoritative domænenavnsoversættelsestjenester til tredjepartsbrug, med undtagelse af rodnavneservere.

Den foreslåede bestemmelse svarer til definitionen i NIS 2-direktivets artikel 6, nr. 20. Det forudsættes, at bestemmelsen fortolkes i overensstemmelse med direktivets definition.

Det foreslås i *nr. 8,* at »domænenavnesystem« eller »DNS« defineres som et hierarkisk distribueret navngivningssystem, der gør det muligt at identificere internettjenester og -ressourcer, således at slutbrugerudstyr kan benytte internetrouting- og konnektivitetstjenester til at nå disse tjenester og ressourcer.

Den foreslåede bestemmelse svarer til definitionen i NIS 2-direktivets artikel 6, nr. 19. Det forudsættes, at bestemmelsen fortolkes i overensstemmelse direktivets definition.

Det foreslås i *nr. 9,* at »enhed« defineres som en fysisk eller juridisk person, der er oprettet og anerkendt som sådan i henhold til den nationale ret på det sted, hvor den er etableret, og som i eget navn kan udøve rettigheder og være underlagt forpligtelser.

Den foreslåede bestemmelse svarer til definitionen i NIS 2-direktivets artikel 6, nr. 38. Det forudsættes, at bestemmelsen fortolkes i overensstemmelse med direktivets definition.

Det foreslås i *nr. 10,* at »enhed, der leverer domænenavnsregistreringstjenester« defineres som en registrator eller en

agent, der handler på vegne af registratorer, såsom en udbyder eller videresælger af privatlivs- eller proxyregistreringstjenester.

Den foreslåede bestemmelse svarer til definitionen i NIS 2-dirketivets artikel 6, nr. 22. Det forudsættes, at bestemmelsen fortolkes i overensstemmelse direktivets definition.

Det foreslås i *nr. 11,* at »forskningsorganisation« defineres som en enhed, hvis primære mål er at udføre anvendt forskning eller udvikling med henblik på at udnytte resultaterne af denne forskning til kommercielle formål. Indbefatter ikke uddannelsesinstitutioner.

Den foreslåede bestemmelse svarer til definitionen i NIS 2-direktivets artikel 6, nr. 41. Den foreslåede bestemmelse indeholder dog en mindre, rent sproglig justering ift. direktivets definition. Det forudsættes, at bestemmelsen fortolkes i overensstemmelse med direktivets definition.

Det bemærkes, at det af NIS 2-direktivets præambelbetragtning nr. 36 fremgår, at begrebet forskningsorganisationer bør forstås som »omfattende enheder, der primært beskæftiger sig med anvendt forskning eller udvikling i den i Organisationen for Økonomisk Samarbejde og Udviklings Frascatimanual fra 2015 (Guidelines for Collecting and Reporting Data and Research and Experimental Development) anvendte betydning med henblik på at udnytte resultaterne heraf til kommercielle formål såsom fremstilling eller udvikling af et produkt eller proces, levering af en tjeneste eller markedsføringen heraf.«

Det foreslås i *nr. 12,* at »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 i *nr. 13,* at »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 i *nr. 14,* at »IKT-proces« defineres som aktiviteter, der udføres for at udforme, udvikle, levere eller vedligeholde et IKT-produkt eller en IKT-tjeneste.

Efter NIS 2-direktivets artikel 6, nr. 14, skal IKT-proces forstås på samme måde som definitionen i artikel 2, nr. 14, 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 i *nr. 15,* at »IKT-produkt« defineres som et element eller en gruppe af elementer i net- og informationssystemer.

Efter NIS 2-direktivets artikel 6, nr. 12, skal IKT-produkt forstås på samme måde som definitionen i artikel 2, nr. 12, 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 i *nr. 16,* at »IKT-tjeneste« defineres som en tjeneste, der helt eller hovedsageligt består af overførsel, lagring, indhentning eller behandling af oplysninger ved hjælp af net- og informationssystemer.

Efter NIS 2-direktivets artikel 6, nr. 13, skal IKT-tjeneste forstås på samme måde som definitionen i artikel 2, nr. 13, 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 i *nr. 17,* at »indholdsleveringsnetværk« defineres som et net af geografisk distribuerede servere med det formål at sikre høj tilgængelighed af, adgang til eller hurtig levering af digitalt indhold og digitale tjenester til internetbrugere på vegne af indholds- og tjenesteudbydere.

Den foreslåede bestemmelse svarer til definitionen i NIS 2-direktivets artikel 6, nr. 32. Det forudsættes, at bestemmelsen fortolkes i overensstemmelse med direktivets definition.

Det foreslås i *nr. 18,* at »kvalificeret tillidstjeneste« defineres som en tillidstjeneste, der opfylder de krav, der er fastsat i Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF.

Efter NIS 2-direktivets artikel 6, nr. 26, skal kvalificeret

tillidstjeneste forstås på samme måde som definitionen i artikel 3, nr. 17, i Europa-Parlamentets og Rådets forordning (EU) 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF.

Den foreslåede bestemmelse svarer til definitionen i den NIS 2-direktivets artikel 6, nr. 26. Det forudsættes, at bestemmelsen fortolkes i overensstemmelse med direktivets definition.

Det foreslås i *nr. 19,* at »kvalificeret tillidstjenesteudbyder« defineres som en tillidstjenesteudbyder, der udbyder en eller flere kvalificerede tillidstjenester og har fået tildelt status som kvalificeret tillidstjenesteudbyder af tilsynsorganet i medfør af Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF.

Efter NIS 2-direktivets artikel 6, nr. 27, skal kvalificeret tillidstjeneste forstås på samme måde som definitionen i artikel 3, nr. 20, i Europa-Parlamentets og Rådets forordning (EU) 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF.

Den foreslåede bestemmelse svarer til definitionen i NIS 2-direktivets artikel 6, nr. 27. Det forudsættes, at bestemmelsen fortolkes i overensstemmelse med direktivets definition.

Det foreslås i *nr. 20,* at »net- og informationssystem« defineres som: a) Et elektronisk kommunikationsnet, hvorved forstås transmissionssystemer, uanset om de bygger på en permanent infrastruktur eller 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, samt kabel-tv-net, uanset hvilken type information der overføres, 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. Det forudsættes, at bestemmelsen fortolkes i overensstemmelse direktivets definition.

Det foreslås i *nr. 21,* at »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. Den foreslåede bestemmelse indeholder dog en mindre, rent sproglig justering sammenlignet med direktivets definition, som har til formål at gøre bestemmelsen lettere at forstå for enheder. Det forudsættes, at bestemmelsen fortolkes i overensstemmelse med direktivets definition.

Det foreslås i *nr. 22,* at »onlinemarkedsplads« defineres som en tjenesteydelse, der gør brug af software, herunder et websted, en del af et websted eller en applikation, der drives af eller på vegne af den erhvervsdrivende, der giver forbrugere mulighed for at indgå fjernsalgsaftaler med andre erhvervsdrivende eller forbrugere.

Efter NIS 2-direktivets artikel 6, nr. 28, skal onlinemarkedsplads forstås på samme måde som definitionen i artikel 2, litra n, i Europa-Parlamentets og Rådets direktiv 2005/29/EF af 11. maj 2005 om virksomheders urimelige handelspraksis over for forbrugere på det indre marked og om ændring af Rådets direktiv 84/450/EØF og Europa-Parlamentets og Rådets direktiv 97/7/EF og 2002/65/EF og Europa-Parlamentets og Rådets forordning (EF) nr. 2006/2004 (direktivet om urimelig handelspraksis).

Det bemærkes, at direktivet er ændret ved Europa-Parlamentets og Rådets direktiv (EU) 2019/2161 af 27. november 2019 om ændring af Rådets direktiv 93/13/EØF og Europa-Parlamentets og Rådets direktiv 98/6/EF, 2005/29/EF og 2011/83/EU for så vidt angår bedre håndhævelse og modernisering af EU-reglerne om forbrugerbeskyttelse. Definitionen i artikel 2, litra n, blev i denne forbindelse ændret.

Den foreslåede bestemmelse svarer til definitionen i direktiv 2005/29/EF af 11. maj 2005 med senere ændringer. Det forudsættes, at bestemmelsen fortolkes i overensstemmelse med denne definition.

Det foreslås i *nr. 23,* at »onlinesøgemaskine« defineres som en digital tjeneste, som giver brugerne mulighed for at indtaste forespørgsler for at foretage søgninger på principielt alle websteder eller alle websteder på et bestemt sprog på grundlag af en forespørgsel om et hvilket som helst emne ved hjælp af et søgeord, en stemmesøgning, en sætning eller andet input, og som fremviser resultater i et hvilket som helst format, hvor der kan findes oplysninger om det ønskede indhold.

Efter NIS 2-direktivets artikel 6, nr. 29, skal onlinesøgemaskine forstås på samme måde som definitionen i artikel 2, nr. 5, i Europa-Parlamentets og Rådets forordning (EU) 2019/1150 af 20. juni 2019 om fremme af retfærdighed og gennemsigtighed for brugere af onlineformidlingstjenester.

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

Det foreslås i *nr. 24,* at »platform for sociale netværkstjenester« defineres som en platform, der sætter slutbrugere i stand til at komme i forbindelse med hinanden på tværs af forskellige anordninger, navnlig via chats, opslag, videoer og anbefalinger.

Den foreslåede bestemmelse svarer til definitionen i NIS 2-direktivets artikel 6, nr. 33, med en mindre, rent sproglig justering. Det forudsættes, at bestemmelsen fortolkes i overensstemmelse med direktivets definition.

Det foreslås i *nr. 25,* at en »repræsentant« defineres som en fysisk eller juridisk person, der er etableret i Den Europæiske Union, som udtrykkeligt er udpeget til at handle på vegne af en DNS-tjenesteudbyder, en topdomænenavneadministrator, en enhed, der leverer domænenavnsregistreringstjenester, eller en udbyder af cloudcomputingtjenester, af datacentertjenester, af indholdsleveringsnetværk, af administrerede tjenester, af administrerede sikkerhedstjenester, af onlinemarkedspladser, af onlinesøgemaskiner eller af platforme for sociale netværkstjenester, som ikke er etableret i Den Europæiske Union, og som kan kontaktes af en kompetent myndighed eller en CSIRT på enhedens sted for så vidt angår denne enheds forpligtelser i henhold til NIS 2-direktivet.

Den foreslåede bestemmelse svarer til definitionen i NIS 2-direktivets artikel 6, nr. 34. Det forudsættes, at bestemmelsen fortolkes i overensstemmelse med direktivets definition.

Det foreslås i *nr. 26,* at »risiko« defineres som potentialet for tab eller forstyrrelse som følge af en hændelse udtrykt som en kombination af størrelsen af et sådant tab eller en sådan forstyrrelse og sandsynligheden for, at hændelsen indtræffer.

Den foreslåede bestemmelse svarer til definitionen i NIS 2-direktivets artikel 6, nr. 9. Det forudsættes, at bestemmelsen fortolkes i overensstemmelse med direktivets definition.

Det foreslås i *nr. 27,* at »sikkerhed i net- og informationssystemer« defineres som net- og informationssystemers evne til, på et givent 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 bestemmelsen fortolkes i overensstemmelse med direktivets definition.

Det foreslås i *nr. 28,* at »sårbarhed« defineres som en svaghed, modtagelighed eller fejl ved IKT-produkter eller -tjenester, som kan udnyttes af en cybertrussel.

Den foreslåede bestemmelse svarer til definitionen i NIS 2-direktivets artikel 6, nr. 15. Det forudsættes, at bestemmelsen fortolkes i overensstemmelse med direktivets definition.

Det foreslås i *nr. 29,* at »tillidstjeneste« defineres som en elektronisk tjeneste, der normalt udføres mod betaling, og som består af: a) generering, kontrol og validering af elektroniske signaturer, elektroniske segl eller elektroniske tidsstempler eller elektroniske registrerede leveringstjenester og certifikater relateret til tjenester, b) generering, kontrol og validering af certifikater for webstedsautentifikation, eller c) bevaring af elektroniske signaturer, segl eller certifikater relateret til disse tjenester.

Efter NIS 2-direktivets artikel 6, nr. 24, skal tillidstjeneste forstås på samme måde som definitionen i artikel 3, nr. 16, i Europa-Parlamentets og Rådets forordning (EU) 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF.

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

Det foreslås i *nr. 30,* at »tillidstjenesteudbyder« defineres som en fysisk eller juridisk person, der udbyder en eller flere tillidstjenester, enten som en kvalificeret eller ikke-kvalificeret tillidstjenesteudbyder.

Efter NIS 2-direktivets artikel 6, nr. 25, skal tillidstjenesteudbyder forstås på samme måde som definitionen i artikel 3, nr. 19, i Europa-Parlamentets og Rådets forordning (EU) 910/2014 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF.

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

Det foreslås i *nr. 31,* at »topdomænenavneadministrator« defineres som en enhed, der har fået uddelegeret et specifikt topdomæne, og som er ansvarlig for at administrere topdomænet, herunder registrering af domænenavne under topdomænet og den tekniske drift af topdomænet, hvilket inkluderer driften af dets navneservere, vedligeholdelsen af dets databaser og distributionen af topdomænezonefiler til navneservere, uanset om nogen af disse operationer udføres af enheden selv eller outsources, men ikke situationer, hvor topdomænenavne kun anvendes af en administrator til eget brug.

Den foreslåede bestemmelse svarer til definitionen i NIS 2-direktivets artikel 6, nr. 21. Det forudsættes, at bestemmelsen fortolkes i overensstemmelse med NIS 2-direktivets definition.

Det foreslås i *nr. 32,* at en »udbyder af administrerede sikkerhedstjenester« defineres som en udbyder af administrerede tjenester, der udfører eller yder assistance til aktiviteter vedrørende styring af cybersikkerhedsrisici.

Den foreslåede bestemmelse svarer til definitionen i NIS 2-direktivets artikel 6, nr. 40. Det forudsættes, at bestem-

melsen fortolkes i overensstemmelse med NIS 2-direktivets definition.

Det foreslås *nr. 33,* at en »udbyder af administrerede tjenester« defineres som en enhed, der leverer tjenester i forbindelse med installation, administration, drift eller vedligeholdelse af IKT-produkter, -net, -infrastruktur, -applikationer eller andre net- og informationssystemer via assistance eller aktiv administration, der udføres enten i kundernes lokaler eller på afstand.

Den foreslåede bestemmelse svarer til definitionen i NIS 2-direktivets artikel 6, nr. 39. Det forudsættes, at bestemmelsen fortolkes i overensstemmelse med NIS 2-direktivets definition.

Det foreslås i *nr. 34,* at en »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 enheds net- og informationssystemer eller på brugerne af enhedens tjenester ved at forårsage betydelig fysisk eller ikke-fysisk skade.

Den foreslåede bestemmelse svarer til definitionen i NIS 2-direktivets artikel 6, nr. 11. Den foreslåede bestemmelse indeholder dog en mindre, rent sproglig justering ift. direktivets definition.

Den danske sprogversion af NIS 2-direktivets artikel 6, nr. 11, henviser til 'materiel eller immateriel skade'. Den engelske sprogversion af direktivet henviser dog til 'material or non-material damage'. Det er Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at 'material or non-material damage' skal forstås som en fysisk eller ikke-fysisk skade.

Det forudsættes, at bestemmelsen fortolkes i overensstemmelse med NIS 2-direktivets definition.

Til § 4

Der var i artikel 5, stk. 1, i 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) en forpligtelse for medlemsstaterne til at identificere operatører af væsentlige tjenester, der opererer på deres område for en række nærmere angivne sektorer og delsektorer.

Efter NIS 1-direktivets artikel 5, stk. 2, er en operatør af væsentlige tjenester følgende: a) en enhed der leverer en tjeneste, der er væsentlig for opretholdelsen af kritiske samfundsmæssige og/eller økonomiske aktiviteter, b) leveringen af denne tjeneste afhænger af net- og informationssystemer, og c) en hændelse ville få væsentlige forstyrrende virkninger for leveringen af den nævnte tjeneste.

NIS 1-direktivet omfatter også udbydere af digitale tjenester, som er visse udbydere af onlinemarkedspladser, onlinesøgemaskiner og cloud-computing-tjenester, jf. direktivets artikel 4, nr. 5.

NIS 1-direktivet blev i dansk ret gennemført sektorvist i regulering gældende for de specifikke sektorer, hvor direktivet finder anvendelse. For en nærmere gennemgang af den sektorvise implementering af NIS 1-direktivet henvises til afsnit 2.4 i lovforslagets almindelige bemærkninger.

Det følger af det foreslåede *stk. 1,* at enheder af en type, som er omfattet af lovens bilag 1, anses for at være væsentlige enheder, hvis 1) enheden beskæftiger mere end 250 ansatte, eller 2) har en årlig omsætning på over 50 mio. EUR og en årlig balance på over 43 mio. EUR.

Den foreslåede bestemmelse vil gennemføre artikel 3, stk. 1, litra a, i NIS 2-direktivet. Det følger af direktivets artikel 3, stk. 1, litra a, at 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, anses for at være væsentlige enheder.

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

Den foreslåede bestemmelse indeholder to kumulative betingelser for, at en enhed er en væsentlig enhed: 1) enheden skal være af en type, som er omfattet af lovens bilag 1 og 2) enheden skal beskæftige mere end 250 ansatte eller have en årlig omsætning på over 50 mio. EUR og en årlig balance på over 43 mio. EUR..

De foreslåede størrelseskriterier udgør definitionen af store virksomheder i henhold til 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.

Den nævnte henstilling fastsætter i artiklerne 3-6, nærmere regler om typer af virksomheder, som tages i betragtning ved beregningen af antal beskæftigede og beløbsstørrelser, om data, der skal anvendes ved beregningen af antal beskæftigede og beløbsstørrelser og referenceperiode, om antal beskæftigede og om fastlæggelse af oplysninger om virksomheden.

Det følger af præambelbetragtning nr. 16 til NIS 2-direktivet, at for at undgå, at enheder, der har partnervirksomheder eller er tilknyttede virksomheder, betragtes som væsentlige eller vigtige enheder, hvor dette ville være uforholdsmæssigt, kan der tages hensyn til den grad af uafhængighed, som en enhed har i forhold til sine partnervirksomheder eller tilknyttede virksomheder, ved at henstillingens artikel 6, stk. 2, om fastlæggelse af oplysninger om virksomheden, anvendes ved vurderingen af, om en enhed er omfattet af NIS 2-direktivet eller ej.

Det fremgår videre af præambelbetragtningen, at der navnlig

kan 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.

I overensstemmelse med principperne i den nævnte præambelbetragtning vil visse enheder efter omstændighederne, kunne anses for *ikke* at opfylde NIS 2-direktivets kriterium om 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 henstilling, hvis den pågældende enhed i betragtning af dens grad af uafhængighed ikke ville være blevet anset for at udgøre en mellemstor virksomhed eller overskride tærsklerne, hvis kun enhedens egne data var blevet taget i betragtning. Dette vil således medføre, at enheden ikke er omfattet af lovens anvendelsesområde.

Af artikel 2 i den nævnte henstilling fremgår de nærmere definitioner i forhold til antal beskæftigede og finansielle tærskler ved afgrænsning af forskellige virksomhedskategorier. Det følger således af henstillingens artikel 2, stk. 1, at kategorien mikrovirksomheder, små og mellemstore virksomheder (SMV'er) omfatter virksomheder, som beskæftiger under 250 personer, og som har en årlig omsætning på ikke over 50 mio. euro eller en årlig samlet balance på ikke over 43 mio. euro.

Det er Ministeriet for Samfundssikkerhed og Beredskabs vurdering, at enhed vil skulle beskæftige 250 personer eller derover eller have en årlig omsætning på over 50 mio. EUR og en årlig balance, der overstiger 43 mio. euro, for at kunne anses for væsentlig i henhold til NIS 2-direktivets artikel 3, stk. 1 og den foreslåede bestemmelse i § 4, stk. 1.

Det følger af det foreslåede *stk. 2,* at i kommuner og regioner anses som væsentlige enheder, såfremt de med et kommercielt formål udfører opgaver som udbydere af offentlige elektroniske kommunikationsnet eller udbydere af offentligt tilgængelige elektroniske kommunikationstjenester, og 1) beskæftiger mere end 50 personer, eller 2) har en årlig omsætning på over 10 mio. EUR og en årlig samlet balance på over 10 mio. EUR.

En kommune eller region vil således skulle beskæftige over 50 personer men under 250 personer og have en årlig omsætning på over 10 mio. euro, men ikke over 50 mio. euro eller have en årlig samlet balance på over 10 mio. euro, men ikke over 43 mio. euro for at kunne anses for væsentlig i henhold til NIS 2-direktivets artikel 3, stk. 1, litra c, og den foreslåede bestemmelse i § 4, stk. 2.

I tilfælde hvor en kommune eller region måtte overskride tærsklerne for at være en mellemstor virksomhed, vil enheden være at betragte som en væsentlig enhed i medfør af den foreslåede bestemmelse i § 4, stk. 1.

Bestemmelsen skal ses i lyset af, at der for henholdsvis kommuner og regioner forventes at blive fastsat tværgående regler. På den baggrund vil det efter Ministeriet for Samfundssikkerhed og Beredskabs opfattelse være uhensigtsmæssigt, såfremt kommuner og regioner, der måtte udføre opgaver som udbydere af offentlige elektroniske kommunikationsnet eller udbydere af offentligt tilgængelige elektroniske kommunikationstjenester omfattes af det samtidig fremsatte forslag til lov om sikkerhed og beredskab i telesektoren. Det er dog samtidig Ministeriet for Samfundssikkerhed og Beredskabs vurdering, at der for kommuner og regioner som udbyder offentlige elektroniske kommunikationsnet eller udbydere af offentligt tilgængelige elektroniske kommunikationstjenester, samt teleudbydere, der er omfattet af forslag til lov om sikkerhed og beredskab i telesektoren, bør fastsættes samme definition. For at sikre overensstemmelse mellem definitionerne af teleudbydere denne lov og lov om sikkerhed og beredskab i telesektoren, er det Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at kommuner og regioner som udbyder offentlige elektroniske kommunikationsnet eller udbydere af offentligt tilgængelige elektroniske kommunikationstjenester alene skal omfattes af reguleringen af nærværende lov, hvis de i øvrigt opfylder kriterierne for at være omfattet af lov om sikkerhed og beredskab i telesektoren.

Det følger af bemærkningerne til forslag til lov om sikkerhed og beredskab i telesektoren, pkt. 3.1.3, at 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. "

Det følger i forlængelse heraf af bemærkningerne til forslag til lov om sikkerhed og beredskab i telesektoren, pkt. 3.1.3, at "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. "

På denne baggrund er det Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at kommuner og regioner, som udfører opgaver som udbydere af offentlige elektroniske kommunikationsnet eller udbydere af offentligt tilgængelige elektroniske kommunikationstjenester, alene vil være omfattet af denne lov, hvis udbuddet sker med et kommercielt formål.

I overensstemmelse med NIS 2-direktivets artikel 6, nr. 36, skal »offentligt elektronisk kommunikationsnet« forstås på samme måde som i artikel 2, nr. 8, i direktiv (EU) 2018/1972. Ved offentligt elektronisk kommunikationsnet

forstås således 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.

I overensstemmelse med NIS 2-direktivets artikel 6, nr. 37, skal »elektronisk kommunikationstjeneste« forstås på samme måde som i artikel 2, nr. 4, i direktiv (EU) 2018/1972. Ved elektronisk kommunikationstjeneste forstås således 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 tjenester: a) »Internetadgangstjenester« som defineret i artikel 2, andet afsnit, nr. 2, i forordning (EU) 2015/2120, b) »interpersonelle kommunikationstjenester«, og c) tjenester, der udelukkende eller overvejende består i overføring af signaler, f.eks. transmissionstjenester, der anvendes til levering af maskine-til-maskine-tjenester og til radio- og tv-spredning.

Den foreslåede bestemmelse vil delvist gennemføre artikel 3, stk. 1, litra c, i NIS 2-direktivet. Det følger af artikel 3, stk. 1, litra c, at 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, anses for at være væsentlige enheder.

Det følger af det foreslåede *stk. 3,* at uanset deres størrelse anses følgende enheder for at være væsentlige enheder: 1) kvalificerede tillidstjenesteudbydere og topdomæneadministratorer samt DNS-tjenesteudbydere, 2) offentlige forvaltningsenheder under den centrale forvaltning, 3) enheder, der er identificeret som kritiske enheder i henhold til lov om kritiske enheders modstandsdygtighed og 4) enheder, der er blevet identificeret som operatører af væsentlige tjenester i overensstemmelse med 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, jf. dog § 5, stk. 2 og 5) øvrige enheder af en type, som er omfattet af lovens bilag 1 eller 2, hvor mindst én af følgende betingelser er opfyldt, jf. dog § 5, stk. 2: a) enheden er den eneste udbyder i Danmark af en tjeneste, der er væsentlig for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter, b) en forstyrrelse af den tjeneste, som enheden leverer, vil kunne have væsentlig indvirkning på den offentlige sikkerhed eller folkesundheden, c) en forstyrrelse af den tjeneste, som enheden leverer, vil kunne medføre en væsentlig systemisk risiko, navnlig for sektorer hvor en sådan forstyrrelse kan have en grænseoverskridende virkning eller d) 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 Danmark.

Den foreslåede bestemmelse vil gennemføre artikel 3, stk. 1, litra b og d-g, i NIS 2-direktivet. Det fremgår således af direktivets artikel 3, stk. 1, litra b og d-g, at følgende enheder anses for at være væsentlige enheder: b) kvalificerede tillidstjenesteudbydere og topdomænenavneadministratorer samt DNS-tjenesteudbydere, uanset deres størrelse, d) offentlige forvaltningsenheder omhandlet i artikel 2, stk. 2, litra f, nr. i, e) alle andre enheder af en type omhandlet i direktivets bilag I eller II, som en medlemsstat har identificeret som væsentlige enheder i medfør af artikel 2, stk. 2, litra b-e, f) enheder, der er identificeret som kritiske enheder i henhold til direktiv (EU) 2022/2557, og g) hvis medlemsstaten træffer afgørelse herom, enheder, som den pågældende medlemsstat inden den 16. januar 2023 har identificeret som operatører af væsentlige tjenester i overensstemmelse med direktiv (EU) 2016/1148 eller national ret.

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

Det følger af det foreslåede *nr. 1,* at kvalificerede tillidstjenesteudbydere og topdomæneadministratorer samt DNS-tjenesteudbydere anses for at være væsentlige enheder.

Ved kvalificerede tillidstjenesteudbydere forstås en tillidstjenesteudbyder, der udbyder en eller flere kvalificerede tillidstjenester og har fået tildelt status som kvalificeret tillidstjenesteudbyder af tilsynsorganet, jf. artikel 3, nr. 20 i i Europa-Parlamentets og Rådets forordning (eu) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF, jf. NIS 2-direktivets artikel 6, nr. 26.

Ved topdomæneadministrator forstås en enhed, der har fået uddelegeret et specifikt topdomæne, og som er ansvarlig for at administrere topdomænet, herunder registrering af domænenavne under topdomænet og den tekniske drift af topdomænet, hvilket inkluderer driften af dets navneservere, vedligeholdelsen af dets databaser og distributionen af topdomænezonefiler til navneservere, uanset om hvorvidt nogen af disse operationer udføres af enheden selv eller outsources, men ikke situationer, hvor topdomænenavne kun anvendes af en administrator til eget brug, jf. NIS 2-direktivets artikel 6, nr. 21.

Ved DNS-tjenesteudbydere forstås en enhed, der leverer a) offentligt tilgængelige rekursive domænenavnsoversættelsestjenester til internetslutbrugere, eller b) autoritative domænenavnsoversættelsestjenester til tredjepartsbrug, med undtagelse af rodnavneservere, jf. NIS 2-direktivets artikel 6, nr. 20.

Det følger af det foreslåede *nr. 2,* at offentlige forvaltningsenheder under den centrale forvaltning myndigheder anses for at være væsentlige enheder.

Det bemærkes, at det i overensstemmelsen med NIS 2-direktivets artikel 6, nr. 35 og NIS 2-direktivets artikel 2,

litra f, i), følger af det foreslåede § 1, stk. 1, at omfattet af lovens anvendelsesområde er statslige myndigheder, som anses som en offentlig forvaltningsenhed under den centrale forvaltning.

Omfattet af den foreslåede bestemmelse i nr. 2, vil være enheder, som er statslige myndigheder, og som opfylder betingelserne for at blive anset som offentlige forvaltningsenheder. Dette betyder, at f.eks. departementer, styrelser og institutioner som f.eks. Udbetaling Danmark må anses som omfattet af loven. Det bemærkes i den forbindelse, at Udbetaling Danmark har organisatorisk tilknytning til Beskæftigelsesministeriet, træffer afgørelser i forhold til borgere og virksomheder, er oprettet ved lov og omfattet af forvaltningsloven.

Der henvises i øvrigt til bemærkningerne til det foreslåede § 1, stk. 1.

Det følger af det foreslåede *nr. 3,* at enheder, der er identificeret som kritiske enheder i henhold til lov om kritiske enheders modstandsdygtighed, anses for at være væsentlige enheder.

Den foreslåede bestemmelse vil således medføre, at enheder, der er identificeret som kritiske i henhold til det samtidigt fremsatte forslag til lov om kritiske enheders modstandsdygtighed, vil anses som væsentlige enheder i henhold til nærværende lov. Bestemmelsen skaber således en forbindelse mellem implementeringen af henholdsvis NIS 2- og CER-direktiverne, jf. hertil lovforslagets pkt. 2.3.

Det følger af det foreslåede *nr. 4,* at enheder, der er blevet identificeret som operatører af væsentlige tjenester i overensstemmelse med NIS 1-direktivet, anses for at være væsentlige enheder.

Den foreslåede bestemmelse vil delvist gennemføre NIS 2-direktivets artikel 3, stk. 1, litra g. Det følger af den nævnte artikel, at hvis medlemsstaten træffer afgørelse herom anses enheder, som den pågældende medlemsstat inden den 16. januar 2023 har identificeret som operatører af væsentlige tjenester i overensstemmelse med NIS 1-direktivet eller national ret, for at være væsentlige enheder.

Den foreslåede bestemmelse vil således medføre, at enheder, der i dag er identificeret som operatører af væsentlige tjenester efter den nationale regulering, der gennemfører NIS 1-direktivet, vil være omfattet af nærværende lov som væsentlige enheder.

Det foreslås med *nr. 5,* at øvrige enheder af en type, som er lovens bilag 1 eller 2, anses for at være væsentlige enheder, hvor: a) enheden er den eneste udbyder i Danmark af en tjeneste, der er væsentlig for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter, b) en forstyrrelse af den tjeneste, enheden leverer, vil kunne have væsentlig indvirkning på den offentlige sikkerhed eller folkesundheden, c) en forstyrrelse af den tjeneste, enheden leverer, vil kunne medføre en væsentlig systemisk risiko, navnlig for sektorer hvor en sådan forstyrrelse kan have en grænseoverskridende virkning, eller d) 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 Danmark.

Af lovens bilag 1 fremgår følgende sektorer af særlig kritisk betydning: 1) transport med delsektorerne: a) luft, b) jernbane, c) vand og d) vejtransport, 2) sundhed, 3) drikkevand, 4) spildevand, 5) digital infrastruktur, 6) forvaltning af informations- og kommunikationstjenester (IKT-tjenester) (buisness-to-buisness, 7) offentlig forvaltning og 8) rummet.

Af lovens bilag 2 fremgår følgende andre kritiske sektorer: 1) post og kurertjenester, 2) affaldshåndtering, 3) fremstilling produktion og distribution af kemikalier, 4) produktion, tilvirkning og distribution af fødevarer, 5) fremstilling med delsektorerne: a) Fremstilling af medicinsk udstyr og medicinsk udstyr til in vitro-diagnostik, b) fremstilling af computere og elektroniske og optiske produkter, c) fremstilling af elektrisk udstyr, d) fremstilling af maskiner og udstyr intet andetsteds nævnt, e) fremstilling af motorkøretøjer, påhængsvogne og sættevogne og f) fremstilling af andre transportmidler, 6) digitale udbydere og 7) forskning.

NIS 2-direktivets artikel 3, stk. 1, litra e, lægger op til, at medlemsstaterne kan identificere enheder omfattet af kriterierne i § 4, stk. 3, nr. 5, som enten væsentlige eller vigtige enheder. Henset til de nævnte enheders samfundsmæssige betydning fastslår lovforslaget, at enhederne som udgangspunkt anses for væsentlige enheder. Der foreslås dog en modifikation til dette udgangspunkt i lovforslagets § 5, stk. 2, jf. nedenfor.

Bestemmelsen i stk. 3, nr. 5, har et forholdsvist skønsmæssigt og kvalitativt præg, hvilket kan gøre det vanskeligt for de enkelte enheder at vurdere, om de betragtes som omfattet af lovens krav til henholdsvis væsentlige eller vigtige enheder. Det forudsættes derfor, at de kompetente myndigheder i relevant omfang vejleder enheder inden for deres sektor om forståelsen af § 4, stk. 3, nr. 5.

Det følger af det foreslåede *stk. 4,* at vedkommende minister efter forhandling med ministeren for samfundssikkerhed og beredskab kan fastsætte nærmere regler om kriterier for, hvornår enheder er omfattet af stk. 3, nr. 5.

De kompetente myndigheder vil med den foreslåede bestemmelse kunne uddybe de skønsmæssige kriterier i bestemmelsens stk. 3, nr. 5, således at kriterierne tilpasses særlige sektorspecifikke forhold. De kompetente myndigheder vil eksempelvis kunne fastsætte nærmere regler om, hvornår en forstyrrelse af den tjeneste, som enheder inden for sin sektor, vil kunne medføre en væsentlig systematisk risiko.

For at sikre, at enheder, der er omfattet af flere sektorer, ikke rammes af modsatrettede krav, kan reglerne alene fastsættes efter forhandling med ministeren for samfundssikkerhed og beredskab.

Der henvises i øvrigt til afsnit 3.1 i lovforslagets almindelige bemærkninger.

Til § 5

Der er i artikel 5, stk. 1, i 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) en forpligtelse for medlemsstaterne til at identificere operatører af væsentlige tjenester, der opererer på deres område for en række nærmere angivne sektorer og delsektorer.

Efter NIS 1-direktivets artikel 5, stk. 2, er operatører af væsentlige tjenester følgende: a) En enhed der leverer en tjeneste, der er væsentlig for opretholdelsen af kritiske samfundsmæssige og/eller økonomiske aktiviteter, b) leveringen af denne tjeneste afhænger af net- og informationssystemer, og c) en hændelse ville få væsentlige forstyrrende virkninger for leveringen af den nævnte tjeneste.

NIS 1-direktivet omfatter også udbydere af digitale tjenester, som er visse udbydere af onlinemarkedspladser, onlinesøgemaskiner og cloud-computing-tjenester, jf. direktivets artikel 4, nr. 5.

NIS 1-direktivet blev i dansk ret gennemført sektorvist i regulering gældende for de specifikke sektorer, hvor direktivet finder anvendelse. For en nærmere gennemgang af den sektorvise implementering af NIS 1-direktivet henvises til afsnit 2.4 i lovforslagets almindelige bemærkninger.

Det følger af det foreslåede *stk. 1,* at enheder, som er omfattet af lovens bilag 1 eller 2, anses for at vigtige enheder, hvis enheden1) beskæftiger mere end 50 personer, eller 2) enheden har en årlig omsætning på over 10 mio. EUR og en årlig samlet balance på over 10 mio. EUR.

Den foreslåede bestemmelse vil delvist 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.

Den foreslåede bestemmelse svarer med sproglige tilpasninger uden indholdsmæssig betydning til NIS 2-direktivets artikel 3, stk. 2, 1. pkt., og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Den foreslåede bestemmelse indebærer således to kumulative kriterier for, hvornår en enhed anses for at være en vigtig enhed: 1) enheden skal være af en type, der er omfattet af lovens bilag 1 eller 2, og 2) enheden skal enten beskæftige mere end 50 personer eller have en årlig omsætning på 10 mio. EUR og en årlig balance på over 10 mio. EUR.

Af lovens bilag 1 fremgår følgende sektorer af særlig kritisk betydning: 1) transport med delsektorerne: a) luft, b) jernbane, c) vand og d) vejtransport, 2) sundhed, 3) drikkevand, 4) spildevand, 5) digital infrastruktur, 6) forvaltning af informations- og kommunikationstjenester (IKT-tjenester) (buisness-to-buisness), 7) offentlig forvaltning og 8) rummet.

Af lovens bilag 2 fremgår følgende andre kritiske sektorer: 1) post og kurertjenester, 2) affaldshåndtering, 3) fremstilling produktion og distribution af kemikalier, 4) produktion, tilvirkning og distribution af fødevarer, 5) fremstilling med delsektorerne: a) Fremstilling af medicinsk udstyr og medicinsk udstyr til in vitro-diagnostik, b) fremstilling af computere og elektroniske og optiske produkter, c) fremstilling af elektrisk udstyr, d) fremstilling af maskiner og udstyr intet andetsteds nævnt, e) fremstilling af motorkøretøjer, påhængsvogne og sættevogne og f) fremstilling af andre transportmidler, 6) digitale udbydere og 7) forskning.

Det følger af det foreslåede *stk. 2,* at den kompetente myndighed kan træffe afgørelse om, at en enhed uanset størrelse, som er omfattet af § 4, stk. 3, nr. 4 eller 5, skal anses for at være en vigtig enhed.

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.

Det følger endvidere af artikel 3, stk. 1, litra e, at alle andre enheder af en type, som omhandlet i direktivets bilag I eller II, som en medlemsstat har identificeret som væsentlige enheder i medfør af artikel 2, stk. 2, litra b-e, anses for at være væsentlige enheder. Det følger endvidere af NIS 2-direktivets artikel 3, stk. 1, litra g, at hvis medlemsstaten træffer afgørelse herom anses enheder, som den pågældende medlemsstat inden den 16. januar 2023 har identificeret som operatører af væsentlige tjenester i overensstemmelse med NIS 1-direktivet eller national ret, for at være væsentlige enheder.

Den foreslåede bestemmelse svarer med sproglige tilpasninger uden indholdsmæssig betydning til NIS 2-direktivets artikel 3, stk. 2, jf. artikel 3, stk. 1, litra e og g, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Det er Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at enheder, der er identificeret som operatører af væsentlige tjenester i overensstemmelse med NIS 1-direktivet som udgangspunkt må anses for at være væsentlige enheder.

Den foreslåede bestemmelse indebærer, at den relevante kompetente myndighed kan træffe afgørelse om, at en enhed, der er identificeret som operatør af væsentlige tjenester efter den danske gennemførelse af NIS 1-direktivet, skal anses for at være en vigtig enhed uanset udgangspunktet i det foreslåede § 4, stk. 3, nr. 4. For en nærmere gennemgang af

den sektorvise implementering af NIS 1-direktivet henvises til lovforslagets pkt. 2.4.

Den foreslåede bestemmelse er navnlig tiltænkt den situation, hvor der siden 16. januar 2023 er indtrådt sådanne ændringer i enhedens forhold, at enheden ikke længere ville blive anset som en operatør af væsentlige tjenester i medfør af den regulering, der gennemførte NIS 1-direktivets artikel 5 om identificering af operatører af væsentlige tjenester.

Særligt i relation til de enheder, der uanset deres størrelse omfattes af direktivet på baggrund af mere kvalitative kriterier i relation til deres samfundsmæssige betydning, jf. NIS 2-direktivets artikel 2, stk. 2, litra b-e, bemærkes det, at direktivet både nævner disse som væsentlige og vigtige enheder. Det er Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at disse enheder henset til deres samfundsmæssige betydning som udgangspunkt må anses for at være væsentlige enheder, men at der kan være situationer, hvor dette ikke bør være tilfældet.

Den foreslåede bestemmelse indebærer, at den relevante kompetente myndighed 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 enhed uanset udgangspunktet i det foreslåede § 4, stk. 3, nr. 5.

Såfremt en enhed i medfør af øvrige dele af lovforslagets § 4 ud over det foreslåede stk. 2, nr. 4 eller 5, må anses for at være en væsentlig enhed, vil der ikke kunne ske ændring af enhedens status fra væsentlig til vigtig efter den foreslåede bestemmelse.

Det bemærkes, at der vil være tale om en forvaltningsretlig afgørelse, der 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 henvises i øvrigt til lovforslagets pkt. 3.1.

Til § 6

Efter artikel 14, stk. 1, NIS 1-direktivet, skulle medlemsstaterne sikre, at operatører af væsentlige tjenester træffer passende og forholdsmæssige tekniske og organisatoriske foranstaltninger for at styre risiciene for sikkerheden i net- og informationssystemer, som de anvender til deres aktiviteter. Under hensyntagen til teknologiens aktuelle stade skulle disse foranstaltninger sikre et sikkerhedsniveau for net- og informationssystemer, der står i forhold til risikoen. Efter artikel 14, stk. 2, skulle medlemsstaterne sikre, at operatører af væsentlige tjenester traf passende foranstaltninger for at forebygge og minimere konsekvensen af hændelser, der berører sikkerheden i net- og informationssystemer, som anvendes til levering af væsentlige tjenester, med henblik på at sikre kontinuiteten i disse tjenester.

Det følger desuden af NIS 1-direktivets artikel 16, stk. 1, at medlemsstaterne skal sikre, at udbydere af digitale tjenester identificerer og træffer passende og forholdsmæssige tekniske og organisatoriske foranstaltninger for at styre risiciene i forhold til sikkerheden i net- og informationssystemer, som de anvender i forbindelse med de omfattede digitale tjenester. Under hensyntagen til teknologiens aktuelle stade skal disse foranstaltninger sikre et sikkerhedsniveau for net- og informationssystemer, der står i forhold til risikoen, under hensyntagen til: a) Systemers og faciliteters sikkerhed, b) håndtering af hændelser, c) styring af driftskontinuitet, d) monitorering, audit og testning og e) overholdelse af internationale standarder. Efter artikel 16, stk. 2, skal medlemsstaterne sikre, at udbydere af digitale tjenester træffer foranstaltninger for at forebygge og minimere konsekvensen af hændelser, der berører sikkerheden i deres net- og informationssystemer, for så vidt angår de onlinemarkedspladser, onlinesøgemaskiner og cloud-computing-tjenester, og som udbydes i Unionen, for at sikre kontinuiteten i disse tjenester.

NIS 1-direktivet blev i dansk ret gennemført sektorvist i regulering gældende for de specifikke sektorer, hvor direktivet finder anvendelse. For en nærmere gennemgang af den sektorvise implementering af NIS 1-direktivet henvises til afsnit 2.4 i lovforslagets almindelige bemærkninger.

Det følger af det foreslåede *stk. 1,* at væsentlige og vigtige enheder 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 eller tage højde for: 1) politikker for risikoanalyse og informationssystemsikkerhed, 2) håndtering af hændelser, 3) driftskontinuitet, eksempelvis backup-styring og reetablering efter en katastrofe, og krisestyring, 4) forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem den enkelte enhed og dens 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 cybersikkerhedsrisici, 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 og 10) brug af løsninger med multifaktorautentificering eller kontinuerlig autentificering, sikret tale-, video- og tekstkommunikation og sikrede nødkommunikationssystemer internt hos enheden, hvor det er relevant.

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, og mindst omfatte 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.

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 forsyningskædesikkerhed 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.

Det fremgår endvidere af NIS 2-direktivets artikel 25, stk. 1, at for at sikre en samordnet gennemførelse af artikel 21, stk. 1 og 2, tilskynder medlemsstaterne til at benytte europæiske og internationale standarder og tekniske specifikationer, der er relevante for sikkerheden i net- og informationssystemer, uden at de påtvinger eller forskelsbehandler til fordel for anvendelse af en bestemt type teknologi.

Det er Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at formuleringen »i net- og informationssystemer, som disse enheder anvender til deres operationer eller til at levere deres tjenester« i NIS 2-direktivets artikel 21, stk. 1, skal forstås som alle de net- og informationssystemer, som disse enheder anvender til deres operationer, eller til at levere deres tjenester.

Bestemmelsen vedrører således alle den pågældende enheds operationer og tjenester, ikke kun specifikke it-aktiver eller kritiske tjenester, som enheden leverer. Der henvises til lovforslagets pkt. 3.1.1.

I overensstemmelse med NIS 2-direktivets præambelbetragtning nr. 82, er det Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at foranstaltninger til styring af cybersikkerhedsrisici bør stå i et passende forhold til graden af de væsentlige eller vigtige enheders risikoeksponering og til den samfundsmæssige og økonomiske indvirkning, som en hændelse ville have. 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.

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 overens-

stemmelse med europæiske og internationale standarder såsom dem, der indgår i ISO/IEC 27000-serien.

I overensstemmelse med direktivets artikel 25, stk. 1 og præambelbetragtning nr. 80, bør medlemsstaterne i samråd med samarbejdsgruppen og Den Europæiske Cybersikkerhedscertificeringsgruppe fremme væsentlige og vigtige enheders anvendelse af relevante europæiske og internationale standarder eller kan eventuelt kræve, at enhederne anvender certificerede IKT-produkter, -tjenester og -processer. Det er Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at relevante europæiske og internationale standarder som for eksempel ISO/IEC 27000-serien, IEC 62443 standarder, NIST standarder og ETSI TR 103 305 standarder kan anvendes som et rammeværktøj til at træffe passende og forholdsmæssige tekniske, operationelle og organisatoriske foranstaltninger.

Hertil kommer, at EU-Kommissionen den 17. oktober 2024 vedtog gennemførelsesforordning (EU) 2024/2690 om regler for anvendelsen af NIS 2-diektivet for så vidt angår tekniske og metodologiske krav til foranstaltninger til styring af cybersikkerhedsrisici og yderligere præcisering af de tilfælde, hvor en hændelse anses for at være væsentlig, for så vidt angår DNS-tjenesteudbydere, topdomænenavneadministratorer og udbydere af cloudcomputingtjenester, af datacentertjenester, af indholdsleveringsnetværk, af administrerede tjenester, af administrerede sikkerhedstjenester, af onlinemarkedspladser, af onlinesøgemaskiner og af platforme for sociale netværkstjenester og af tillidstjenester. Gennemførelsesforordningen finder således kun anvendelse for DNS-tjenesteudbydere, topdomænenavneadministratorer og udbydere af cloudcomputingtjenester, af datacentertjenester, af indholdsleveringsnetværk, af administrerede tjenester, af administrerede sikkerhedstjenester, af onlinemarkedspladser, af onlinesøgemaskiner og af platforme for sociale netværkstjenester og af tillidstjenester.

I overensstemmelse med direktivets forudsætninger, som udtrykt i præambelbetragtning nr. 81, bør foranstaltninger til styring af cybersikkerhedsrisici stå i et rimeligt forhold til den risiko, det pågældende net- og informationssystem er udsat for, under hensyntagen til sådanne foranstaltningers aktuelle teknologiske stade og i givet fald til relevante europæiske og internationale standarder samt omkostningerne ved deres gennemførelse med henblik på at undgå, at operatører af væsentlige og vigtige enheder pålægges en uforholdsmæssig stor økonomisk og administrativ byrde.

Det bemærkes, at krav om foranstaltninger over for enheder skal stå i et passende forhold til graden af de væsentlige eller vigtige enheders risikoeksponering og til den samfundsmæssige og økonomiske indvirkning, som en hændelse ville have. Der vil således være tale om en konkret vurdering af enhedens samfundskritikalitet. Det bemærkes, at den kompetente myndighed som led i sin generelle vejledningsforpligtelse over for enheder, vil kunne yde vejledning til omfattede enheder vedrørende foranstaltninger.

Det foreslås i *nr. 1,* at foranstaltningerne skal omfatte politiker for risikoanalyse og informationssystemsikkerhed.

Dette vil bl.a. indebære, 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 net- og informationssystemer. Enheder skal endvidere udarbejde en politik for risikostyring, som indeholder metoder til at identificere og adressere eventuelle risici.

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

Dette vil bl.a. indebære, at enheder skal udarbejde procedurer for håndtering af hændelser. Enheder skal 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 driftskontinuitet, herunder backup-styring og reetablering efter en katastrofe og krisestyring.

Dette vil indebære, at enheder skal udarbejde procedurer til sikring af driftskontinuitet i tilfælde af en hændelse. På grundlag af enhedernes risikostyring, jf. nr. 2, og driftskontinuitets-procedure, 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 forsyningssikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem den enkelte enhed og dens direkte leverandører eller tjenesteudbydere.

Dette vil indebære, 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 koordinerede 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 sikker-

hedsrisikovurderinger af specifikke kritiske IKT-tjenester, -systemer eller -produktforsyningskæder under hensyntagen til tekniske og, hvor det er relevant, ikketekniske risikofaktorer.

Der henvises i 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 sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer, herunder håndtering og offentliggørelse af sårbarheder.

Dette vil indebære, 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 politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici.

Dette vil indebære, 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 grundlæggende cyberhygiejnepraksisser og cybersikkerhedsuddannelse.

Dette vil bl.a. indebære, 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 politikker og procedurer vedrørende brug af kryptografi og, hvor det er relevant, kryptering.

Dette vil bl.a. indebære, 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 personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver.

Dette vil bl.a. indebære, at enhederne 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 net- og informationssystemer.

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

Dette vil bl.a. indebære, 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 overensstemmelse med politikken for brug af kryptografi og kryptering og under hensyntagen til kommunikationsmidlernes tilgængelighed, også i en nødsituation.

Det følger af det foreslåede *stk. 2,* at en enhed, der ikke overholder ét eller flere krav til foranstaltningerne 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 i stk. 2 understreger, at enheder vil skulle 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 § 7 om ledelsens ansvar.

Det følger af det foreslåede *stk. 3,* at vedkommende minister efter forhandling med ministeren for samfundssikkerhed og beredskab kan fastsætte nærmere regler om foranstaltninger efter stk. 1.

Det er Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at de ansvarlige ressortministre bør bemyndiges til at konkretisere lovens generelle krav om foranstaltninger, såfremt særlige sektorspecifikke hensyn tilsiger. En sådan 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. Reglerne bør udstedes af de enkelte ressortministre efter forhandling med ministeren for samfundssikkerhed og beredskab, jf. afsnit 2.2.

Den foreslåede bestemmelse vil indebære, at de relevante ressortministre inden for deres områder – efter forhandling med ministeren for samfundssikkerhed og beredskab – kan fastsætte nærmere regler om de foranstaltninger, som væsentlige og vigtige enheder skal træffe til styring af cybersikkerhedsrisici. Bemyndigelsesbestemmelsen forudsættes anvendt i tilfælde, hvor særlige sektorspecifikke hensyn tilsiger et behov for konkretisering af denne lovs krav til foranstaltninger.

Det foreslåede vil indebære, at der vil blive udarbejdet sektorspecifikke bekendtgørelser, som i relevant omfang vil kunne tilpasses de enkelte sektorers specifikke forhold, ligesom der i overensstemmelse med direktivets forudsætninger ud fra en risikobaseret tilgang vil kunne fastsættes differentierede regler henset til eksempelvis forskellige kategorier af enheder inden for samme sektor, henset til forskelle i enhedernes risikoeksponering, størrelse og den potentielle samfundsmæssige og økonomiske betydning af eventuelle hændelser.

Efter det foreslåede stk. 3 vil reglerne skulle udstedes efter forhandling med ministeren for samfundssikkerhed og beredskab. Formålet med kravet om forhandling med ministeren for samfundssikkerhed og beredskab er at sikre, at der opnås ensartethed på tværs af de sektorspecifikke bekendtgørelser, dog under hensyntagen til særlige sektorforhold og eventuelle behov for differentiering af reglerne inden for sektorerne.

Det bemærkes, at Europa-Kommissionens gennemførelsesforordning (EU) 2024/2690 fastsætter de tekniske og metodologiske krav til de foranstaltninger, der er omhandlet i NIS 2-direktivets artikel 21, stk. 2, for så vidt angår DNS-tjenesteudbydere, topdomænenavneadministratorer og udbydere af cloudcomputingtjenester, at datacentertjenester, af indholdsleveringsnetværk, af administrerede tjenester, af administrerede sikkerhedstjenester, af on-linmarkedspladser af onlinesøgemaskiner og af platforme for sociale netværkstjenester og af tillidstjenester.

Det følger af direktivets præambelbetragtning nr. 84, at de i artikel 21, stk. 5, 1. led, omhandlede enheder – i betragtning af deres grænseoverskridende karakter – bør være underlagt en høj grad af harmonisering på EU-plan. Det anføres i den forbindelse, at gennemførelsen af foranstaltninger til styring af cybersikkerhedsrisici med hensyn til disse enheder derfor bør lettes ved hjælp af en gennemførelsesretsakt.

For så vidt angår andre væsentlige og vigtige enheder end dem, der er omhandlet i direktivets artikel 21, stk. 5, 1. led., fremgår det af 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 er på denne baggrund Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at udstedelsen af bekendtgørelser i medfør af den foreslåede bemyndigelse i stk. 3, ikke behøver at afvente Europa-Kommissionens eventuelle vedtagelse af de nævnte gennemførelsesretsakter.

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.

Der henvises i øvrigt til afsnit 3.2 i lovforslagets almindelige bemærkninger.

Til § 7

Der er i 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) ikke nærmere

regulering af ledelsens ansvar og opgaver. Der er på denne baggrund i dag ikke fastsat regler herom.

Det foreslås i *stk. 1,* at de foranstaltninger, som en væsentlig eller vigtig enhed træffer på baggrund af forpligtelserne i § 6, stk. 1 og 2, samt regler fastsat i medfør af § 6, stk. 3, skal være godkendt af enhedens ledelsesorgan. 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 vil fastslå, at overholdelsen af forpligtelserne i den foreslåede § 6, stk. 1-3, er et ledelsesmæssigt ansvar. For så vidt angår den del af direktivets artikel 20, stk. 1, der foreskriver, at ledelsesorganer skal kunne gøres ansvarlige for overtrædelser af enhedernes forpligtelser, henvises til den foreslåede § 23, stk. 1, nr. 2.

Den foreslåede bestemmelse vil medføre, at en enheds ledelse vil være forpligtet til at godkende de foranstaltninger, som enheden træffer på baggrund af den foreslåede § 6, stk. 1 og 2, samt regler fastsat i medfør af § 6, stk. 3. Derudover vil ledelsen være forpligtet til at føre tilsyn med foranstaltningernes gennemførelse.

Det bemærkes, at der i dansk ret ikke findes en definition af et 'ledelsesorgan'. Lov om aktie- og anpartsselskaber, jf. lovbekendtgørelse nr. 1168 af 1. september 2023 (selskabsloven) definerer dog i § 5, nr. 4 '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.

Det følger af det foreslåede *stk. 2,* at medlemmerne af en væsentlig eller vigtig enheds ledelsesorgan skal deltage i relevante kurser om styring af cybersikkerhedsrisici og tilskynde til at tilsvarende kurser tilbydes til enheden øvrige ansatte.

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.

Den foreslåede bestemmelse svarer med sproglige tilpasninger uden indholdsmæssig betydning til NIS 2-direktivets artikel 20, stk. 2, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Den foreslåede bestemmelse vil indebære, at medlemmerne af en væsentlig eller vigtig enheds ledelsesorgan vil skulle deltage i relevante kurser om styring af cybersikkerhedsrisici, og tilskynde til at tilsvarende kurser tilbydes enhedens øvrige ansatte.

Der henvises i øvrigt til afsnit 3.2 i lovforslagets almindelige bemærkninger.

Til § 8

Der er i 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) ikke nærmere regulering om brug af særlige informations- og kommunikationstjenester (IKT)-produkter, -tjenester og -processer. På denne baggrund er der i dag ikke fastsat regler herom-

Det følger af den foreslåede *§ 8,* at vedkommende minister efter forhandling med ministeren for samfundssikkerhed og beredskab kan fastsætte regler om, at væsentlige og vigtige enheder skal anvende særlige IKT-produkter, -tjenester og -processer, som er certificeret i henhold til en europæisk cybersikkerhedscertificeringsordning for at påvise overensstemmelse med bestemte krav i § 6, stk. 1, eller regler om krav til foranstaltninger fastsat i medfør af § 6, stk. 3. Pro-

duktet kan udvikles af den væsentlige eller vigtige enhed eller indkøbes fra tredjeparter.

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.

For i videst muligt omfang af sikre ensartethed på tværs af sektorer, foreslås det, at eventuelle regler, der udstedes i medfør af den foreslåede bestemmelse, fastsættes efter forhandling med ministeren for samfundssikkerhed og beredskab.

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.

Der henvises i øvrigt til afsnit 3.2 i lovforslagets almindelige bemærkninger.

Til § 9

Der er i 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) ikke nærmere regulering om, at de enheder, der er omfattet af den nationale regulering, der gennemfører direktivet, skal registrere sig ved de nationale myndigheder.

Baggrunden herfor er, at det med NIS 1-direktivet påhvilede myndighederne at identificere de enheder, der er omfattet af direktivets anvendelsesområde.

Det følger af den foreslåede *stk. 1,* at DNS-tjenesteudbydere, topdomænenavneadministratorer, enheder der leverer domænenavnsregistreringstjenester og udbydere af cloudcomputingtjenester, datacentertjenester, indholdsleveringsnetværk, administrerede tjenester, administrerede sikkerhedstjenester, onlinemarkedspladser, onlinesøgemaskiner og platforme for sociale netværkstjenester, skal registrere sig hos den relevante kompetente myndighed og i den forbindelse oplyse følgende 1) enhedens navn, 2) adressen på enhedens hovedforretningssted og dens andre forretningssteder i Den Europæiske Union eller, hvis den ikke er etableret i Unionen, den repræsentant, der er udpeget i henhold til § 2, stk. 4, 3) den relevante sektor, delsektor og typen af enhed, som enheden udgør, jf. lovens bilag 1 eller 2, 4) ajourførte kontaktoplysninger, herunder e-mailadresser, IP-intervaller og telefonnumre på enheden og i givet fald kontaktoplysninger på dens repræsentant udpeget i henhold til § 2, stk. 4, og 5) de medlemsstater i Den Europæiske Union, hvor enheden leverer tjenester.

Den foreslåede bestemmelse vil gennemføre artikel 27, stk. 2, i 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 følgende oplysninger til de kompetente myndigheder: a) Enhedens navn, b) den relevante sektor og delsektor og typen af enhed, som i givet fald er omhandlet i direktivets bilag I eller II, c) adressen på enhedens hovedforretningssted og dens andre retlige forretningssteder i Unionen eller, hvis den ikke er etableret i Unionen, på den repræsentant, der er udpeget i henhold til direktivets artikel 26, stk. 3, d) ajourførte kontaktoplysninger, herunder e-mailadresser og telefonnumre på enheden og i givet fald dens repræsentant udpeget i henhold til direktivets artikel 26, stk. 3, e) de medlemsstater, hvor enheden leverer tjenester og f) enhedens IP-intervaller.

Den foreslåede bestemmelse svarer indholdsmæssigt til NIS

2-direktivets artikel 27, stk. 2, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Den foreslåede bestemmelse indebærer, at der indføres en særlig registreringspligt for visse typer af digitale tjenester.

Det bemærkes, at NIS 2-direktivets artikel 27, stk. 2, og artikel 3, stk. 4, begge indeholder bestemmelser om, at nærmere angivne enheder skal registrere sig hos de kompetente myndigheder. Henset til, at registreringspligterne i de to artikler vedrører forskellige grupper af enheder, og da der er forskelle i, hvilke oplysninger enhederne skal afgive til de kompetente myndigheder, lægges der op til, at de to artikler gennemføres ved henholdsvis nærværende bestemmelse og den foreslåede bestemmelse i § 10

Det forudsættes, at enhedernes registrering – på samme vis som registreringen efter den foreslåede bestemmelse i § 10 – vil ske via en fælles digital indgang såsom Virk.dk.

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, 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 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.

De kompetente myndigheder vil – via det centrale kontaktpunkt – i overensstemmelse med NIS 2-direktivets artikel 27, stk. 4, videresende oplysninger modtaget i medfør af bestemmelsen til ENISA.

Det følger af det foreslåede *stk. 2,* at oplysningerne efter stk. 1, skal indgives senest tre måneder efter, at enheden omfattes af loven.

Bestemmelsen vil gennemføre dele af artikel 27, stk. 2, i NIS 2-direktivet, som bl.a. fastslår, at oplysningerne skal indgives til de kompetente myndigheder senest den 17. januar 2025. Det bemærkes i den forbindelse, at NIS 2-direktivet skulle være implementeret i dansk ret senest den 17. oktober 2024. Denne lov forventes at træde i kraft den 1. juli 2025. Det er på den baggrund Ministeriet for Samfundssikkerhed og Beredskabs vurdering, at af fristen for indgivelse af oplysninger bør udskydes til efter lovens ikrafttrædelse.

Den foreslåede bestemmelse svarer indholdsmæssigt til dele af NIS 2-direktivets artikel 27, stk. 2, 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 enhederne 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 enhed 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 § 33, stk. 3, skulle indgive de nævnte oplysninger senest den 1. oktober 2025.

Det foreslås i *stk. 3,* at i tilfælde af ændringer i de oplysninger, der er afgivet i medfør af stk. 1, skal enheden give den relevante kompetente myndighed underretning herom senest tre måneder efter datoen for ændringen.

Den foreslåede bestemmelse vil medføre, at i tilfælde af ændringer i de oplysninger der er afgivet i medfør af det foreslåede stk. 1, vil enheden skulle underrette den kompetente myndighed herom senest tre måneder 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.

Til § 10

Der er i 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) ikke nærmere regulering om, at de enheder, der er omfattet af den nationale regulering, der gennemfører direktivet, skal registrere sig ved de nationale myndigheder.

Baggrunden herfor er, at det med NIS 1-direktivet påhvilede myndighederne at identificere de enheder, der er omfattet af direktivets anvendelsesområde.

Det følger af det foreslåede *stk. 1,* at væsentlige og vigti-

ge enheder samt enheder, der leverer domænenavnsregistreringstjenester, skal registrere sig hos den relevante kompetente myndighed og i den forbindelse oplyse følgende: 1) Enhedens navn, 2) adresse og ajourførte kontaktoplysninger, herunder e-mailadresser, IP-intervaller og telefonnumre, 3) den relevante sektor og delsektor, som enheden er omfattet af, jf. lovens bilag 1 eller 2 og 4) i givet fald en liste over de øvrige medlemsstater i Den Europæiske Union, hvor enheden leverer tjenester, der er omfattet af anvendelsesområdet i artikel 2 i NIS 2-direktivet.

Den foreslåede bestemmelse vil gennemføre artikel 3, stk. 4, 1. led, i NIS 2-direktivet. Det følger af direktivets artikel 3, stk. 4, 1. led, at medlemsstaterne skal pålægge væsentlige og vigtige enheder, samt enheder der leverer domænenavnsregistreringsdata, at indgive mindst 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 og delsektor i bilag I eller II, samt d) i givet fald en liste over de medlemsstater, hvor enheden leverer tjenester, der er omfattet af direktivets anvendelsesområde.

Den foreslåede bestemmelse svarer indholdsmæssigt til NIS 2-direktivets artikel 3, stk. 4, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Det bemærkes, at NIS 2-direktivets artikel 27, stk. 2, og artikel 3, stk. 4, begge indeholder bestemmelser om, at nærmere angivne enheder skal registrere sig hos de kompetente myndigheder. Henset til, at registreringspligterne i de to artikler vedrører forskellige grupper af enheder, og da der er forskelle i, hvilke oplysninger enhederne skal afgive til de kompetente myndigheder, lægges der op til, at de to artikler gennemføres ved henholdsvis nærværende bestemmelse og den foreslåede bestemmelse i § 10.

Baggrunden for registreringspligten i artikel 3, stk. 4, er, at medlemsstaterne efter NIS 2-direktivets artikel 3, stk. 3, senest den 17. april 2025 skal udarbejde en liste over væsentlige og vigtige enheder samt enheder, der leverer domænenavnsregistreringstjenester.

Med de indsamlede oplysninger sikres der således et overblik over de væsentlige og vigtige enheder, og de enheder der leverer domænenavnsregistreringstjenester, som er omfattet af lovens anvendelsesområde. Det forudsættes, at enheder, der leverer tjenester i flere sektorer, vil skulle foretage én samlet registrering via en fælles digital indgang, såsom Virk.dk. Dette vil sikre, at disse enheder alene skal foretage én indledende registrering, som fordeles samtidigt til de relevante myndigheder. Det forudsættes, at CSIRT'en kan tilgå oplysningerne, således at CSIRT'en har et samlet overblik over de registrerede enheder på tværs af sektorer.

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, 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 selvinkriminering ikke er 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.

De kompetente myndigheder vil – via det centrale kontaktpunkt – i overensstemmelse med NIS 2-direktivets artikel 3, stk. 5, bl.a. vil orientere Europa-Kommissionen og Samarbejdsgruppen om antallet af væsentlige og vigtige enheder for hver sektor og delsektor.

Det følger af det foreslåede *stk. 2,* at oplysningerne efter stk. 1 skal indgives senest to uger efter, at enheden 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 enhederne 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 enhed 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 § 33, stk. 3, skulle indgive de nævnte oplysninger senest den 1. oktober 2025.

Det følger af det foreslåede *stk. 3,* at enheden i tilfælde af ændring i de oplysninger, der er afgivet i medfør af stk. 1, skal give den relevante kompetente myndighed underretning herom senest to uger efter datoen for ændringen.

Bestemmelsen vil gennemføre NIS 2-direktivets artikel 3, stk. 4, 2. pkt., som fastsætter, at væsentlige og vigtige enheder, samt enheder, der leverer domænenavnsregistreringstjenester, i tilfælde af ændringer af de oplysninger, de har indgivet i henhold til artikel 3, stk. 4, 1. pkt., straks skal give underretning herom og under alle omstændigheder senest to uger efter datoen for ændringen.

Ministeriet for Samfundssikkerhed og Beredskab har lagt vægt på, at der foretages en direktivnær minimumsimplementering. Den foreslåede bestemmelse svarer indholdsmæssigt til NIS 2-direktivets artikel 3, stk. 4, 2. pkt., og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Til § 11

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), indeholder ikke nærmere regulering om, at topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester skal føre en database over domænenavnsregistreringsdata.

Der er i lov nr. 164 af 26. februar 2014 om internetdomæner fastsat en række forpligtelser for administratorerne af topdomænenavne, der særligt tildeles Danmark, og topdomænenavne, der på anden vis er tilknyttet Danmark.

Der er således i § 18 bl.a. en forpligtelse for administratoren af et topdomænenavn til at oprette og vedligeholde en såkaldt WHOIS-database, hvoraf registranternes navn, adresse og telefonnummer fremgår. Der er desuden en forpligtelse for administratoren til at sikre, at oplysningerne i databasen er retvisende, opdaterede og offentligt tilgængelige. Med WHOIS-databasen sikres det, at enhver ved et opslag kan få oplyst, hvem der er registrant bag et domænenavn.

Det følger af det foreslåede *stk. 1,* at topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester, skal føre en særskilt database, der indeholder nøjagtige og fuldstændige domænenavnsregistreringsdata.

Den foreslåede bestemmelse vil gennemføre artikel 28, stk. 1, i NIS 2-direktivet. Det følger af artikel 28, stk. 1, at med henblik på at bidrage til DNS' sikkerhed, stabilitet og modstandsdygtighed pålægger medlemsstaterne topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringsdata, med rettidig omhu at indsamle og vedligeholde nøjagtige og fuldstændige domænenavnsregistreringsdata i en særlig database i overensstemmelse med EU-databeskyttelsesretten for så vidt angår personoplysninger.

Det fremgår af NIS 2-direktivets præambelbetragtning nr. 109, at det er et afgørende element i at sikre et højt cybersikkerhedsniveau i Den Europæiske Union, at der føres nøjagtige og fuldstændige databaser over domænenavnsregistreringsdata (WHOIS-data), og at der gives lovlig adgang til sådanne data.

Den foreslåede bestemmelse svarer med sproglige tilpasninger uden indholdsmæssig betydning til artikel 28, stk. 1, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Særligt for så vidt angår forholdet mellem § 18 i lov om internetdomæner og den foreslåede § 11, som gennemfører NIS 2-direktivets artikel 28, bemærkes, at regelsættene har forskellige anvendelsesområder. § 18 i lov om internetdomæner gælder således over for administratoren af det danske domænenavn ». dk«, mens den foreslåede § 11 omfatter alle de administratorer af topdomænenavne og registratorer, som udfører aktiviteter rettet mod EU. Derudover er de krav, som lov om internetdomæner stiller, væsentligt mere vidtgående end forpligtelserne i den foreslåede § 11.

Det følger af det foreslåede *stk. 2*, at databasen efter stk. 1 skal indeholde oplysninger om: 1) domænenavnet, 2) registreringsdatoen, 3) den registreredes navn, e-mailadresse og telefonnummer og 4) e-mailadresse og telefonnummer på det kontaktpunkt, der administrerer domænenavnet, hvis kontaktpunktet er forskelligt fra den registrerede.

Den foreslåede bestemmelse vil gennemføre NIS 2-direktivets artikel 28, stk. 2, hvoraf det følger, at medlemsstaterne stiller krav om, at databasen over domænenavnsregistreringsdata indeholder de fornødne oplysninger til at identificere og kontakte indehaverne af domænenavne og kontaktpunkter, der forvalter domænenavne under topdomæner. Sådanne oplysninger omfatter: a) Domænenavnet, b) registreringsdatoen, c) registrantens navn, kontakt-e-mailadresse og telefonnummer og d) kontakt-e-mailadresse og telefonnummer på det kontaktpunkt, der administrerer domænenavnet, i det tilfælde at de er forskellige fra registranten.

Den foreslåede bestemmelse svarer indholdsmæssigt til NIS 2-direktivets artikel 28, stk. 2, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Det følger af det foreslåede *stk. 3*, at topdomænenavneadministratorerne og enheder, der leverer domænenavnsregistreringstjenester, skal indføre politikker og procedurer, herunder verifikationsprocedurer, for at sikre, at databaserne indeholder nøjagtige og fuldstændige oplysninger. Politikkerne og procedurerne skal gøres offentligt tilgængelige.

Den foreslåede bestemmelse vil gennemføre NIS 2-direktivets artikel 28, stk. 3, hvoraf det følger, at medlemsstaterne stiller krav om, at topdomænenavneadministratorerne og de enheder, der leverer domænenavnsregistreringstjenester, har indført politikker og procedurer, herunder verifikationsprocedurer, for at sikre, at de i artikel 28, stk. 1, omhandlede databaser indeholder nøjagtige og fuldstændige oplys-

ninger. Medlemsstaterne kræver, at sådanne politikker og procedurer gøres offentligt tilgængelige

Den foreslåede bestemmelse svarer indholdsmæssigt til NIS 2-direktivets artikel 28, stk. 3, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

I overensstemmelse med NIS 2-direktivets præambelbetragtning nr. 111, vil topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester, efter bestemmelsen skulle fastlægge politikker og procedurer for indsamling og vedligeholdelse af nøjagtige og fuldstændige domænenavnsregistreringsdata samt forebyggelse og rettelse af unøjagtige registreringsdata i overensstemmelse med EU-databeskyttelsesretten. De indførte politikker og procedurer skal så vidt muligt tage hensyn til de standarder, der er udviklet af multiinteressentstyringsstrukturerne på internationalt plan. Topdomænenavneadministratorerne og de enheder, der leverer domænenavnsregistreringstjenester, bør således fastlægge og indføre forholdsmæssige procedurer til verifikation af domænenavnsregistreringsdata. Procedurerne bør afspejle industriens best practice og så vidt muligt de fremskridt, der er gjort inden for elektronisk identifikation. Verifikationsprocedurerne kan eksempelvis bestå i forudgående kontrol, der foretages på tidspunktet for registreringen, og efterfølgende kontrol der foretages efter registreringen. Topdomænenavneadministratorerne og de enheder, der leverer domænenavnsregistreringstjenester, bør navnlig verificere mindst én kontaktmåde for registranten.

Det følger af det foreslåede *stk. 4*, at topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester, uden unødigt ophold efter registreringen af et domænenavn skal gøre domænenavnsregistreringsdata, som ikke er personoplysninger, offentligt tilgængelige.

Den foreslåede bestemmelse vil gennemføre NIS 2-direktivets artikel 28, stk. 4, hvoraf det følger, at medlemsstaterne pålægger topdomænenavneadministratorerne og de enheder, der leverer domænenavnsregistreringstjenester, uden unødigt ophold efter registreringen af et domænenavn at gøre domænenavnsregistreringsdata, som ikke er personoplysninger, offentligt tilgængelige.

Den foreslåede bestemmelse svarer indholdsmæssigt til NIS 2-direktivets artikel 28, stk. 4, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Efter bestemmelsen vil enhederne bl.a. skulle sikre, at der ikke indgår personoplysninger i de domæneregistreringsdata, der gøres offentligt tilgængelige.

Det følger af det foreslåede *stk. 5*, at topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester, på baggrund af en anmodning og efter en konkret vurdering af nødvendigheden skal give legitime adgangssøgende adgang til specifikke domænenavnsregistreringsdata, herunder personoplysninger. Anmodninger skal besvares uden unødigt ophold og senest inden for 72 timer efter modtagelse af anmodningen. Topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester, skal indføre og offentliggøre politikker og procedurer for adgangen til data.

Den foreslåede bestemmelse vil gennemføre NIS 2-direktivets artikel 28, stk. 5, hvoraf det følger, at medlemsstaterne pålægger topdomænenavneadministratorerne og de enheder, der udbyder domænenavnsregistreringstjenester, at give adgang til specifikke domænenavnsregistreringsdata efter lovlige og behørigt begrundede anmodninger fra legitime adgangssøgende i overensstemmelse med EU-databeskyttelsesretten. Medlemsstaterne pålægger topdomænenavneadministratorerne og de enheder, der udbyder domænenavnsregistreringstjenester, at besvare anmodninger om adgang uden unødigt ophold og under alle omstændigheder inden for 72 timer efter modtagelse af anmodninger. Medlemsstaterne skal kræve, at sådanne politikker og procedurer gøres offentligt tilgængelige.

Den foreslåede bestemmelse svarer indholdsmæssigt til NIS 2-direktivets artikel 28, stk. 5, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Den foreslåede bestemmelse indebærer, at topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester, efter anmodning fra en legitim adgangssøgende vil skulle give adgang til specifikke domænenavnsregistreringsdata uden unødigt ophold og under alle omstændigheder inden for 72 timer efter anmodningen. Domænenavnsregistreringsdata vil som udgangspunkt være offentligt tilgængeligt, jf. det foreslåede stk. 4. Adgangen efter stk. 5 vil således primært indebære, at den legitime adgangssøgende også kan få adgang til personoplysninger, som indgår i de pågældende data. Det forudsættes, at en sådan adgang til personoplysninger alene gives, hvis det er i overensstemmelse med databeskyttelsesretten.

Vurderingen af, hvornår der er tale om en legitim adgangssøgende, skal ske i overensstemmelse med NIS 2-direktivets præambelbetragtning nr. 110, hvoraf det fremgår, at der ved legitime adgangssøgende forstås enhver fysisk eller juridisk person, der fremsætter en anmodning i henhold til EU-retten eller national ret. Dette omfatter de kompetente myndigheder, CSIRT'en og myndigheder, som i henhold til EU-retten eller dansk ret arbejder med at forebygge, efterforske eller retsforfølge strafbare handlinger. Anmodningen fra den legitime adgangssøgende skal i overensstemmelse med præambelbetragtning nr. 110 ledsages af en begrundelse, der gør det muligt at vurdere nødvendigheden af adgangen til de efterspurgte data.

Det følger af det foreslåede *stk. 6*, at topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester, skal samarbejde om overholdelsen af de forpligtelser, der er fastsat i stk. 1-5, med henblik på at undgå dobbeltindsamling af domænenavnsregistreringsdata.

Bestemmelsen vil gennemføre NIS 2-direktivets artikel 28, stk. 6, som fastsætter, at overholdelse af forpligtelser efter

stk. 1-5 ikke må føre til en gentagelse af indsamlingen af domænenavnsregistreringsdata. Med henblik herpå pålægger medlemsstaterne topdomænenavne administratorer og enheder, der leverer domænenavnsregistreringstjenester, at samarbejde med hinanden.

Den foreslåede bestemmelse svarer indholdsmæssigt til NIS 2-direktivets artikel 28, stk. 6, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Det følger af det foreslåede *stk. 7,* at den kompetente myndighed kan meddele topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester, forbud eller påbud for at sikre overholdelsen af kravene efter stk. 1-6, eller regler udstedt i medfør af stk. 8.

Den foreslåede bestemmelse indebærer, at den kompetente myndighed vil kunne meddele topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester, forbud eller påbud for at sikre overholdelsen af kravene efter stk. 1-6, eller regler udstedt i medfør af stk. 8.

Den foreslåede bestemmelse implementerer delvist NIS 2-direktivets artikel 31, stk. 1, hvorefter medlemsstaterne skal sikre, at deres kompetente myndigheder effektivt overvåger og træffer de nødvendige foranstaltninger til at sikre, at direktivet overholdes.

Det fremgår i den forbindelse af direktivets præambelbetragtning nr. 132, at hvor dette direktiv ikke harmoniserer administrative sanktioner eller hvor det i andre tilfælde er nødvendigt, f.eks. i tilfælde af en alvorlig overtrædelse af dette direktiv, bør medlemsstaterne indføre en ordning, der giver mulighed for at pålægge sanktioner, som er effektive, står i rimeligt forhold til overtrædelsen og har afskrækkende virkning.

Det bemærkes, at der ved udstedelse af påbud og forbud vil være tale om forvaltningsretlige afgørelser, og at forvaltningslovens regler om bl.a. partshøring, vil finde anvendelse.

Ved vurderingen af, om der skal udstedes forbud eller påbud vil der skulle foretages en konkret vurdering af sagens samlede omstændigheder, som overholder det forvaltningsretlige proportionalitetsprincip.

Det følger af det foreslåede *stk. 8,* at digitaliseringsministeren kan fastsætte nærmere regler om krav til politikker og procedurer efter stk. 3 og 5.

Bestemmelsen skal sikre, at der kan udstedes administrative forskrifter på baggrund af retningslinjer udarbejdet af Europa-Kommissionen, ENISA eller Samarbejdsgruppen nedsat iht. NIS2-direktivet.

Bemyndigelsesbestemmelsen vil bl.a. kunne anvendes til at fastsætte bestemmelser om bl.a. validerings- og verifikationsmetoder af e-mailadresse, telefonnummer og navn for en registrant af et domænenavn, samt hvornår en validering og verifikation skal finde sted. Endvidere hvilke oplysninger der skal afgives ved anmodninger fra legitime adgangssøgende og evt. andre, der fremsætter en begrundet anmodning om udlevering af ikke-offentliggjorte domænenavnsregistreringsdata og tidsrammerne herfor, herunder tidsrammerne for udlevering af oplysninger ved hasteanmodninger i tilfælde af situationer, som eksempelvis udgør en trussel mod liv, kritisk infrastruktur eller i tilfælde af misbrug af børn.

Til § 12

Det følger af artikel 14, stk. 3, i 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), at medlemsstaterne sikrer, at operatører af væsentlige tjenester hurtigst muligt foretager en underretning til den kompetente myndighed eller CSIRT af hændelser, der har væsentlige konsekvenser for kontinuiteten af de væsentlige tjenester, som de leverer. Underretningerne skal indeholde oplysninger, der gør det muligt for den kompetente myndighed eller CSIRT at fastslå eventuelle grænseoverskridende konsekvenser af hændelsen. Underretning gør ikke den underrettende part til genstand for et øget ansvar.

Efter NIS 1-direktivets artikel 14, stk. 4, skal der med henblik på at fastlægge omfanget af en hændelses konsekvenser navnlig tages følgende kriterier i betragtning: a) antallet af brugere, der berøres af afbrydelsen af den væsentlige tjeneste, b) hændelsens varighed og c) den geografiske udbredelse med hensyn til det område, der er berørt af hændelsen.

Det følger derudover af NIS 1-direktivets artikel 16, stk. 3, at medlemsstaterne sikrer, at udbydere af digitale tjenester hurtigst muligt foretager en underretning til den kompetente myndighed eller CSIRT af enhver hændelse, der har betydelige konsekvenser for leveringen af en tjeneste som omhandlet i bilag III, som de udbyder i Unionen. Underretninger skal indeholde oplysninger, der gør det muligt for den kompetente myndighed eller CSIRT at fastslå betydningen af eventuelle grænseoverskridende konsekvenser. Underretningen gør ikke den underrettende part genstand for et øget ansvar.

Af NIS 1-direktivets bilag III fremgår følgende tjenester: Onlinemarkedspladser, onlinesøgemaskiner og cloud computing-tjenester.

NIS 1-direktivet blev i dansk ret gennemført sektorvist i regulering gældende for de specifikke sektorer, hvor direktivet finder anvendelse. Der henvises til afsnit 2.4 i lovforslagets almindelige bemærkninger.

Det følger af det foreslåede *stk. 1,* at væsentlige og vigtige enheder skal underrette den relevante kompetente myndighed og Computer Security Incident Response Team (CSIRT) om enhver væsentlig hændelse. En underretning skal indeholde oplysninger, der gør det muligt at fastslå eventuelle grænseoverskridende virkninger af hændelsen.

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 væsentlige og vigtige enheder skal underrette både den relevante kompetente myndighed og CSIRT'en i tilfælde af hændelser, der har en væsentlig indvirkning på levering af deres tjenester. Dermed sikres det, at både den relevante kompetente myndighed og CSIRT'en hurtigt og effektivt vil kunne varetage sine myndighedsopgaver. Med den relevante kompetente myndighed forstås den, som i medfør af den foreslåede § 20 er udpeget som kompetent myndighed for en given sektor eller delsektor. Såfremt enheden leverer tjenester i flere sektorer, som påvirkes af hændelsen, skal enheden underrette de kompetente myndigheder i de pågældende sektorer. Det forudsættes, at underretningerne af de forskellige relevante myndigheder vil skulle foretages via en fælles digital indgang, såsom Virk.dk. Dette vil sikre, at de berørte enheder alene skal foretage én samlet underretning, som fordeles samtidigt til de relevante myndigheder.

I overensstemmelse med præambelbetragtning nr. 83 vil den foreslåede forpligtelse til at foretage underretning ved hændelser finde anvendelse på de væsentlige og vigtige enheder, uanset om disse enheder 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 enheds ansvar, at der sker underretning i fornødent omfang.

De nærmere oplysninger, der skal indgives i medfør af den foreslåede bestemmelse, fremgår af den foreslåede bestemmelse i § 13, stk. 1.

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. 2,* at en hændelse anses for at være væsentlig, hvis 1) den har forårsaget eller er i stand til at forårsage alvorlige driftsforstyrrelser af tjenesterne eller økonomiske tab for den berørte enhed, eller 2) den har påvirket eller er i stand til at påvirke andre fysiske eller juridiske personer ved at forårsage betydelig fysisk eller ikke fysisk skade.

Det følger af den foreslåede bestemmelse i *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 den foreslåede *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. 3,* at vedkommende minister efter forhandling med ministeren 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 det hensigtsmæssigt, at der gives mulighed for, at der sektorvist kan fastsættes nærmere regler om, hvornår en hændelse anses for at være væsentlig. De kompetente myndigheder vil herefter i særlige tilfælde kunne fastsætte nærmere regler om væsentlige hændelser inden for deres respektive sektor, som tager de fornødne hensyn. Med henblik på at sikre, at der ikke fastsættes indbyrdes modsatrettede regler, vil en ressortministers eventuelle fastsættelse af regler om væsentlige hændelser inden for sektoren skulle ske efter forhandling med ministeren for samfundssikkerhed og beredskab. Dette skal også ses som led i Ministeriet for Samfundssikkerheds koordinerende rolle, hvor ministeriet skal sikre en tæt koordination og samarbejde mellem tilsynsmyndighederne, herunder i forhold til tilsyn og håndhævelse.

Den foreslåede bestemmelse har således til formål at give den relevante ressortminister mulighed for efter behov at præcisere, under hvilke omstændigheder der skal foretages en underretning. Der vil eksempelvis kunne fastsættes kvantitative eller i øvrigt mere objektivt konstaterbare kriterier, der anses for nødvendige for den pågældende sektor. De regler, der kan fastsættes i medfør af det foreslåede stk. 3, vil således i givet fald præcisere den foreslåede bestemmelse i stk. 2, såfremt sektorspecifikke forhold tilsiger det.

Reguleringen i sektorvise bekendtgørelser vil muliggøre, at der kan tages højde for de særlige hensyn, der måtte gøre sig gældende i de enkelte sektorer. Samtidigt foreslås det, at bekendtgørelserne udstedes efter forhandling med ministeren for samfundssikkerhed og beredskab, således, at der – med respekt for de sektorvise forhold – i videst muligt omfang sikres ensartethed.

Det bemærkes, at Europa-Kommissionens gennemførelsesforordning (EU) 2024/2690 fastsætter de tekniske og metodologiske krav til de foranstaltninger, der er omhandlet i NIS 2-direktivets artikel 23, stk. 3, for så vidt angår DNS-tjenesteudbydere, topdomænenavneadministratorer og udbydere af cloudcomputingtjenester, at datacentertjenester, af indholdsleveringsnetværk, af administrerede tjenester, af administrerede sikkerhedstjenester, af on-linmarkedspladser af onlinesøgemaskiner og af platforme for sociale netværkstjenester og af tillidstjenester.

Europa-Kommissionen kan også vedtage sådanne gennemførelsesretsakter for så vidt angår andre væsentlige og vigtige enheder.

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, om underretning af myndighederne om hændelser.

Det vil til enhver tid skulle sikres, at bekendtgørelser, der er udstedt 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.

Der henvises i øvrigt til pkt. 3.3 i lovforslagets almindelige bemærkninger.

Til § 13

Det følger af artikel 14, stk. 3, i 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), at medlemsstaterne sikrer, at operatører af væsentlige tjenester hurtigst muligt foretager en underretning til den kompetente myndighed eller CSIRT af hændelser, der har væsentlige konsekvenser for kontinuiteten af de væsentlige tjenester, som de leverer. Underretningerne skal indeholde oplysninger, der gør det muligt for den kompetente myndighed eller CSIRT at fastslå eventuelle grænseoverskridende konsekvenser af hændelsen. Underretning gør ikke den underrettende part til genstand for et øget ansvar.

Efter NIS 1-direktivets artikel 14, stk. 4, skal der med henblik på at fastlægge omfanget af en hændelses konsekvenser navnlig tages følgende kriterier i betragtning: a) antallet af brugere, der berøres af afbrydelsen af den væsentlige tjeneste, b) hændelsens varighed og c) den geografiske udbredelse med hensyn til det område, der er berørt af hændelsen.

Det følger af NIS 1-direktivets artikel 14, stk. 5, 2. led, at hvis omstændighederne tillader det, leverer den kompetente myndighed eller CSIRT relevante oplysninger til den underrettende operatør af væsentlige tjenester vedrørende opfølgningen af dennes underretning, som f.eks. oplysninger, der kan støtte en effektiv håndtering af hændelsen.

Det følger desuden af NIS 1-direktivets artikel 16, stk. 3, at medlemsstaterne sikrer, at udbydere af digitale tjenester hurtigst muligt foretager en underretning til den kompetente myndighed eller CSIRT af enhver hændelse, der har betydelige konsekvenser for leveringen af en tjeneste som omhandlet i bilag III, som de udbyder i Unionen. Underretninger skal indeholde oplysninger, der gør det muligt for den kompetente myndighed eller CSIRT at fastslå betydningen af eventuelle grænseoverskridende konsekvenser. Underretningen gør ikke den underrettende part genstand for et øget ansvar.

NIS 1-direktivet blev i dansk ret gennemført sektorvist i regulering gældende for de specifikke sektorer, hvor direktivet finder anvendelse. For en nærmere gennemgang af den sektorvise implementering af NIS 1-direktivet henvises til afsnit 2.4 i lovforslagets almindelige bemærkninger.

Der følger af den foreslåede *§ 13, stk. 1,* at underretning efter § 12, stk. 1, 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 under alle omstændigheder inden for 24 timer efter, at enheden 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 under alle omstændigheder inden for 72 timer efter, at enheden har fået kendskab til den væsentlige hændelse, jf. dog stk. 2, 3) en foreløbig rapport med relevante statusopdateringer sendes efter anmodning fra CSIRT'en, 4) en endelig rapport sendes 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) såfremt hændelsen fortsat pågår på tidspunktet for fremsendelsen af den endelige rapport, jf. nr. 4, skal den berørte enhed forelægge en statusrapport på det pågældende tidspunkt og en endelig rapport senest en måned efter, at hændelsen er håndteret.

Bestemmelsen vil gennemføre artikel 23, stk. 4, i NIS 2-direktivet.

Artikel 23, stk. 4, fastsætter, at medlemsstaterne sikrer, at de berørte enheder med henblik på den i artikel 23, stk. 1, omhandlede underretning fremsender følgende til CSIRT'en eller i givet fald den kompetente myndighed: a) uden unødigt ophold og under alle omstændigheder inden for 24 timer efter at have fået kendskab til den væsentlige hændelse en tidlig varsling, som i givet fald skal angive, om den væsentlige hændelse mistænkes for at være forårsaget af ulovlige eller ondsindede handlinger eller kunne have en grænseoverskridende virkning, b) uden unødigt ophold og under alle omstændigheder inden for 72 timer efter at have fået kendskab til den væsentlige hændelse, en hændelsesunderretning, som i givet fald skal ajourføre de oplysninger, der er omhandlet under litra a, og give en indledende vurdering af den væsentlige hændelse, herunder dens alvor og indvirkning samt kompromitteringsindikatorerne, hvor sådanne foreligger, c) efter anmodning fra en CSIRT eller den kompetente myndighed en foreløbig rapport om relevante statusopdateringer, d) en endelig rapport senest en måned efter forelæggelsen af den i litra b omhandlede hændelsesunderretning, der skal omfatte følgende: i) En detaljeret beskrivelse af hændelsen, herunder dens alvor og indvirkning, ii) den type trussel eller grundlæggende årsag, der sandsynligvis har udløst hændelsen, iii) anvendte og igangværende afbødende foranstaltninger og iv) i givet fald de grænseoverskridende virkninger af hændelsen og e) i tilfælde af at en hændelse pågår på tidspunktet for indgivelsen af den i litra d, omhandlede endelige rapport, sikrer medlemsstaterne, at berørte enheder forelægger en statusrapport på det pågældende tidspunkt og en endelig rapport senest en måned efter deres håndtering af hændelsen.

Den foreslåede bestemmelse svarer med enkelte sproglige tilpasninger uden indholdsmæssig betydning til NIS 2-direktivets artikel 23, stk. 4, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

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

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 enheder 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 under alle omstændigheder 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 enhed vil skulle sende en endelig rapport senest en måned efter forelæggelsen af hændelsesunderretningen efter den foreslåede § 13, 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 enhed 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 tik at sende en endelig rapport senest én måned efter, at hændelsen er håndteret.

Det følger af det foreslåede *stk. 2,* at tillidstjenesteudbydere i tilfælde af væsentlige hændelser skal afgive underretningen efter stk. 1, nr. 2, uden unødigt ophold og senest inden for 24 timer efter at være blevet bekendt med den væsentlige hændelse.

Den foreslåede bestemmelse vil gennemføre NIS 2-direktivets artikel 23, stk. 4, sidste pkt., som fastsætter, at tillidstjenesteudbydere for så vidt angår væsentlige hændelser, der har en virkning på leveringen af dens tillidstjeneste, skal underrette CSIRT'en eller i givet fald den kompetente myndighed uden unødigt ophold og under alle omstændigheder inden for 24 timer efter at være blevet bekendt med den væsentlige hændelse.

Den foreslåede bestemmelse svarer med enkelte sproglige tilpasninger uden indholdsmæssig betydning til NIS 2-direktivets artikel 23, stk. 4, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Den foreslåede bestemmelse indebærer, at tillidstjenesteudbydere skal indgive hændelsesunderretningen på et tidligere

tidspunkt end den frist på maksimalt 72 timer, som gælder for andre typer af enheder.

Det følger af det foreslåede *stk. 3,* at CSIRT'en sikrer, at den underrettende enhed uden unødigt ophold og, hvor det er muligt, 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 enheden skal CSIRT'en desuden yde vejledning, operativ rådgivning om gennemførelsen af mulige afbødende foranstaltninger og supplerende teknisk bistand.

Den foreslåede bestemmelse vil gennemføre NIS 2-direktivets artikel 23, stk. 5, som bl.a. fastsætter, at CSIRT'en eller den 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 enhed anmoder herom. Hvor den væsentlige hændelse mistænkes for at være af strafferetlig karakter, giver CSIRT'en eller den kompetente myndighed 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 enhederne, og i denne forbindelse give indledende tilbagemeldinger om den væsentlige hændelse.

Svar og tilbagemeldinger vil kunne gives af CSIRT'en selv, en kompetent myndighed. Svar og tilbagemeldinger vil bl.a. kunne bestå i, at der gives vejledning om mulige afværgeforanstaltninger, om anden relevant viden, som CSIRT'en eller den myndighed, der afgiver svaret, 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 den myndighed, som afgiver svaret, skal tilvejebringe oplysninger fra tredjemand.

Efter bestemmelsen vil CSIRT'en desuden efter anmodning fra enheden skulle yde vejledning, operativ rådgivning om gennemførelsen af mulige afbødende foranstaltninger eller supplerende teknisk bistand, jf. også den foreslåede § 17.

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.

Der henvises i øvrigt til lovforslagets pkt. 3.3.

Til § 14

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), indeholder ikke nærmere regler om, at fysiske eller juridiske personer anonymt kan rapportere om sårbarheder til myndighederne.

Det følger af § 8, 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, at myndigheder og virksomheder kan underrette Styrelsen for Samfundssikkerhed (tidligere Center for Cybersikkerhed) om hændelser, der negativt påvirker eller vurderes at ville kunne påvirke tilgængelighed, integritet eller fortrolighed af data, informationssystemer, digitale netværk eller digitale servicer.

Det følger af § 8, stk. 2, i lov om sikkerhed i net og tjenester, at underretninger efter stk. 1 er undtaget fra aktindsigt efter lov om offentlighed i forvaltningen og partsaktindsigt efter forvaltningsloven.

Det følger af det foreslåede *stk. 1*, at offentlige og private enheder uanset, at de ikke er omfattet af lovens anvendelsesområde, kan underrette CSIRT'en om hændelser, nærvedhændelser og cybertrusler.

Den foreslåede bestemmelse vil indebære en videreførelse med de fornødne tilpasninger af den gældende bestemmelse i § 8, stk. 1, i lov om sikkerhed i net og tjenester.

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.

Underretning af CSIRT'en ved større sikkerhedshændelser skaber gode forudsætninger for, at CSIRT'en 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. Underretninger sætter således CSIRT'en i stand til at varsle hurtigere om trusler og styrke grundlaget for rådgivningen om risici og passende sikkerhedstiltag.

Den foreslåede bestemmelse vil indebære, at alle offentlige og private enheder uanset, at de ikke er omfattet af lovens

anvendelsesområde kan underrette CSIRT'en om hændelser, nærvedhændelser og cybertrusler.

Det følger af den foreslåede *stk. 2,* at CSIRT'en behandler underretninger efter stk. 1 på samme måde som underretninger modtaget i medfør af § 13. CSIRT'en kan prioritere håndteringen af underretninger, der er modtaget i medfør af § 13 fremfor underretninger efter 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 vil skulle behandle frivillige underretninger, der er indgivet i medfør af den foreslåede bestemmelse i § 14, stk. 1, efter procedurebestemmelsen i den foreslåede § 13. De forpligtelser for myndigheder, der er angivet i § 13 og bemærkningerne hertil, vil således også gælde for underretninger, der indgives i medfør af den foreslåede bestemmelse i § 14, stk. 1.

Det bemærkes, at den foreslåede bestemmelse ikke indebærer, at enheden er forpligtet til at følge proceduren efter den foreslåede bestemmelse i § 13, når der indgives underretning efter den foreslåede § 14, stk. 1.

Den foreslåede bestemmelse indebærer desuden, at CSIRT'en kan prioritere at håndtere de underretninger, der er modtaget i medfør af § 12, før CSIRT'en behandler de underretninger, der er modtaget i medfør af § 14, stk. 1.

Det følger af det foreslåede *stk. 3*, at underretninger efter stk. 1 er undtaget fra aktindsigt efter lov om offentlighed i forvaltningen og partsaktindsigt efter forvaltningsloven.

Den foreslåede bestemmelse vil videreføre af den gældende § 8, stk. 2, i lov om sikkerhed i net og tjenester.

Særligt for virksomheder kan oplysninger om, at der f.eks. er gennemført et vellykket hackerangreb, hvor virksomheden har mistet data, i høj grad skade virksomhedens omdømme, og det kan i praksis afholde mange virksomheder fra frivilligt at underrette CSIRT'en om et sådant hackerangreb. Derfor foreslås det med bestemmelsen, at underretningerne i deres helhed undtages fra aktindsigt, herunder partsaktindsigt efter forvaltningsloven. Undtagelsen kan omfatte underretningssagen som helhed. Der henvises til Folketingstidende 2015-16, tillæg A, L 10 som fremsat, side 22.

Undtagelsen fra aktindsigt omfatter derimod ikke virksomheders adgang til at gøre sig bekendt med oplysninger, der vedrører deres egne forhold. Dette gælder allerede i dag. Der henvises til Folketingstidende 2015-16, tillæg A, L 10 som fremsat, side 22.

Det bemærkes, at bestemmelsens anvendelsesområde er begrænset til at omfatte de frivillige underretninger, der modtages i medfør af § 14, stk. 1. De obligatoriske underretninger i medfør af § 12, vil således ikke være omfattet af den foreslåede undtagelsesbestemmelse.

Til § 15

Der var ikke i NIS 1-direktivet fastsat nærmere bestemmelser, der regulerede, i hvilket omfang operatører af væsentlige tjenester skulle underrette modtagerne af deres tjenester om væsentlige hændelser, der påvirker de tjenester, som operatørerne leverede.

Det følger af det foreslåede *stk. 1,* at væsentlige og vigtige uden unødigt ophold underretter modtagerne af deres tjenester om væsentlige hændelser, der sandsynligvis vil påvirke leveringen af deres tjenester negativt.

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.

Bestemmelsen vil indebære en forpligtelse for enhederne til at underrette modtagerne af deres tjenester om en væsentlig hændelse. Underretning af modtagerne vil alene skulle ske i relevant omfang. Det indebærer, at enhederne 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 § 12, stk. 2, og ud fra regler, der måtte være udstedt i en given sektor i medfør af § 12, stk. 3.

Der stilles ingen formkrav til underretningen, og de pågældende enheder 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,* at væsentlige og vigtige enheder uden unødigt ophold oplyser modtagerne af deres tjenester, som potentielt er berørt af en væsentlig cybertrussel, om eventuelle foranstaltninger og modforanstaltninger, som modtagerne kan træffe som reaktion på den pågældende trussel. Hvor det er relevant, skal enhederne også informere de pågældende modtagere om 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.

Den foreslåede bestemmelse vil i overensstemmelse med NIS 2-direktivets præambelbetragtning nr. 103 indebære, 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 cybertrussel. Enhederne vil desuden, hvor det er hensigtsmæssigt, og navnlig hvor den væsentlige cybertrussel sandsynligvis vil indtræde, skulle informere deres tjenestemodtagere om selve truslen. Kravet om at informere modtagerne om væsentlige cybertrusler bør opfyldes efter bedste evne, men vil ikke fritage enhederne for forpligtelsen til at træffe passende og øjeblikkelige foranstaltninger til at forebygge eller afhjælpe enhver trussel og genoprette tjenestens normale sikkerhedsniveau, jf. den foreslåede bestemmelse i § 6, stk. 1.

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

Der vil i øvrigt ikke blive stillet formkrav til oplysningen, og de pågældende enheder vil derfor have metodefrihed i forhold til, hvordan underretningen af modtagerne vil skulle ske.

Der henvises i øvrigt til pkt. 3.3 i lovforslagets almindelige bemærkninger.

Til § 16

Efter artikel 14, stk. 6, i NIS 1-direktivet, kunne den kompetente myndighed eller CSIRT'en efter høring af den underrettende operatør af væsentlige tjenester CSIRT'en oplyse offentligheden om konkrete hændelser, hvis offentlighedens kendskab hertil var nødvendig for at forebygge en hændelse eller håndtere en igangværende hændelse.

Det fulgte endvidere af artikel 16, stk. 7, i NIS 1-direktivet, at efter høring af udbyderen af de digitale tjenester kunne den kompetente myndighed eller CSIRT'en og, hvis det er relevant, myndighederne eller CSIRT'erne i andre berørte medlemsstater oplyse offentligheden om konkrete hændelser eller kræve, at udbyderen af digitale tjenester gør det, hvis offentlighedens kendskab hertil er nødvendigt for at forebygge en hændelse eller håndtere en igangværende hændelse, eller hvis offentliggørelse af hændelsen i øvrigt er i offentlighedens interesse.

NIS 1-direktivet blev i dansk ret gennemført sektorvist i regulering gældende for de specifikke sektorer, hvor direktivet finder anvendelse. For en nærmere gennemgang af den sektorvise implementering af NIS 1-direktivet henvises til lovforslagets pkt. 2.4.

Det følger af den foreslåede *stk. 1,* at den relevante kompetente myndighed efter høring af en enhed, der er ramt af en væsentlig hændelse kan informere offentligheden om den væsentlige hændelse, hvis offentliggørelsen er nødvendig for at forebygge videre udbredelse af 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 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 i stk. 1 vil indebære, at den relevante kompetente myndighed 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.

Den relevante kompetente myndighed vil i medfør af bestemmelsen skulle høre den berørte enhed, før der sker offentliggørelse af hændelsen.

Formålet med høringen vil være at sikre, at den kompetente myndighed 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 den kompetente myndighed at tage stilling til formen for orienteringen. Orientering af offentligheden kan således ske på den måde, som den kompetente myndighed 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 den relevante kompetente myndighed, og ikke CSIRT'en, der foretager offentliggørelsen af en væsentlig hændelse, jf. dog det foreslåede stk. 3, idet den kompetente myndighed vil være nærmest til at foretage afvejningen af enhedens eventuelle interesse i, at der ikke sker offentliggørelse, over for hensynet til offentligheden.

Det følger af den foreslåede bestemmelse i *stk. 2*, at den kompetente myndighed i de situationer, der er nævnt i stk. 1, kan kræve, at den relevante enhed informerer offentligheden om en væsentlig hændelse.

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 relevante kompetente myndighed vil efter den foreslåede bestemmelse skulle foretage høring af den berørte enhed, før der træffes afgørelse om, at enheden 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 vil indebære, 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 enhed, før der træffes afgørelse om, at enheden 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.

Herudover forudsættes det, at der sker en tæt koordination mellem CSIRT'en og de relevante kompetente myndigheder 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 betydningtil NIS 2-direktivets artikel 23, stk. 7, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Den foreslåede bestemmelse vil indebære, at CSIRT'en efter høring af en enhed i en anden medlemsstat, hvor enheden er ramt af en væsentlig hændelse, vil kunne informere offentligheden i Danmark om den væsentlige hændelse.

Det vil være 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 enheden skal offentliggøre hændelsen, vil CSIRT'en skulle foretage høring af den berørte enhed i overensstemmelse med proceduren beskrevet i bemærkningerne til det foreslåedes stk. 1. Det forudsættes dog, at høringen af enheden 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.

Der henvises i øvrigt til lovforslagets pkt. 3.3.

Til § 17

Det følger af bilag 1, nr. 2, i NIS 1-direktivet, at CSIRT'ers opgaver som minimum skal omfatte følgende: 1) Monitorering af hændelser på nationalt plan, 2) tidlig varsling, advarsler, meddelelser og formidling af information til relevante interessenter om risici og hændelser, 3) at reagere på hændelser, 4) udarbejdelse af dynamiske risiko- og hændelsesanalyser og situationsrapporter og 5) deltagelse i CSIRT-netværket.

NIS 1-direktivet blev i dansk ret gennemført sektorvist i regulering gældende for de specifikke sektorer, hvor direktivet finder anvendelse. For en nærmere gennemgang af den sektorvise implementering af NIS 1-direktivet henvises til lovforslagets pkt. 2.4.

Det følger af lov om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter, jf. lov nr. 437 af 8. maj 2018, at netsikkerhedstjenesten i dag varetager de tværgående opgaver som CSIRT og centralt kontaktpunkt efter NIS 1-direktivet.

Det følger af den foreslåede *stk. 1,* at CSIRT'en håndterer it-sikkerhedshændelser og varetager de opgaver, der relaterer sig hertil, herunder følgende opgaver i forhold til væsentlige og vigtige enheder: 1) efter anmodning fra en væsentlig eller vigtig enhed at yde bistand vedrørende realtids- eller nærrealtidsmonitorering af enhedens net- og informationssystemer, 2) at reagere på hændelser og i givet fald yde bistand til de berørte enheder og 3) efter anmodning fra en væsentlig eller vigtig enhed at foretage en proaktiv scanning af enhedens net- og informationssystemer, der anvendes til levering af enhedens tjenester, for at opdage sårbarheder med en potentielt væsentlig indvirkning.

Den foreslåede bestemmelse vil gennemføre artikel 11, stk. 3, i 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).

Det følger af NIS 2-direktivets artikel 11, stk. 3, 1. led, at CSIRT'erne har følgende opgaver: a) overvågning og analyse af cybertrusler, sårbarheder og hændelser på nationalt plan og efter anmodning ydelse af bistand til væsentlige og vigtige enheder vedrørende realtids- eller nærrealtidsovervågning af deres net- og informationssystemer, b) tidlig varsling, alarmer, meddelelser og formidling af oplysninger til berørte væsentlige og vigtige enheder samt til de kompetente myndigheder og andre relevante interessenter om cybertrusler, sårbarheder og hændelser, om muligt i nærrealtid, c) at reagere på hændelser og i givet fald yde bistand til de berørte væsentlige og vigtige enheder, d) at indsamle og analysere kriminaltekniske data og udarbejde dynamiske risiko- og hændelsesanalyser samt skabe situationsbevidsthed vedrørende cybersikkerhed, e) på anmodning af en væsentlig eller vigtig enhed at foretage en proaktiv scanning af den pågældende enheds net- og informationssystemer for at opdage sårbarheder med en potentielt væsentlig indvirkning, f) at deltage i CSIRT-netværket og yde gensidig bistand i overensstemmelse med deres kapacitet og kompetencer til andre medlemmer af CSIRT-netværket efter anmodning fra disse, g) i givet fald fungere som koordinator med henblik på den koordinerede offentliggørelse af sårbarheder i henhold til artikel 12, stk. 1, samt h) at bidrage til udbredelsen af sikre værktøjer til udveksling af oplysninger i henhold til direktivets artikel 10, stk. 3.

Efter NIS 2-direktivets artikel 11, stk. 3, 2. led, kan CSIRT'erne foretage proaktiv ikke-indgribende scanning af væsentlige og vigtige enheders offentligt tilgængelige net- og informationssystemer. En sådan scanning skal foretages for at opdage sårbare eller usikkert konfigurerede net- og informationssystemer og informere de berørte enheder. En sådan scanning må ikke have nogen negativ indvirkning på enhedernes tjenester.

Det følger endvidere af artikel 11, stk. 3, 3. led, at CSIRT'en ved udførelsen af de opgaver, der er omhandlet i første led (artikel 11, stk. 3, litra a-h, kan prioritere særlige opgaver på grundlag af en risikobaseret tilgang.

Den foreslåede bestemmelse svarer med sproglige tilpasninger uden indholdsmæssig betydning til NIS 2-direktivets artikel 11, stk. 3, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Bestemmelsen indebærer, at CSIRT'en håndterer it-sikkerhedshændelser og varetager de opgaver, der relaterer sig hertil. Det omfatter samtlige de opgaver, der fremgår af NIS 2-direktivets artikel 11, stk. 3. I det omfang CSIRT'ens opgaver indebærer rettigheder eller forpligtelser for enhederne, er de enkelte opgaver udtrykkeligt reguleret i bestemmelsens stk. 1, nr. 1-3.

Det følger af det foreslåede *nr. 1*, at CSIRT'en efter anmodning fra en væsentlig eller vigtig enhed yder bistand vedrørende realtids- eller nærrealtidsmonitorering af enhedens net- og informationssystemer.

Indholdet i den nærmere bistand vil blive besluttet af CSIRT'en og vil kunne variere afhængigt af de nærmere omstændigheder omkring anmodningen, herunder enhedens risikoeksponering, dens størrelse og samfundsmæssige betydning. Der vil eksempelvis kunne ydes bistand ved, at CSIRT'en giver råd og vejledning i forhold til specifikation af ydelser eller produkter, som enheden kan købe hos private leverandører.

Det følger af det foreslåede *nr. 2*, at CSIRT'en har til opgave at reagere på hændelser og i givet fald yde bistand til de berørte enheder.

Bistand skal forstås bredt og kan således omfatte rådgivning om afhjælpende foranstaltninger, herunder eventuelt råd og vejledning i forhold til specifikation af ydelser eller produkter, som enheden kan købe hos private leverandører, samt efter omstændighederne mere konkret teknisk bistand.

Bestemmelsen skal bl.a. ses i sammenhæng med den foreslåede § 13, stk. 3, som gennemfører artikel 23, stk. 5, i NIS 2-direktivet, og som fastsætter, at CSIRT'en – i forlængelse af, at en enhed indgiver en underretning til myndighederne om en væsentlig hændelse – giver den underrettende enhed et svar, herunder indledende tilbagemeldinger om den væsentlige hændelse og, efter anmodning fra enheden, vejledning, operativ rådgivning om gennemførelsen af mulige afbødende foranstaltninger og supplerende teknisk bistand.

Det følger af det foreslåede *nr. 3*, at CSIRT'en efter anmodning fra en væsentlig eller vigtig enhed foretager proaktiv scanning af enhedens net- og informationssystemer, der anvendes til levering af enhedens tjenester, for at opdage sårbarheder med en potentielt væsentlig indvirkning.

Det er Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at der ved NIS 2-direktivets anvendelse af begrebet »scanning« i direktivets artikel 11, stk. 3, litra e, må forstås både indgribende og ikke-indgribende scanninger. I NIS 2-direktivets artikel 11, stk. 3, 2. led, omtales således brugen af ikke-indgribende scanninger af enheders offentligt tilgængelige net- og informationssystemer uden at enheden har anmodet herom.

Den foreslåede bestemmelse indebærer dermed, at der kan foretages både indgribende og ikke-indgribende proaktive scanninger. Det er en betingelse for anvendelse af proaktive scanninger efter bestemmelsen, at enheden har anmodet herom.

CSIRT'en vil desuden, som omtalt i NIS 2-direktivets artikel 11, stk. 3, 2. led, jf. ovenfor, kunne foretage proaktiv ikke-indgribende scanninger af væsentlige og vigtige enheders offentligt tilgængelige net- og informationssystemer uden anmodning herom. I modsætning til scanningerne omfattet af den foreslåede bestemmelse i nr. 3 vil disse scanninger således være rettet mod enhedernes offentligt tilgængelige net- og informationssystemer. Henset hertil, og til at der er tale om ikke-indgribende scanninger, vurderes dette ikke at kræve udtrykkelig lovhjemmel.

Den foreslåede bestemmelse i stk. 1 indeholder en positiv hjemmel til udførelsen af de nævnte opgaver i relation til væsentlige og vigtige enheder. Der er således med bestemmelsen ikke tilsigtet en negativ afgrænsning ift. CSIRT'ens opgaver i øvrigt.

Det følger af det foreslåede *stk. 2,* at ved udførelsen af opgaver efter stk. 1 kan CSIRT'en prioritere særlige opgaver ud fra en risikobaseret tilgang.

Den foreslåede bestemmelse vil gennemføre NIS 2-direktivets artikel 11, stk. 3, sidste led, hvoraf det fremgår, at ved udførelsen af de opgaver, der er omhandlet i første led, kan CSIRT'erne prioritere særlige opgaver på grundlag af en risikobaseret tilgang.

Den foreslåede bestemmelse svarer indholdsmæssigt til dele af NIS 2-direktivets artikel 11, stk. 3, sidste led, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Bestemmelsen vil indebære, at CSIRT'en ud fra en risikobaseret tilgang vil kunne prioritere udførelsen af de i stk. 1 nævnte opgaver. CSIRT'en vil således ud fra en risikobaseret tilgang kunne prioritere på hvilken måde og i hvilken rækkefølge, opgaverne skal løses. CSIRT'en vil endvidere ud fra en prioritering af sine opgaver i særlige tilfælde kunne afvise en anmodning efter stk. 1. Der kan ved prioriteringen eksempelvis lægges vægt på en enheds risikoeksponering, dennes størrelse og samfundsmæssige betydning, samt CSIRT'ens arbejdspres og ressourcer.

Der henvises i øvrigt til lovforslagets pkt. 2.2.2.

Til § 18

NIS 1-direktivet indeholdte ikke nærmere regler om, at fysiske eller juridiske personer anonymt kunne rapportere om sårbarheder til myndighederne.

Det følger af det foreslåede *stk. 1,* at CSIRT'en sikrer, at fysiske og juridiske personer i anonymiseret form kan rapportere om sårbarheder.

Bestemmelsen vil gennemføre artikel 12, stk. 1, 2. led, 1. og 2. pkt., i 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), hvoraf det følger, at medlemsstaterne sikrer, at fysiske eller juridiske personer er i stand til at rapportere en sårbarhed anonymt, hvor de anmoder herom, til den CSIRT, der er udpeget som koordinator. Den CSIRT, der er udpeget som koordinator, sørger for omhyggelig opfølgning med hensyn til den rapporterede sårbarhed og sikrer anonymiteten for den fysiske eller juridiske person, der rapporterer sårbarheden.

Den foreslåede bestemmelse svarer indholdsmæssigt til NIS 2-direktivets artikel 12, stk. 1, 2. led, 1. og 2. pkt., og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Den foreslåede bestemmelse vil indebære en forpligtelse for CSIRT'en til at sikre, at det er muligt for fysiske og juridiske personer at rapportere om sårbarheder.

Bestemmelsen indebærer desuden en forpligtelse for CSIRT'en til at sikre, at de pågældende fysiske eller juridiske personer har muligheden for at indgive rapporteringen anonymt.

I overensstemmelse med NIS 2-direktivets artikel 12, stk. 1, 2. led, 2. pkt., vil CSIRT'en efter modtagelse af en anonym rapportering som led i sin opgavevaretagelse skulle sikre opfølgning på rapporteringen. Dette indebærer bl.a., at CSIRT'en så vidt muligt vil skulle identificere de enheder, der er berørte af sårbarheden, og kontakte dem med henblik på at få udbedret sårbarheden. Efter omstændighederne vil det endvidere være relevant for CSIRT'en at overveje, om der er grundlag for at orientere den relevante kompetente myndighed.

I overensstemmelse med NIS 2-direktivets artikel 12, stk. 1, 2. led, sidste pkt., vil CSIRT'en, hvis en rapporteret sårbarhed kan have væsentlig indvirkning på enheder i mere end én medlemsstat i Den Europæiske Union, skulle samarbejde med de andre medlemsstaters CSIRT'er igennem CSIRT-netværket.

Bestemmelsen vil ikke få betydning for om en handling, der ligger bag rapporteringen, måtte være strafbar. I det omfang en fysisk eller juridisk person f.eks. måtte have tilegnet sig information om den sårbarhed, der rapporteres om, på en måde, som efter anden lovgivning kan være strafbar, vil den pågældende således fortsat kunne straffes herfor.

Det følger af det foreslåede *stk. 2*, at ministeren for samfundssikkerhed og beredskab kan fastsætte nærmere regler om rapportering efter stk. 1.

Der vil bl.a. kunne fastsættes nærmere regler om, hvordan rapporteringen skal foregå, herunder om denne skal foretages digitalt, hvordan CSIRT'en nærmere skal håndtere en rapportering, samt i hvilket omfang CSIRT'en kan dele oplysningerne med andre.

Til § 19

NIS 1-direktivet fastsatte ikke nærmere regler om enhedernes frivillige indbyrdes udveksling af cybersikkerhedsoplysninger mv.

Det følger af det foreslåede *stk. 1,* at CSIRT'en faciliterer, at der på frivillig basis kan ske udveksling af oplysninger mellem enheder i cybersikkerhedsfællesskaber.

Bestemmelsen vil gennemføre artikel 29, stk. 1 og 2 i NIS 2-direktivet.

Det følger af NIS 2-direktivets artikel 29, stk. 1, at medlemsstaterne sikrer, at enheder, der er omfattet af direktivets anvendelsesområde, og, hvor det er relevant, andre enheder, der ikke er omfattet af direktivets anvendelsesområde, på frivillig basis er i stand til at udveksle relevante cybersikkerhedsoplysninger indbyrdes, herunder oplysninger om cybertrusler, nærvedhændelser, sårbarheder, teknikker og procedurer, kompromitteringsindikatorer, fjendtlige taktikker, specifikke oplysninger vedrørende trusselsaktører, cybersikkerhedsadvarsler og anbefalinger vedrørende konfiguration af cybersikkerhedsværktøjer til opdagelse af cyberangreb, hvor sådan udveksling af oplysninger a) har til formål at forebygge, opdage, reagere på eller reetablere sig efter hændelser eller afbøde deres virkninger og b) øger cybersikkerhedsniveauet, navnlig ved at øge bevidstheden om cybertrusler, begrænse eller hindre sådanne truslers evne til at sprede sig, støtte en række forsvarskapaciteter, afhjælpe og offentliggøre sårbarheder, teknikker til opdagelse, begrænsning og forebyggelse af trusler, afbødningsstrategier eller indsats- og genopretningsfaser eller fremme samarbejde mellem offentlige og private enheder om forskning i trusler.

Efter NIS 2-direktivets artikel 29, stk. 2, skal medlemsstaterne sikre, at udvekslingen af oplysninger finder sted inden for fællesskaber af væsentlige og vigtige enheder og, hvor det er relevant, deres leverandører eller tjenesteudbydere. En sådan udveksling skal gennemføres ved hjælp af ordninger for udveksling af cybersikkerhedsoplysninger for så vidt angår den potentielt følsomme karakter af de udvekslede oplysninger.

Den foreslåede bestemmelse svarer med sproglige tilpasninger uden indholdsmæssig betydningtil NIS 2-direktivets arti-

kel 29, stk. 2, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Det fremgår af NIS 2-direktivets præambelbetragtning nr. 119 og 120, at baggrunden for bestemmelserne i artikel 29 er, at oprettelsen af cybersikkerhedsfællesskaber vil sikre grundlaget for, at der kan ske en regelmæssig udveksling af trussels- og sårbarhedsefterretninger mellem enhederne, hvilket kan styrke deres evne til at opdage cybertrusler og træffe effektive forebyggelsesforanstaltninger. Det vil i disse cybersikkerhedsfællesskaber således være muligt for enhederne at udveksle viden og praktisk erfaring på et strategisk, taktisk og operationelt plan med henblik på at styrke deres individuelle kapacitet til i tilstrækkeligt omfang at forebygge, opdage, reagere på eller reetablere sig efter hændelser eller afbøde deres virkninger. Det er derfor nødvendigt at gøre det muligt på EU-plan at etablere frivillige ordninger for udveksling af cybersikkerhedstjenester og -forskning, samt relevante enheder, der ikke er omfattet af NIS 2-direktivets anvendelsesområde til at deltage i sådanne ordninger for udveksling af cybersikkerhedsoplysninger. Disse ordninger bør etableres i overensstemmelse med EU-konkurrencereglerne og EU-databeskyttelsesretten.

På den baggrund er det Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at artikel 29, stk. 1 og 2, primært stiller krav til medlemsstaternes facilitering af cybersikkerhedsfællesskaber med henblik på enhedernes indbyrdes udveksling af oplysninger, og at der således ikke har været tiltænkt en begrænsning i forhold til enhedernes indbyrdes frivillige udveksling af cybersikkerhedsoplysninger i andre fora.

Den foreslåede bestemmelse indebærer dermed en forpligtelse for CSIRT'en til at facilitere, at der oprettes et eller flere cybersikkerhedsfællesskaber, hvor enheder på frivillig basis kan udveksle oplysninger med hinanden.

Det bemærkes i den forbindelse, at enheder som deltager i et eller flere cybersikkerhedsfællesskaber og udveksler oplysninger skal iagttage EU-konkurrencereglerne og EU-databeskyttelsesretten, herunder Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) artikel 6, om lovlig behandling.

Den foreslåede bestemmelse i § 19, stk. 1, omfatter alle enheder og dermed også enheder, der ikke anses for at være væsentlige eller vigtige enheder. Det er dog en forudsætning, at enhederne hører under dansk jurisdiktion, jf. den foreslåede bestemmelse i § 2.

Det følger af det foreslåede *stk. 2,* at væsentlige og vigtige enheder, der indgår i eller udtræder af cybersikkerhedsfællesskaber efter stk. 1, skal underrette den kompetente myndighed herom.

Bestemmelsen vil gennemføre NIS 2-direktivets artikel 29, stk. 4, hvoraf det følger, at medlemsstaterne sikrer, at væsentlige og vigtige enheder underretter de kompetente myndigheder om deres deltagelse i de i stk. 2 omhandlede ordninger for udveksling af cybersikkerhedsoplysninger, når de indtræder i sådanne ordninger, eller i givet fald om deres udtræden af sådanne ordninger, når denne udtræden træder i kraft.

Den foreslåede bestemmelse svarer med sproglige tilpasninger uden indholdsmæssig betydning til NIS 2-direktivets artikel 29, stk. 4, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Den foreslåede bestemmelse indebærer en forpligtelse for væsentlige og vigtige enheder til at underrette den relevante kompetente myndighed, når de indgår i eller udtræder af de cybersikkerhedsfællesskaber, som CSIRT'en faciliterer efter stk. 1.

Forpligtelsen til at underrette den relevante kompetente myndighed, når enheden indtræder eller udtræder af et cybersikkerhedsfællesskab, vil ikke gælde for enheder, der alene er omfattet af lovens anvendelsesområde som følge af den foreslåede bestemmelse i § 1, stk. 6.

Til § 20

Det fremgik af artikel 8, stk. 1, i NIS 1-direktivet, at hver medlemsstat udpeger en eller flere nationale kompetente myndigheder for sikkerheden i net- og informationssystemer, som mindst omfatter de sektorer, der fremgår af direktivets bilag I, og de tjenester, der er omhandlet i direktivets bilag II. Efter artikel 8, stk. 2, fører de kompetente myndigheder tilsyn med anvendelsen af NIS 1-direktivet på nationalt plan.

NIS 1-direktivet indeholder ikke nærmere bestemmelser, der regulerer tilsynsmyndigheders operationelle uafhængighed.

NIS 1-direktivet blev i dansk ret gennemført sektorvist i regulering gældende for de specifikke sektorer, hvor direktivet finder anvendelse. For en nærmere gennemgang af den sektorvise gennemførelse af NIS 1-direktivet henvises til lovforslagets pkt. 2.4.

Det følger af det foreslåede *stk. 1,* at ministeren for samfundssikkerhed og beredskab efter forhandling med vedkommende minister fastsætter regler om, hvilken myndighed der skal varetage funktionen som kompetent myndighed inden for en given sektor eller delsektor eller for en bestemt enhed, jf. lovens bilag 1 eller 2. Ministeren for samfundssikkerhed og beredskab kan efter forhandling med den minister, som anvender bemyndigelsen i § 1, stk. 6, fastsætte regler om hvilken myndighed, der skal varetage funktionen som kompetent myndighed for disse enheder.

Som led i implementeringen af NIS 2-direktivet vil det påhvile ministeren for samfundssikkerhed og beredskab – efter forhandling med de relevante ressortministerier – at oprette eller udpege kompetente myndigheder for de enkelte sekto-

rer i lovens bilag. Det følger således af direktivets artikel 8, stk. 1 og 2, at hver medlemsstat udpeger eller opretter en eller flere kompetente myndigheder med ansvar for cybersikkerhed og for de tilsynsopgaver, der er omhandlet i direktivets kapitel VII (tilsyn og håndhævelse), og at de kompetente myndigheder fører tilsyn med gennemførelsen af direktivet på nationalt plan.

Den foreslåede bestemmelse vil indebære, at ministeren for samfundssikkerhed og beredskab ved bekendtgørelse vil kunne fastsætte regler om, hvilken myndighed der skal varetage funktionen som kompetent myndighed inden for de enkelte sektorer. Dermed vil der hurtigt og smidigt kunne ske justeringer, såfremt der måtte ske ændringer i arbejdsfordelingen mellem myndigheder på områder, samtidig med at det vil være tydeligt for enhederne, hvilken myndigheds tilsyn de er underlagt. Der vil kunne blive udpeget én eller flere kompetente myndigheder inden for en sektor eller delsektor.

Der henvises i øvrigt til lovforslagets pkt. 2.2.2 om nationale myndigheder og samarbejde.

Det følger af den foreslåede *stk. 2,* at for at sikre operationel uafhængighed ved tilsyn med den offentlige forvaltning kan ministeren for samfundssikkerhed og beredskab efter forhandling med en anden minister fastsætte regler om, at tilsyn med Ministeriet for Samfundssikkerhed og Beredskab og underliggende myndigheder helt eller delvist overlades til den pågældende minister.

Den foreslåede bestemmelse vil gennemføre artikel 31, stk. 4, i NIS 2-direktivet. Det følger af artikel 31, stk. 4, at uden at det berører nationale lovgivningsmæssige og institutionelle rammer sikrer medlemsstaterne, at de kompetente myndigheder ved tilsynet med offentlige forvaltningsenheders overholdelse af dette direktiv og indførelsen af håndhævelsesforanstaltninger for så vidt angår overtrædelser af dette direktiv, har passende beføjelser til at udføre sådanne opgaver med operationel uafhængighed i forhold til de offentlige forvaltningsenheder, der føres tilsyn med. Medlemsstaterne kan beslutte at indføre passende, forholdsmæssige og effektive tilsyns- og håndhævelsesforanstaltninger over for disse enheder i overensstemmelse med de nationale lovgivningsmæssige og institutionelle rammer.

Det er Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at artikel 31, stk. 4, bl.a. indebærer, at det skal sikres, at tilsynet med den offentlige sektor er operationelt uafhængigt. Der er således en forpligtelse for medlemsstaterne til at sikre, at den myndighed, der skal føre tilsyn med den offentlige sektor, er uafhængig af de offentlige myndigheder, som den fører tilsyn med, og som den træffer afgørelser over for.

Ved den danske gennemførelse af NIS 2-direktivet vil tilsynet med den statslige del af den offentlige forvaltning høre under ministeren for samfundssikkerhed og beredskabs ressort. Dermed kan der potentielt opstå en situation, hvor der ikke er operationel uafhængighed.

Med henblik på at sikre den operationelle uafhængighed, vurderes det nødvendigt at indføre en bestemmelse om, at tilsynet med Ministeriet for Samfundssikkerhed og Beredskab samt underliggende myndigheder helt eller delvist kan overlades til en anden minister. Dette vil sikre, at tilsynsmyndigheden for den offentlige sektor ikke skal føre tilsyn med sig selv eller med en overordnet myndighed, som har instruksbeføjelse over for tilsynsmyndigheden. Dette vil sikre overensstemmelse med NIS 2-direktivets artikel 31, stk. 4.

Den foreslåede bestemmelse vil omfatte tilsynet, herunder kompetencen til at træffe afgørelser, der er relateret til tilsynet. Den pågældende minister vil herefter kunne delegere tilsynsopgaven til en eller flere af de myndigheder, der hører under ministerens ressort.

Det foreslås i *stk. 3,* at ministeren for samfundssikkerhed og beredskab kan fastsætte regler om koordinering, ansvar, fordeling af opgaver og udveksling af oplysninger mellem de kompetente myndigheder, samt de kompetente myndigheder og CSIRT'en, herunder i forhold til hændelsesunderretninger efter kapitel 3 og tilsyn samt håndhævelse efter kapitel 6.

Bemyndigelsesbestemmelsen har til formål at give ministeren for samfundssikkerhed og beredskab mulighed for at fastsætte nærmere regler om ansvarsdelingen og samarbejdet mellem de kompetente myndigheder, samt de kompetente myndigheder og CSIRT'en.

Bemyndigelsesbestemmelsen skal ses i lyset af, at Ministeriet for Samfundssikkerhed og Beredskab har en koordinerende rolle i forbindelse med implementeringen af NIS 2-direktivet. Heri ligger bl.a., at ministeriet har ansvaret for at varetage en række tværgående, rådgivende og koordinerende funktioner, herunder i forhold til at sikre vejledning om udmøntningen af direktivets krav og forpligtelser på tværs af ressortministerierne.

Til § 21

Det følger af artikel 15, stk. 1, i NIS 1-direktivet, at medlemsstaterne sikrer, at de kompetente myndigheder har de nødvendige beføjelser og midler til at vurdere, hvorvidt operatører af væsentlige tjenester opfylder deres forpligtelser i medfør af artikel 14 (sikkerhedskrav og underretning om hændelser) og virkningerne heraf på net- og informationssystemers sikkerhed. Efter artikel 15, stk. 2, skal medlemsstaterne sikre, at de kompetente myndigheder har beføjelser til at pålægge operatører af væsentlige tjenester at levere a) de oplysninger, der er nødvendige for at vurdere sikkerheden i deres net- og informationssystemer, herunder dokumenterede sikkerhedspolitikker, og b) dokumentation for den faktiske gennemførelse af sikkerhedspolitikker, som f.eks. resultaterne af en sikkerhedsaudit udført af den kompetente myndighed eller en kvalificeret auditør og i sidstnævnte til-

fælde stille resultaterne heraf, herunder den tilgrundliggende dokumentation, til rådighed for den kompetente myndighed.

For så vidt angår udbydere af digitale tjenester, følger det af NIS 1-direktivets artikel 17, stk. 1, at medlemsstaterne sikrer, at de kompetente myndigheder om nødvendigt griber ind ved hjælp af efterfølgende tilsynsforanstaltninger, når det kan dokumenteres, at en udbyder af digitale tjenester ikke opfylder kravene i direktivets artikel 16 (sikkerhedskrav og underretning om hændelser).

Efter artikel 17, stk. 2, skal de kompetente myndigheder tillægges de fornødne beføjelser og midler til at pålægge udbydere af digitale tjenester at: a) Forelægge de oplysninger, der er nødvendige for at vurdere sikkerheden af deres net- og informationssystemer, herunder dokumenterede sikkerhedspolitikker og b) afhjælpe mangler i opfyldelsen af de krav, der er fastsat i artikel 16.

NIS 1-direktivet blev i dansk ret gennemført sektorvist i regulering gældende for de specifikke sektorer, hvor direktivet finder anvendelse. For en nærmere gennemgang af den sektorvise gennemførelse af NIS 1-direktivet henvises til lovforslagets pkt. 2.4.

Det foreslås i *stk. 1,* at de kompetente myndigheder 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 enhed.

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.

Det foreslås med *nr. 1,* at de kompetente myndigheder uden retskendelse of mod behørig legitimation kan foretage kontrol på stedet og eksternt tilsyn, herunder foretage stikprøvekontroller.

Den foreslåede bestemmelse vil gennemføre artikel 32, stk. 1 og 2, i NIS 2-direktivet.

Det er Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at der ved NIS 2-direktivets anvendelse af »på stedet« forstås en enheds lokaler, hvorfra enheden driver sine aktiviteter, samt arbejdssteder uden for enhedens lokaler. Det vil således efter bestemmelsen være muligt for de kompetente myndigheder at foretage tilsyn på enhedens forretningssteder.

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.

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

Den foreslåede bestemmelse vil betyde, at de kompetente myndigheder som led i et tilsyn kan foretage kontrol på stedet til enhver tid. Det forudsættes dog almindeligvis, at den kompetente myndighed forinden et evt. besøg vil varsle den væsentlige enhed herom.

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 de kompetente myndigheder 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 den kompetente myndigheder.

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 med-

lemsstaterne 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 de kompetente myndigheder kan foretage sikkerhedsaudits.

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 de kompetente myndigheder 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 de kompetente myndigheder 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 de kompetente myndigheder 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 den kompetente myndighed 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 følger af det foreslåede *stk. 2,* at de kompetente myndigheder ved anvendelsen af tiltagene i stk. 1, nr. 5-7, skal angive formålet med kravet og præcisere, hvilke oplysninger der kræves udleveret, og hvordan og i hvilken form oplysningerne og materialet nævnt i stk. 1, nr. 5-7, 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.

Efter den foreslåede bestemmelse vil der eksempelvis kunne stilles krav om anvendelse af bestemte skemaer, eller at der skal foretages indtastninger på en hjemmeside.

Der henvises i øvrigt til lovforslagets pkt. 3.4.

Til § 22

Det følger af artikel 15, stk. 1, i 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), at medlemsstaterne sikrer, at de kompetente myndigheder har de nødvendige beføjelser og midler til at vurdere, hvorvidt operatører af væsentlige tjenester opfylder deres forpligtelser i medfør af artikel 14 og virkningerne heraf på net- og informationssystemers sikkerhed.

Det fremgår desuden af NIS 1-direktivets artikel 15, stk. 2, at medlemsstaterne sikrer, at de kompetente myndigheder har beføjelser og midler til at pålægge operatører af væsentlige tjenester at levere a) de oplysninger, der er nødvendige for at vurdere sikkerheden i deres net- og informationssystemer, herunder dokumenterede sikkerhedspolitikker og b) dokumentation for den faktiske gennemførelse af sikkerhedspolitikker, som f.eks. resultaterne af en sikkerhedsaudit udført af den kompetente myndighed eller en kvalificeret auditør og i sidstnævnte tilfælde stille resultaterne heraf, herunder den tilgrundliggende dokumentation, til rådighed for den kompetente myndighed. Når der anmodes om sådanne oplysninger eller sådan dokumentation, angiver de kompetente myndigheder formålet med anmodningen og anfører, hvilke oplysninger der kræves.

Det følger af NIS 1-direktivets artikel 15, stk. 3, at efter vurderingen af oplysninger eller resultaterne af en sikkerhedsaudit, jf. stk. 2, kan den kompetente myndighed udstede påbud til operatører af væsentlige tjenester for at afhjælpe de påviste mangler.

Det følger af artikel 17, stk. 1, i NIS 1-direktivet bl.a., at medlemsstaterne sikrer, at de kompetente myndigheder om nødvendigt griber ind ved hjælp af efterfølgende tilsynsforanstaltninger, når det kan dokumenteres, at en udbyder af digitale tjenester ikke opfylder kravene i artikel 16 (sikkerhedskrav og underretning om hændelser).

Efter NIS 1-direktivets artikel 17, stk. 2, litra b, skal de kompetente myndigheder tillægges de fornødne beføjelser og midler til at pålægge udbydere af digitale tjenester at afhjælpe mangler i opfyldelsen af de krav, der er fastsat i artikel 16.

NIS 1-direktivet blev i dansk ret gennemført sektorvist i regulering gældende for de specifikke sektorer, hvor direktivet finder anvendelse. For en nærmere gennemgang af den sektorvise gennemførelse af NIS 1-direktivet henvises til afsnit 2.4 i lovforslagets almindelige bemærkninger.

Det følger af den foreslåede *§ 22,* at en kompetent myndighed kan anvende følgende håndhævelsesforanstaltninger over for en væsentlig enhed 1) udstede advarsler om enhedens overtrædelse af denne lov, 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 4, 3) påbyde enheden at træffe foranstaltninger, der er nødvendige for at forhindre eller afhjælpe en hændelse, 4) meddele enheden påbud og forbud for at sikre overholdelsen af de krav, der er fastsat i loven eller regler udstedt i medfør af loven, 5) påbyde enheden at underrette de fysiske eller juridiske personer, som enheden 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 enheden 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 enhedens overholdelse af lovens kapitel 2 og 3 samt regler udstedt i medfør heraf og 8) påbyde enheden 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.

Den foreslåede bestemmelse vil gennemføre NIS 2-direktivets artikel 32, stk. 4, litra a-h.

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.

Det bemærkes i den forbindelse, at det følger af NIS 2-direktivets artikel 32, stk. 1, at de håndhævelsesforanstaltninger, der anvendes overfor væsentlige enheder 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 den kompetente myndighed skal foretage en konkret vurdering af omstændighederne i hver enkelt sag, når centret anvender håndhæ-

velsesforanstaltningerne over for væsentlige enheder, således at proportionalitetsprincippet overholdes ved valg mellem de oplistede håndhævelsesmuligheder.

Den kompetente myndighed 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 den kompetente myndighed, 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 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 den kompetente myndighed.

Det følger endvidere af artikel 32, stk. 7, i NIS 2-direktivet, 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 afgørelsen for domstolene.

Der vil i forbindelse med en afgørelse om påbud eller forbud efter den foreslåede § 22 blive fastsat en frist, inden for hvilken enheden skal efterkomme indholdet i afgørelsen.

En enhed, der modtager en afgørelse om påbud eller forbud efter den foreslåede § 22, vil i overensstemmelse med den foreslåede bestemmelse i § 32, som vil gennemføre NIS 2-direktivets artikel 34, stk. 2, samtidig også kunne ifalde straf for en eventuel overtrædelse af denne lov eller regler udstedt i medfør af loven.

Det følger af det foreslåede *nr. 1,* at den kompetente myndighed kan udstede advarsler om enhedens overtrædelse af denne lov.

Den foreslåede bestemmelse vil give de kompetente myndigheder 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 de kompetente myndigheder.

Det følger af den foreslåede *nr. 2,* at den kompetente myndighed 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 den kompetente myndighed 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 det foreslåede *nr. 3,* at den kompetente myndighed kan påbyde enheden at træffe foranstaltninger, der er nødvendige for at forhindre eller afhjælpe en hændelse.

Den foreslåede bestemmelse vil medføre, at den kompetente myndighed kan 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 den kompetente myndighed kan meddele enheden 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 en enhed eksempelvis ikke lever op til de krav, der er fastsat i loven, vil en kompetent myndighed kunne angive, hvilke nærmere foranstaltninger enheden 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 enhedens anvendelse af bestemte logningsmetoder.

Det bemærkes, at der vil være tale om en forvaltningsretlig afgørelse, hvorfor forvaltningslovens regler herom vil finde anvendelse.

Det følger af det foreslåede *nr. 5,* at den kompetente myndighed kan påbyde enheden at underrette de fysiske eller

juridiske personer, til hvilke enheden 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 § 16, stk. 2, som indeholder en forpligtelse for væsentlige og vigtige enheder 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 enhederne også informere de pågældende modtagere om den væsentlige cybertrussel.

Med den foreslåede bestemmelse vil den kompetente myndighed kunne påbyde, at der skal foretages underretning af modtagerne af enhedens tjenester, uanset om enheden selv vurderer, at det er relevant.

Det bemærkes, at der vil være tale om en forvaltningsretlig afgørelse, hvorfor forvaltningslovens regler herom vil finde anvendelse.

Det følger af det foreslåede *nr. 6,* at den kompetente myndighed kan påbyde enheden 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 den kompetente myndighed kan foretage regelmæssige og målrettede sikkerhedsaudits eller stille krav om, at enheden får et kvalificeret uafhængigt organ til at foretage disse audits, samt den foreslåede § 22, stk. 1, nr. 3, hvorefter den kompetente myndighed kan foretage sikkerhedsaudits ad hoc.

Det bemærkes, at der vil være tale om en forvaltningsretlig afgørelse, hvorfor forvaltningslovens regler herom vil finde anvendelse.

Det følger af det foreslåede *nr. 7,* at den kompetente myndighed kan udpege en person med ansvar for i en nærmere fastsat periode at føre tilsyn med enhedens overholdelse af §§ 6, 12, 13, 15 og 16, stk. 2, samt regler udstedt i medfør heraf.

Den kompetente myndighed vil 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 enhedens overholdelse af krav til foranstaltninger til styring af cybersikkerhedsrisici i medfør af den foreslåede § 6 og enhedens overholdelse af oplysnings- og underretningspligterne i de foreslåede §§ 12, 14, 15 og 16, samt regler udstedt i medfør af de nævnte bestemmelser.

Det følger af det foreslåede *nr. 8,* at den kompetente myndighed kan påbyde enheden 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 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.

Der henvises i øvrigt til lovforslagets pkt. 3.4.

Til § 23

Der er i artikel 15 og 17 i 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), fastsat forpligtelser for de kompetente myndigheder til at føre tilsyn med opfyldelsen af direktivet i de omfattede sektorer.

NIS 1-direktivet indeholder ikke bestemmelser om, at de kompetente myndigheder kan træffe afgørelse om midlertidig suspension af en enheds certificeringer eller godkendelser eller om midlertidigt forbud mod, at en fysisk person med ledelsesansvar i enheden kan udøve ledelsesfunktioner.

Straffelovens § 79 indeholder regler om rettighedsfrakendelse ved dom for strafbare forhold, og bestemmelsen udgør den almindelige regel i dansk ret om rettighedsfrakendelse.

Efter straffelovens § 79, stk. 1, kan den, som udøver en af de i straffelovens § 78, stk. 2, omhandlede virksomheder (bl.a. den som virker som advokat, taxachauffør eller læge), ved dom for strafbart forhold frakendes retten til fortsat at udøve den pågældende virksomhed eller til at udøve den under visse former. Det samme gælder, når særlige omstændigheder taler derfor, om udøvelsen af anden virksomhed, jf. straffelovens § 79, stk. 2. Efter samme regel kan der ske frakendelse af retten til at deltage i ledelsen af en erhvervsvirksomhed her i landet eller i udlandet uden at hæfte personligt og ubegrænset for virksomhedens forpligtelser. Frakendelsen sker for et tidsrum fra 1 til 5 år regnet fra endelig dom eller indtil videre.

Det følger af det foreslåede *§ stk. 1,* at har de håndhævelsesforanstaltninger, der er pålagt i medfør af § 22, nr. 1-4, vist sig at være utilstrækkelige, kan den kompetente myndighed fastsætte en frist, inden for hvilken den væsentlige enhed skal foretage de nødvendige tiltag for at afhjælpe manglerne eller opfylde den kompetente myndigheds krav. Er tiltagene ikke foretaget inden for den fastsatte frist, kan den kompetente myndighed træffe afgørelse om 1) midlertidigt at su-

spendere en certificering eller godkendelse vedrørende dele af eller alle de relevante tjenester, enheden leverer, eller aktiviteter, der udføres af enheden og 2) midlertidigt at forbyde enhver fysisk person med ledelsesansvar på niveau med administrerende direktør eller den juridiske repræsentant hos enheden at udøve ledelsesfunktioner i den pågældende enhed.

Bestemmelsen vil gennemføre artikel 32, stk. 5, 1. led, i NIS 2-direktivet. 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.

Den foreslåede bestemmelse svarer indholdsmæssigt til NIS 2-direktivets artikel 32, stk. 5, 1. led, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Det bemærkes i den forbindelse, at det af den danske oversættelse af NIS 2-direktivets artikel 32, stk. 5, 1. led, fremgår, at bestemmelsen kan anvendes, hvor de relevante håndhævelsesforanstaltninger er »virkningsløse«. Denne oversættelse er efter Ministeriet for Samfundssikkerhed og Beredskabs opfattelse imidlertid ikke forenelig med den engelske udgave af direktivet, hvori »ineffective« er anvendt. Det er således Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at formuleringen »virkningsløse« ville udgøre en indholdsmæssig forskydning i forhold til den engelske sprogversion. Det er desuden Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at et kriterium om, at foranstaltningerne er »virkningsløse«, ville indebære, at enhver virkning af de anvendte foranstaltninger – uanset om virkningen måtte være utilstrækkelig eller endda negativ – ville betyde, at bestemmelsen ikke ville kunne anvendes. Det er Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at dette reelt ville gøre bestemmelsen uanvendelig i praksis i strid med direktivets forudsætninger. Der er på den baggrund anvendt et kriterium om, at foranstaltningerne er »utilstrækkelige«, da dette i en dansk juridisk sammenhæng vurderes at svare til »ineffektive« og afspejler et indbygget proportionalitetsprincip, som svarer til det forvaltningsretlige proportionalitetsprincip.

Det følger på den baggrund af den foreslåede bestemmelse, at det vil være en forudsætning for at anvende bestemmelsen, at håndhævelsesforanstaltninger pålagt i medfør af den foreslåede § 22, stk. 1-4, 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 enheden foretager de nødvendige tiltag for at afhjælpe mangler, som den kompetente myndighed har konstateret, eller opfylder den kompetente myndigheds 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 materielle eller immaterielle skade.

Den kompetente myndighed 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 § 23 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 enheden skal have truffet de nødvendige tiltag for at afhjælpe manglerne eller opfylde den kompetente myndigheds krav. Varigheden af fristen vil afhænge af en konkret vurdering, som foretages af den kompetente myndighed.

Det foreslås, at afgørelse om suspension eller forbud træffes af den kompetente myndighed i første instans. Det skal ses i lyset af, at muligheden for suspension og forbud ligger i forlængelse af den kompetente myndigheds 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 håndhævelsesforan-

staltninger 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, der er fastsat i §§ 6, 12, 13, 15 og 16, 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 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 enhed ikke har iværksat tiltag for at afhjælpe manglerne eller efterkomme den kompetente myndigheds krav inden for den fastsatte frist, kan den kompetente myndighed træffe afgørelse om midlertidigt at suspendere en certificering eller godkendelse vedrørende dele af eller alle de relevante tjenester, enheden leverer, eller aktiviteter, der udføres af enheden.

Den foreslåede bestemmelse skal læses i sammenhæng med den foreslåede bestemmelse i stk. 5, hvorefter vedkommende minister efter forhandling med ministeren for samfundssikkerhed og beredskab 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 1, nr. 1, ikke anvendes, før bemyndigelsen i den foreslåede stk. 5, er anvendt.

En afgørelse efter nr. 1 vil være af midlertidig karakter, jf. også det foreslåede stk. 2, hvorefter afgørelsen kun kan opretholdes, så længe enheden ikke har truffet de nødvendige tiltag for at afhjælpe de mangler eller efterleve de krav fra myndigheden, som gav anledning til, at foranstaltningerne blev anvendt.

Den foreslåede bestemmelse i stk. 1*, nr. 2,* indebærer, at såfremt den væsentlige enhed ikke har iværksat tiltag for at afhjælpe manglerne eller efterkomme den kompetente myndigheds krav inden for den fastsatte frist, kan den kompetente myndighed træffe afgørelse om midlertidigt at forbyde enhver fysisk person med ledelsesansvar på niveau med administrerende direktør eller den juridiske repræsentant hos enheden at udøve ledelsesfunktioner i den pågældende enhed.

Det bemærkes i denne forbindelse, 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 enhed, 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 opretholdes, så længe enheden ikke har truffet de nødvendige tiltag for at afhjælpe de mangler eller efterleve de krav fra myndigheden, som gav anledning til, at foranstaltningerne blev anvendt.

Det foreslås i *stk. 2,* at suspensioner eller forbud, som er pålagt i medfør af stk. 1, kun kan anvendes, indtil enheden 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, 2. led, 1. pkt., hvoraf det følger, 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, 2. led, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Bestemmelsen indebærer, at den kompetente myndighed, der 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 hos enheden at udøve ledel-

sesfunktioner i den pågældende enhed, skal træffe afgørelse om at ophæve foranstaltningen, når enheden 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 ikke kan indbringes for anden administrativ myndighed. Dette skal navnlig ses i lyset af, at der på de forskellige sektorer kan være forskellig praksis for administrativ rekurs. Det er på denne baggrund Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at muligheden for administrativ rekurs bør afskæres, således at alle enheder, der er underlagt denne lov, ligestilles.

Den foreslåede bestemmelse vil indebære, at en afgørelse vil kunne forlanges indbragt for domstolene af enheden eller den fysiske person, afgørelsen vedrører. Den myndighed, som har truffet afgørelse i sagen skal i givet fald anlægge en sag inden for rammerne af den civile retspleje mod den enhed eller person, som har forlangt sagen indbragt.

Den foreslåede bestemmelse vil gennemføre NIS 2-direktivets artikel 32, stk. 5, 2. led, 2. pkt., 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 enheden 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 de foreslåede bestemmelser i stk. 1-3 ikke finder anvendelse på offentlige forvaltningsenheder.

Den foreslåede bestemmelse vil gennemføre NIS 2-direktivets artikel 32, stk. 5, 3. led, hvorefter håndhævelsesforanstaltningen i artikel 32, stk. 5, ikke finder anvendelse på offentlige forvaltningsenheder, der er omfattet af direktivet.

Den foreslåede bestemmelse svarer med sproglige tilpasninger uden indholdsmæssig betydning til NIS 2-direktivets artikel 32, stk. 5, 3. led, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Den foreslåede bestemmelse indebærer, at muligheden for suspension eller forbud ikke finder anvendelse på enheder i den offentlige forvaltning, herunder både den centrale offentlige forvaltning og forvaltningsenheder på lokal plan.

Det følger af det foreslåede *stk. 5,* at vedkommende minister fastsætter forhandling med ministeren for samfundssikkerhed og beredskab kan fastsætte nærmere regler om, hvilke certificeringer og godkendelser der er omfattet af stk. 1, nr. 1.

Den foreslåede bestemmelse i stk. 5 indebærer, at vedkommende minister kan fastsætte nærmere regler om, hvilke certificeringer og godkendelser der er omfattet af den midlertidige suspensionsordning i § 23, stk. 1, nr. 1.

Ved at fastsætte nærmere regler i bekendtgørelsesform sikres det, at det vil være klart og forudsigeligt for enhederne, 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 1, nr. 1, ikke anvendes, før bemyndigelsen i den foreslåede stk. 5, er anvendt.

Der henvises i øvrigt til lovforslagets pkt. 3.4.

Til § 24

Det følger af artikel 15, stk. 1, i 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), at medlemsstaterne sikrer, at de kompetente myndigheder har de nødvendige beføjelser og midler til at vurdere, hvorvidt operatører af væsentlige tjenester opfylder deres forpligtelser i medfør af artikel 14 (sikkerhedskrav og underretning om hændelser) og virkningerne heraf på net- og informationssystemers sikkerhed. Efter artikel 15, stk. 2, skal medlemsstaterne sikre, at de kompetente myndigheder har beføjelser til at pålægge operatører af væsentlige tjenester at levere a) de oplysninger, der er nødvendige for at vurdere sikkerheden i deres net- og informationssystemer, herunder dokumenterede sikkerhedspolitikker, og b) dokumentation for den faktiske gennemførelse af sikkerhedspolitikker, som f.eks. resultaterne af en sikkerhedsaudit udført af den kompetente myndighed eller en kvalificeret auditør og i sidstnævnte tilfælde stille resultaterne heraf, herunder den tilgrundliggende dokumentation, til rådighed for den kompetente myndighed.

For så vidt angår udbydere af digitale tjenester, følger det af NIS 1-direktivets artikel 17, stk. 1, at medlemsstaterne sikrer, at de kompetente myndigheder om nødvendigt griber ind ved hjælp af efterfølgende tilsynsforanstaltninger, når det kan dokumenteres, at en udbyder af digitale tjenester ikke opfylder kravene i direktivets artikel 16 (sikkerhedskrav og underretning om hændelser).

Efter NIS 1-direktivets artikel 17, stk. 2, skal de kompetente myndigheder tillægges de fornødne beføjelser og midler til

at pålægge udbydere af digitale tjenester at a) forelægge de oplysninger, der er nødvendige for at vurdere sikkerheden af deres net- og informationssystemer, herunder dokumenterede sikkerhedspolitikker og b) afhjælpe mangler i opfyldelsen af de krav, der er fastsat i artikel 16.

NIS 1-direktivet blev i dansk ret gennemført sektorvist i regulering gældende for de specifikke sektorer, hvor direktivet finder anvendelse. For en nærmere gennemgang af den sektorvise gennemførelse af NIS 1-direktivet henvises til afsnit 2.4 i lovforslagets almindelige bemærkninger.

Det foreslås i *stk. 1,* at de kompetente myndigheder som led i sit kan anvende nærmere angivne tilsynsforanstaltninger over for en vigtig teleudbyder.

I overensstemmelse med direktivets forudsætninger, som udtrykt i præambelbetragtning nr. 122, vil vigtige enheder – i modsætning til væsentlige enheder – 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 enheder 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 de kompetente myndigheder 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 § 24, 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, 5, 6 og den del af bestemmelsen i nr. 2, der vedrører, at der kan stilles krav om, at enheden får et kvalificeret uafhængigt organ til at foretage sikkerhedsaudits, og at resultaterne herfor skal stilles til rådighed for den kompetente myndighed, vil være tale om oplysningspligter omfattet af lov om retssikkerhed ved forvaltningens anvendelse af tvangsindgreb og oplysningspligter finder anvendelse. 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 de kompetente myndigheder uden retskendelse og mod behørig legitimation kan foretage kontrol på stedet og eksternt efterfølgende tilsyn.

Den foreslåede bestemmelse vil gennemføre artikel 33, stk. 1 og 2, i NIS 2-direktivet.

Det er Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at der ved NIS 2-direktivets anvendelse af »på stedet« forstås en enheds lokaler, hvorfra enheden driver sine aktiviteter, samt arbejdssteder uden for enhedens lokaler. Det vil således efter bestemmelsen være muligt for de kompetente myndigheder at foretage tilsyn på enhedens forretningssteder.

Det følger af NIS 2-direktivets artikel 33, stk. 1, at når medlemsstaterne kommer i besiddelse af dokumentation for eller tegn på eller oplysninger om, at en vigtig enhed angiveligt ikke overholder dette direktiv, navnlig artikel 21 og 23 deri, sikrer de, at de kompetente myndigheder træffer foranstaltninger, hvor det er nødvendigt, gennem efterfølgende tilsynsforanstaltninger. Medlemsstaterne sikrer, at disse foranstaltninger er effektive, står i rimeligt forhold til overtrædelsen og har afskrækkende virkning under hensyntagen til omstændighederne i hver enkelt sag.

For effektivt at kunne konstatere, om vigtige enheder i praksis har gennemført de nødvendige foranstaltninger til at sikre deres net- og informationssystemer, er det nødvendigt, at de kompetente myndigheder som led i et tilsyn har adgang til forretningssteder hos vigtige enheder. Det foreslås derfor,

at der skal være adgang til kontrol på stedet uden retskendelse og mod behørig legitimation.

Den foreslåede bestemmelse vil betyde, at de kompetente myndigheder som led i et tilsyn kan foretage kontrol på stedet til enhver tid. Det forudsættes dog almindeligvis, at den kompetente myndighed forinden et evt. besøg vil varsle den vigtige enhed herom.

Det foreslås i *nr. 2,* at de kompetente myndigheder 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 den kompetente myndighed.

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 de kompetente myndigheder 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 de kompetente myndigheder kan kræve at få udleveret oplysninger, der er nødvendige for efterfølgende at vurdere de foranstaltninger til styring af sikkerhedsrisici, som den berørte enhed 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 de kompetente myndigheder 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 de kompetente myndigheder 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 følger af det foreslåede *stk. 2,* at de kompetente myndigheder ved anvendelse af tiltagene i stk. 1, nr. 4-6, skal angive formålet med kravet og præcisere, hvilke oplysninger der kræves udleveret, og hvordan og i hvilken form oplysningerne og materialet nævnt i stk. 1, nr. 4-6, skal udleveres.

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.

Den foreslåede bestemmelse svarer indholdsmæssigt til NIS 2-direktivets artikel 33, stk. 3, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Det foreslås i *stk. 3,* at de kompetente myndigheder kan stille nærmere krav om, hvordan og i hvilken form oplysningerne eller materialet nævnt i stk. 1, nr. 4-6, skal afgives.

Den foreslåede bestemmelse indebærer, at en kompetent myndighed i forbindelse med, at der stilles krav om udlevering af oplysninger eller materiale efter de foreslåede bestemmelser i stk. 1, nr. 4-6, 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.

Der henvises i øvrigt til afsnit 3.4 i lovforslagets almindelige bemærkninger.

Til § 25

Det følger af artikel 15, stk. 1, i 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), at medlemsstaterne sikrer, at de kompetente myndigheder har de nødvendige beføjelser og midler til at vurdere, hvorvidt operatører af væsentlige tjenester opfylder deres

forpligtelser i medfør af artikel 14 og virkningerne heraf på net- og informationssystemers sikkerhed.

Det fremgår desuden af NIS 1-direktivets artikel 15, stk. 2, at medlemsstaterne sikrer, at de kompetente myndigheder har beføjelser og midler til at pålægge operatører af væsentlige tjenester at levere a) de oplysninger, der er nødvendige for at vurdere sikkerheden i deres net- og informationssystemer, herunder dokumenterede sikkerhedspolitikker og b) dokumentation for den faktiske gennemførelse af sikkerhedspolitikker, som f.eks. resultaterne af en sikkerhedsaudit udført af den kompetente myndighed eller en kvalificeret auditør og i sidstnævnte tilfælde stille resultaterne heraf, herunder den tilgrundliggende dokumentation, til rådighed for den kompetente myndighed. Når der anmodes om sådanne oplysninger eller sådan dokumentation, angiver de kompetente myndigheder formålet med anmodningen og anfører, hvilke oplysninger der kræves.

Det følger endvidere af NIS 1-direktivets artikel 15, stk. 3, at efter vurderingen af oplysninger eller resultaterne af en sikkerhedsaudit, jf. stk. 2, kan den kompetente myndighed udstede påbud til operatører af væsentlige tjenester for at afhjælpe de påviste mangler.

Det følger herudover af NIS 1-direktivets artikel 17, stk. 1, at medlemsstaterne sikrer, at de kompetente myndigheder om nødvendigt griber ind ved hjælp af efterfølgende tilsynsforanstaltninger, når det kan dokumenteres, at en udbyder af digitale tjenester ikke opfylder kravene i artikel 16 (sikkerhedskrav og underretning om hændelser).

Efter NIS 1-direktivets artikel 17, stk. 2, litra b, skal de kompetente myndigheder tillægges de fornødne beføjelser og midler til at pålægge udbydere af digitale tjenester at afhjælpe mangler i opfyldelsen af de krav, der er fastsat i artikel 16.

NIS 1-direktivet blev i dansk ret gennemført sektorvist i regulering gældende for de specifikke sektorer, hvor direktivet finder anvendelse. For en nærmere gennemgang af den sektorvise gennemførelse af NIS 1-direktivet henvises til afsnit 2.4 i lovforslagets almindelige bemærkninger.

Det følger af den foreslåede *§ 25,* at en kompetent myndighed ud fra en konkret vurdering af omstændighederne i hver enkelt sag kan anvende følgende håndhævelsesforanstaltninger over for en vigtig enhed: 1) udstede advarsler om enhedens overtrædelse af denne lov, 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 enheden påbud og forbud for at sikre overholdelsen af de krav, der er fastsat i loven eller regler udstedt i medfør af loven, 4) påbyde enheden at underrette de fysiske eller juridiske personer, til hvilke den 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 enheden at gennemføre de anbefalinger, der er fremsat i forbindelse med en gennemført sikkerhedsaudit, og 6) påbyde enheden i ikke-anonymiseret form og på en nærmere angiven måde at offentliggøre afgørelser om håndhævelsesforanstaltninger efter nr. 3-5 samt resumeer af domme eller bødevedtagelser, hvor der idømmes eller vedtages en bøde.

Den foreslåede bestemmelse vil gennemføre artikel 33, stk. 4, litra a-g, i NIS 2-direktivet. Bestemmelsen indeholder en forpligtelse for medlemsstaterne til at sikre, at deres kompetente myndigheder, når de udøver deres håndhævelsesbeføjelser over for vigtige enheder, som minimum har beføjelse til at: 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.

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.

De foranstaltninger, der anvendes i forhold til vigtige enheder, skal i overensstemmelse efter 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 § 25, at en kompetent myndighed skal foretage en konkret vurdering af omstændighederne i hver enkelt sag, når den anvender håndhævelsesforanstaltningerne over for vigtige enheder. Den kompetente myndighed 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 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, 12, 15 og 16, stk. 2, 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 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.

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 vil i forbindelse med en afgørelse om påbud eller forbud efter den foreslåede § 25 blive fastsat en frist, inden for hvilken enheden skal overholde indholdet i afgørelsen.

Det følger af det foreslåede *nr. 1,* at den kompetente myndighed kan udstede advarsler om enhedens overtrædelse af denne lov.

Den foreslåede bestemmelse vil give de kompetente myndigheder 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 de kompetente myndigheder.

Det følger af den foreslåede *nr. 2,* at den kompetente myndighed 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 den kompetente myndighed 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 det foreslåede *nr. 3,* at den kompetente myndighed kan meddele enheden 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 en enhed ikke lever op til de krav, der er fastsat i loven, vil den kompetente myndighed eksempelvis kunne angive, hvilke nærmere foranstaltninger enheden 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 enhedens anvendelse af bestemte logningsmetoder.

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 den kompetente myndighed kan påbyde enheden at underrette de fysiske eller juridiske personer, til hvilke den 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 § 15, stk. 2, som indeholder en forpligtelse for væsentlige og vigtige enheder 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 enhederne også informere de pågældende modtagere om den væsentlige cybertrussel.

Med det foreslåede nr. 4 vil den kompetente myndighed kunne påbyde, at der skal foretages underretning af modtagerne af enhedens tjenester, uanset om enheden selv vurderer, at det er relevant.

Det bemærkes, at der vil være tale om en forvaltningsretlig afgørelse, hvorfor forvaltningslovens regler herom vil finde anvendelse.

Det følger af det foreslåede *nr. 5,* at den kompetente myndighed kan påbyde enheden at gennemføre de anbefalinger, der er fremsat i forbindelse med en gennemført sikkerhedsaudit.

Bestemmelsen skal ses i sammenhæng med den foreslåede § 25, stk. 1, nr. 2, hvorefter den kompetente myndighed kan foretage målrettede sikkerhedsaudits eller stille krav om, at enheden får et kvalificeret uafhængigt organ til at foretage disse audits.

Det bemærkes, at der vil være tale om en forvaltningsretlig afgørelse, hvorfor forvaltningslovens regler herom vil finde anvendelse.

Det følger af det foreslåede *nr. 6,* at den kompetente myndighed kan påbyde enheden 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 bag 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.

Det bemærkes, at der vil være tale om en forvaltningsretlig afgørelse, hvorfor forvaltningslovens regler herom vil finde anvendelse.

Der henvises i øvrigt til lovforslagets pkt. 3.4.

Til § 26

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), stiller ikke nærmere krav om kompetente myndigheders forudgående høring eller begrundelse i forbindelse med deres afgørelsesvirksomhed.

Det følger af den foreslåede *§ 26,* at inden den kompetente myndighed træffer afgørelse om at anvende håndhævelsesforanstaltninger efter §§ 22, 23 eller 25, underrettes den berørte enhed om de påtænkte håndhævelsesforanstaltninger og begrundelsen herfor. Den kompetente myndighed skal give enheden 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, i NIS 2-direktivet. 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.

Ministeriet for Samfundssikkerhed og Beredskab har lagt vægt på at der foretages en direktivnær minimumsimplementering. 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 den kompetente myndighed til at foretage en høring af en enhed, før der træffes beslutning om at anvende en påtænkt håndhævelsesforanstaltning efter §§ 22, 23 eller 25.

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 enhedens bemærkninger til høringen kan få indflydelse på resultatet, at den kompetente myndighed lader høringsskrivelsen få virkning som en afgørelse, hvis enheden ikke kommer med bemærkninger til høringen inden dennes udløb, og hvornår høringsskrivelsen vil få retsvirkning som en afgørelse. Idet høringsskrivelsen vil kunne få virkning som en afgørelse, skal forvaltningslovens krav til bl.a. klagevejledning desuden overholdes.

Høringsskrivelsen skal indeholde en rimelig frist for enheden til at afgive bemærkninger til agterskrivelsens 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.

Der henvises i øvrigt til lovforslagets pkt. 3.4.

Til § 27

Det fremgår af artikel 17, stk. 3, i 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), at hvis en udbyder af digitale tjenester har sit hjemsted eller en repræsentant i én medlemsstat, men dets net- og informationssystemer er beliggende i en eller flere andre medlemsstater, samarbejder den kompetente myndighed i den medlemsstat, hvor hjemstedet eller repræsentanten befinder sig, og de kompetente myndigheder i de pågældende andre medlemsstater og bistår hinanden efter behov. En sådan bistand og et sådant samarbejde kan omfatte udveksling af oplysninger mellem de berørte kompetente myndigheder og anmodninger om at gennemføre de tilsynsforanstaltninger, som direktivet giver mulighed for.

NIS 1-direktivet blev i dansk ret gennemført sektorvist i regulering gældende for de specifikke sektorer, hvor direktivet finder anvendelse. For en nærmere gennemgang af den sektorvise gennemførelse af NIS 1-direktivet henvises til afsnit 2.4 i lovforslagets almindelige bemærkninger.

Det følger af den foreslåede *stk. 1,* at hvor en enhed leverer tjenester i mere end én medlemsstat i Den Europæiske Union, eller hvor enheden leverer tjenester i en eller flere medlemsstater, og enhedens net- og informationssystemer er beliggende i en eller flere andre medlemsstater, samarbejder de kompetente myndigheder med de andre medlemsstaters kompetente myndigheder i relevant omfang.

Bestemmelsen vil gennemføre artikel 37, stk. 1, i NIS 2-direktivet, hvoraf det følger, at hvor en enhed leverer tjenester i mere end én medlemsstat, eller hvor den leverer tjenester i en eller flere medlemsstater, og dens net- og informationssystemer er beliggende i en eller flere andre medlemsstater, samarbejder de kompetente myndigheder i de pågældende medlemsstater med og bistår hinanden efter behov. Dette samarbejde indebærer mindst: a) at de kompetente myndigheder, der anvender tilsyns- eller håndhævelsesforanstaltninger i en medlemsstat, via det fælles kontaktpunkt underretter og hører de kompetente myndigheder i de øvrige berørte medlemsstater om de tilsyns- og håndhævelsesforanstaltninger, der er truffet, b) at en kompetent myndighed kan anmode en anden kompetent myndighed om at træffe tilsyns- eller håndhævelsesforanstaltninger, og c) at en kompetent myndighed efter modtagelse af en begrundet anmodning fra en anden kompetent myndighed yder bistand til den anden kompetente myndighed, der står i et rimeligt forhold til dens egne ressourcer, således at tilsyns- eller håndhævelsesforanstaltningerne kan gennemføres på en effektiv, virkningsfuld og konsekvent måde.

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 foreslås i *nr. 1,* at de kompetente myndigheder underretter via det centrale kontaktpunkt de kompetente myndigheder i relevante medlemsstater om anvendelse tilsyns- og håndhævelsesforanstaltninger.

Den foreslåede bestemmelse vil medføre, at de kompetente myndigheder, når en enhed leverer tjenester i mere end én medlemsstat, eller hvor enheden leverer tjenester i en eller flere medlemsstater, og enhedens net- og informationssystemer er beliggende i en eller flere andre medlemsstater, via det centrale kontaktpunkt, de kompetente myndigheder i relevante medlemsstater om anvendte tilsyns- og håndhævelsesforanstaltninger.

Samarbejdet indebærer således, 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 enheden leverer tjenester, eller hvor dens net- og informationssystemer er beliggende.

Det foreslås i *nr. 2.,* at de kompetente myndigheder kan anmode en anden medlemsstats kompetente myndigheder om at anvende tilsyns- og håndhævelsesforanstaltninger over for enheder i det pågældende land.

Den foreslåede bestemmelse vil medføre, at de kompetente myndigheder, når en enhed leverer tjenester i mere end én medlemsstat, eller hvor enheden leverer tjenester i en eller flere medlemsstater, og enhedens net- og informationssystemer er beliggende i en eller flere andre medlemsstater, kan anmode en anden medlemsstats kompetente myndigheder om at anvende tilsyns- og håndhævelsesforanstaltninger over for enheder i det pågældende land.

Samarbejdet indebærer desuden, at de danske kompetente myndigheder kan anmode en anden medlemsstats kompetente myndigheder om at iværksætte tilsyns- og håndhævelsesforanstaltninger.

Det foreslås i *nr. 3,* de kompetente myndigheder yder i rimeligt omfang bistand til en anden medlemsstats kompetente myndighed efter modtagelse af en begrundet anmodning herom.

Den foreslåede bestemmelse vil indebære, at de kompetente myndigheder, når en enhed leverer tjenester i mere end én medlemsstat, eller hvor enheden leverer tjenester i en eller flere medlemsstater, og enhedens net- og informationssystemer er beliggende i en eller flere andre medlemsstater, yder bistand til en anden medlemsstats kompetente myndighed efter modtagelse af en begrundet anmodning herom.

Samarbejdet indebærer endvidere, at de kompetente myndigheder 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 den kompetente myndigheds 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, offentlig sikkerhed eller forsvar. Før der kan ske afvisning af en anmodning, skal den kompetente myndighed 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.

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, offentlig 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 indebærer ikke, at andre medlemsstaters myndigheder selvstændigt kan udøve tilsynsbeføjelser her i landet. Tilsynsforanstaltninger vil således altid foretages under den danske kompetente myndigheds ansvar.

Det følger af det foreslåede *stk. 2*, at de kompetente myndigheder 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, hvoraf det følger, at hvor det er hensigtsmæssigt og efter fælles overenskomst, kan de kompetente myndigheder fra forskellige medlemsstater gennemføre fælles tilsynstiltag.

Den foreslåede bestemmelse svarer 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.

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. Den foreslåede bestemmelse i stk. 2 vil derfor ikke finde anvendelse i situationer, hvor en anden medlemsstat ønsker, at der gennemføres fælles tilsynstiltag vedrørende overholdelsen af medlemsstatens nationale overimplementering af NIS 2-direktivet.

Det følger af det foreslåede *stk. 3,* at modtages der en anmodning om gensidig bistand, jf. den foreslåede bestemmelse i § 27, vedrørende DNS-tjenesteudbydere, topdomænenavneadministratorer, enheder, der leverer domænenavneregistreringstjenester, og udbydere af henholdsvis cloudcomputingtjenester, datacentertjenester, indholdsleveringsnetværk, administrerede tjenester, administrerede sikkerhedstjenester, onlinemarkedspladser, onlinesøgemaskiner og platforme for sociale netværkstjenester, kan der træffes passende tilsyns- og håndhævelsesforanstaltninger over for enheden, hvis denne leverer tjenester eller har et net- og informationssystem i Danmark.

Bestemmelsen vil gennemføre NIS 2-direktivets artikel 26, stk. 5, som fastsætter, at medlemsstater, der har modtaget en anmodning om gensidig bistand, jf. direktivets artikel 37, vedrørende en enhed som omhandlet i stk. 1, litra b, inden for rammerne af denne anmodning kan træffe passende tilsyns- og håndhævelsesforanstaltninger over for den pågældende enhed, der leverer tjenester eller har et net- og informationssystem på deres område.

Den foreslåede bestemmelse svarer indholdsmæssigt til NIS 2-direktivets artikel 26, stk. 5, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Bestemmelsen indebærer, at der som led i gensidig bistand mellem medlemsstater kan iværksættes tilsyns- og håndhævelsesforanstaltninger over for bestemte enheder i tilfælde, hvor enheden ellers ikke ville høre under dansk jurisdiktion.

Til § 28

Det følger af den foreslåede bestemmelse i *§ 28,* at de kompetente myndigheder kan videregive oplysninger til andre medlemsstaters myndigheder og til institutioner i Den Europæiske Union for at varetage de opgaver, som følger af denne lov eller regler udstedt i medfør af loven.

Bestemmelsen indebærer, at de kompetente myndigheder som led i den nationale gennemførelse af direktivet, kan videregive oplysninger til andre medlemsstater eller EU-institutioner, hvis det er nødvendigt for at sikre overholdelsen af forpligtelserne i NIS 2-direktivet.

Det følger således af NIS 2-direktivets artikel 23, stk. 6, at hvor det er relevant, informerer CSIRT'en, den kompetente myndighed eller det centrale kontaktpunkt uden unødigt ophold de øvrige berørte medlemsstater og ENISA om den væsentlige hændelse, navnlig hvor den væsentlige hændelse berører to eller flere medlemsstater. Det følger af samme bestemmelse, at sådan information omfatter den type af oplysninger, der er modtaget i overensstemmelse med artikel 23, stk. 4, om enhedernes underretninger om væsentlige hændelser, og at CSIRT'en, den kompetente myndighed eller det centrale kontaktpunkt i den forbindelse i overensstemmelse med EU-retten eller national ret sikrer enhedens sikkerhed og kommercielle interesser samt fortrolig behandling af de afgivne oplysninger.

Efter bestemmelsen i artikel 23, stk. 6, vil CSIRT'en, de

kompetente myndigheder eller det centrale kontaktpunkt således i relevant omfang skulle videregive oplysninger, som er modtaget i medfør af de foreslåede bestemmelser i §§ 12 og 13 om hændelsesunderretninger, til øvrige berørte medlemsstater og ENISA.

I overensstemmelse med NIS 2-direktivets artikel 2, stk. 13, vil det skulle sikres, at de oplysninger, der udveksles, begrænses til, hvad der er relevant og forholdsmæssigt under hensyn til formålet med udvekslingen. Udvekslingen af oplysninger skal bevare de pågældende oplysningers fortrolighed og beskytte de berørte enheders sikkerhed og kommercielle interesser.

Til § 29

Det følger af artikel 1, stk. 6, i 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), at direktivet ikke berører de tiltag, som iværksættes af medlemsstaterne med henblik på at sikre deres centrale statslige funktioner, navnlig for at værne om den nationale sikkerhed, herunder foranstaltninger til beskyttelse af oplysninger, hvis udbredelse efter medlemsstaternes opfattelse ville stride mod deres væsentlige sikkerhedsinteresser, og opretholde lov og orden, navnlig for at tillade efterforskning, afsløring og retsforfølgelse af strafbare handlinger.

NIS 1-direktivet blev i dansk ret gennemført sektorvist i regulering gældende for de specifikke sektorer, hvor direktivet finder anvendelse. For en nærmere gennemgang af den sektorvise gennemførelse af NIS 1-direktivet henvises til afsnit 2.4 i lovforslagets almindelige bemærkninger.

Derudover reguleres videregivelse af oplysninger, der ville stride mod væsentlige interesser af hensyn til den nationale sikkerhed, offentlige orden eller forsvar, bl.a. i forvaltningslovens regler om tavshedspligt og videregivelse af oplysninger, straffelovens regler om tavshedspligt, samt Justitsministeriets cirkulære nr. 10338 af 17. december 2014 om sikkerhedsbeskyttelse af information af fælles interesse for landene i NATO eller EU, andre klassificerede informationer samt informationer af sikkerhedsmæssig beskyttelsesinteresse i øvrigt (sikkerhedscirkulæret).

Det følger af de foreslåede *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 vil gennemføre artikel 2, stk. 11, i NIS 2-direktivet, som 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.

Baggrunden for artikel 2, stk. 11, er beskrevet i NIS 2-direktivets præambelbetragtning nr. 9, 4. pkt., hvor det fremgår, at ingen medlemsstat bør være forpligtet til at meddele oplysninger, hvis videregivelse efter dens opfattelse 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.

Under hensyn til bestemmelsen i NIS 2-direktivets artikel 2, stk. 7 (om at direktivet ikke finder anvendelse på offentlige forvaltningsenheder, der udfører aktiviteter inden for national sikkerhed, offentlig sikkerhed, forsvar eller retshåndhævelse), og den foreslåede bestemmelse i § 1, stk. 4 (om undtagelse af specifikke enheder, der udfører aktiviteter inden for national sikkerhed, offentlig sikkerhed, forsvar eller retshåndhævelse mv.), er det Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at den foreslåede bestemmelse i § 29, stk. 1, vil have et yderst begrænset anvendelsesområde.

Bestemmelsen vil desuden alene vedrøre meddelelsen af oplysninger, som efter en konkret vurdering vil stride mod væsentlige interesser med hensyn til den nationale sikkerhed, offentlige sikkerhed eller forsvar. Bestemmelsen vil således eksempelvis ikke medføre, at en virksomhed mere generelt kan undlade at efterkomme oplysningsforpligtelserne over for de kompetente myndigheder, herunder som et led i myndighedernes tilsyn.

Den foreslåede bestemmelse i *stk. 2* indebærer, 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. Sådan information omfatter den type af oplysninger, der er modtaget i overensstemmelse med artikel 23, stk. 4. CSIRT'en, den kompetente

myndighed eller det centrale kontaktpunkt sikrer i den forbindelse i overensstemmelse med EU-retten eller national ret enhedens sikkerhed og kommercielle interesser samt fortrolig behandling af de afgivne oplysninger.

Den foreslåede bestemmelse vil finde anvendelse, uanset om oplysningerne modtages direkte fra den pågældende nationale myndighed eller via andre, herunder Europa-Kommissionen.

Til § 30

Det følger af den foreslåede *§ 30,* at vedkommende minister efter forhandling med 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.

Vedkommende minister får efter bestemmelsen hjemmel til efter forhandling med ministeren for samfundssikkerhed og beredskab at fastsætte regler, som er nødvendige for at gennemføre retsakter udstedt af Europa-Kommissionen.

Til § 31

Det følger af den foreslåede *§ 31,* 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 enheder at anvende bestemte internetløsninger, herunder selvbetjeningsløsninger.

Den foreslåede bestemmelse skal ses i lyset af forvaltningslovens § 32 a, hvoraf det følger, at vedkommende minister kan fastsætte regler om ret til at anvende digital kommunikation ved henvendelser til den offentlige forvaltning og om de nærmere vilkår herfor, herunder fravige formkrav i lovgivningen, der hindrer anvendelsen af digital kommunikation.

Der kan 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 enhederne skal foretage underretninger om hændelser i medfør af de foreslåede §§ 12, 13 og 14. 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 §§ 9 og 10 skal efterkommes ved anvendelse af bestemte internetløsninger såsom Virk.dk.

Der kan med hjemmel i bestemmelsen fastsættes regler om, at skriftlige henvendelser til myndighederne, herunder de kompetente myndigheder, CSIRT'en mv., om forhold, som er omfattet af et krav om digital kommunikation, ikke anses for behørigt modtaget af myndighederne, hvis de indsendes på anden vis end den foreskrevne digitale måde.

Hvis en enhed retter henvendelse til en myndighed på anden måde end den foreskrevne digitale måde, følger det af den almindelige vejledningspligt, jf. forvaltningslovens § 7, at myndigheden 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 enheds computere ikke fungerer, at enheden har mistet koden til sin digitale signatur, eller at der opstår lignende hindringer, som det er op til enheden at overvinde, vil ikke kunne føre til fritagelse for pligten til digital kommunikation. I så fald må den pågældende enhed 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 foreslås, at regler i medfør af bestemmelsen udstedes ministeren for samfundssikkerhed og beredskab.

Det bemærkes, at Europa-Kommissionen på visse punkter er tillagt kompetence til at fastsætte nærmere regler om, hvordan oplysninger skal afgives fra enhederne. 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 § 32

Det følger af artikel 21 i 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), at medlemsstaterne fastsætter regler om sanktioner, der skal anvendes i tilfælde af overtrædelser af de nationale regler, der er vedtaget i medfør af dette direktiv, og træffer alle nødvendige foranstaltninger til at sikre, at de gennemføres. Sanktionerne skal være effektive, stå i rimeligt forhold til overtrædelsen og have afskrækkende virkning.

NIS 1-direktivet indeholder ikke nærmere bestemmelser om ansvar for bestemte fysiske personer.

NIS 1-direktivet blev i dansk ret gennemført sektorvist i regulering gældende for de specifikke sektorer, hvor direktivet finder anvendelse. For en nærmere gennemgang af den sektorvise gennemførelse af NIS 1-direktivet, henvises til afsnit 2.4 i lovforslagets almindelige bemærkninger.

Det følger af det foreslåede *§ 32, stk. 1,* at den der: 1) overtræder § 6, stk. 1 eller 2, §§ 9 eller 10, § 11, stk. 1-6, § 12, stk. 1, § 13, stk. 1 eller 2, eller § 15, 2) undlader at efterkomme en kompetent myndigheds afgørelse efter § 23, stk. 1, nr. 1 eller 2, 3) undlader at efterkomme påbud eller forbud efter §§ 22 eller 25, 4) undlader at efterkomme krav efter § 16, stk. 2, § 21, stk. 1, nr. 2 eller nr. 5-7, eller § 24, stk. 1, nr. 2 eller nr. 4-6, eller 5) hindrer de kompetente myndigheder i at føre tilsyn efter bestemmelserne i § 21, stk. 1, nr. 1-4, eller § 24, stk. 1, nr. 1-3, straffes med bøde.

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 § 7, stk. 1 – gennemføre NIS 2-direktivets artikel 20, stk. 1, hvoraf det følger, at medlemsstaterne sikrer, 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 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 enheders overtrædelse af bestemmelserne i § 6, stk. 1, §§ 12, 13 og 15 og § 16, stk. 2, 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 endvidere i overensstemmelse med en minimumsimplementering af NIS 2-direktivets artikel 34, stk. 5, at bødens størrelse for vigtige enheders overtrædelse af bestemmelserne i § 6, stk. 1, §§ 12, 13 og 15 og § 16, stk. 2, 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 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, der er fastsat i §§ 6, 12, 13, 15 og 16, 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.

De almindelige regler i straffelovens kapitel 10 om henholdsvis strafskærpende og strafformildende omstændigheder skal ligeledes iagttages ved anvendelsen af nærværende strafbestemmelser.

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 §§ 22, 23 og 25.

Det bemærkes, at manglende efterlevelse af bestemmelserne i § 22, stk. 1, nr. 2, og § 25, stk. 1, nr. 2, vil kunne straffes efter både § 32, stk. 1, nr. 4 og 5. Baggrunden er, at de kompetente myndigheder efter de pågældende bestemmelser enten kan stille krav om, at enhederne foretager sikkerhedsaudits, eller selv kan foretage sikkerhedsaudits hos de berørte enheder. En enhed vil således efter omstændighederne kunne straffes for at undlade at efterkomme et krav fra en kompetent myndighed efter nr. 4 eller for at hindre de kompetente myndigheder i at føre tilsyn efter nr. 5.

Det foreslås i *nr. 1,* at den der overtræder § 6, stk. 1 eller 2, §§ 9 eller 10, § 11, stk. 1-6, § 12, stk. 1, § 13, stk. 1 eller 2, eller § 15, straffes med bøde.

Den foreslåede bestemmelse vil indebære, at en enhed, der ikke træffer passende, forholdsmæssige, operationelle og organisatoriske foranstaltninger efter den foreslåede § 6, stk. 1 eller 2.

Den foreslåede bestemmelse vil endvidere indebære, at enheder omfattet af de foreslåede bestemmelser i §§ 9 og 10 vil kunne straffes med bøde, hvis registreringspligterne i de foreslåede §§ 9 og 10 ikke overholdes.

Den foreslåede bestemmelse vil endvidere indebære, at topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester straffes med bøde, hvis de ikke overholder reglerne i den foreslåede § 11, stk. 1-6, herunder vedrørende krav om en særskilt database, indførsel af politikker og procedure, offentliggørelse af domænenavnsregistreringsdata mv.

Den foreslåede bestemmelse vil endvidere medføre, at væsentlige og vigtige enheder vil kunne straffes med bøde, hvis de overtræder underretningspligten efter den foreslåede § 12, stk. 1 og 2, eller den fastsatte procedure for underretninger i den foreslåede § 13, stk. 1 eller 2.

Den foreslåede bestemmelse vil endvidere medføre, at væsentlige og vigtige enheder vil kunne straffes med bøde, hvis de overtræder reglerne om underretning af modtagere af deres tjenester efter den foreslåede § 15.

Det foreslås i *nr. 2,* at den, der undlader at efterkomme en kompetent myndigheds afgørelse efter § 23, stk. 1, nr. 1 eller 2, straffes med bøde.

Den foreslåede bestemmelse vil indebære, at væsentlige eller vigtige enheder, der undlader at efterkomme en afgørelse om midlertidig suspension af en certificering eller godkendelse efter den foreslåede § 23, stk. 1, nr. 1, eller et midlertidigt forbud mod at udøve ledelsesfunktioner i den pågældende enhed efter den foreslåede § 23, stk. 1, nr. 2, vil kunne straffes med bøde.

Det foreslås i *nr. 3,* at den, der undlader at efterkomme påbud eller forbud efter § 22, stk. 1, nr. 3-6 eller § 25, stk. 1, nr. 3-6, straffes med bøde.

Den foreslåede bestemmelse vil indebære, at en væsentlig enhed, der undlader at efterkomme påbud eller forbud efter den foreslåede bestemmelse i § 22, stk. 1, nr. 3-6, vil kunne straffes med bøde.

Den foreslåede bestemmelse vil indebære, at en vigtig enhed, der undlader at efterkomme påbud eller forbud efter den foreslåede bestemmelse i § 25, stk. 1, nr. 3-6, vil kunne straffes med bøde.

Det foreslås i *nr. 4,* at den, der undlader at efterkomme en afgørelse efter § 16, stk. 2, § 21, stk. 1, nr. 2 eller nr. 5-7, eller § 24, stk. 1, nr. 2 eller nr. 4-6, straffes med bøde.

Den foreslåede bestemmelse vil indebære, at enhed, der ikke efterkommer en kompetent myndigheds afgørelse om informering af offentligheden om en væsentlig hændelse, eller hvordan informeringen skal ske, vil kunne straffes med bøde.

Den foreslåede bestemmelse vil endvidere indebære, at en væsentlig enhed, der ikke efterkommer en kompetent myndigheds afgørelse om tilsyns- og kontrolforanstaltninger efter § 21, stk. 1, nr. 2, eller nr. 5-7, vil kunne straffes med bøde.

Den foreslåede bestemmelse vil endelig medføre, at en vigtig enhed, der ikke efterkommer en kompetent myndigheds afgørelse om tilsyns- og kontrolforanstaltninger efter § 24, stk. 1, nr. 2 eller 4-6, vil kunne straffes med bøde.

Det foreslås i *nr. 5,* at den, der hindrer de kompetente myndigheder i at føre tilsyn efter bestemmelserne i § 21, stk. 1, nr. 1-4, eller § 24, stk. 1, nr. 1-3.

Den foreslåede bestemmelse vil endvidere indebære, at en væsentlig enhed, hindrer en kompetent myndigheds tilsyns efter § 21, stk. 1, nr. 1-4, vil kunne straffes med bøde.

Den foreslåede bestemmelse vil endelig medføre, at en vigtig enhed, der hindrer en kompetent myndigheds tilsyns efter § 24, stk. 1, nr. 1-3, vil kunne straffes med bøde.

Om valg af ansvarssubjekt henvises til lovforslagets pkt. 3.5.2.3.

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, kan fastsættes straf af bøde for overtrædelse af bestemmelserne i forskrifterne.

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, 15 og 16, 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.

De almindelige regler i straffelovens kapitel 10 om henholdsvis strafskærpende og strafformildende omstændigheder skal ligeledes iagttages ved anvendelsen af nærværende strafbestemmelser.

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 §§ 23, 24 og 26.

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. 3.5.

Til § 33

Bestemmelsens *stk. 1* fastsætter tidspunktet for lovens ikrafttræden.

Det foreslås, at loven træder i kraft den 1. juli 2025.

Det følger af artikel 41, stk. 1, i 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), 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 lidt over ni måneder efter direktivets implementeringsfrist.

Det foreslås i *stk. 2,* at senest 3 år efter lovens ikrafttræden udarbejder ministeren for samfundssikkerhed og beredskab en rapport om erfaringerne med loven, som oversendes til Folketinget.

Det er Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at denne lov bør evalueres tre år efter lovens ikrafttræden. Evalueringen vil bl.a. skulle omfatte offentlige myndigheders efterlevelse af loven.

Til brug for rapporten vil der blive indhentet bidrag fra de kompetente myndigheder og erhvervslivet. Den samlede rapport vil blive sendt til Folketinget.

Det foreslås i *stk. 3,* at oplysningerne efter §§ 9, stk. 1 og § 10, stk. 1, skal indgives senest den 1. oktober 2025. Der er tale om en overgangsbestemmelse.

Det henvises i den forbindelse til den foreslåede bestemmelse i § 9, stk. 2 og § 10, stk. 2.

Det foreslås i *stk. 4,* at lov nr. 436 af 8. maj 2018 om net- og informationssikkerhed for domænenavnssystemer og visse digitale tjenester ophæves.

Bestemmelsen vil indebære, at loven ophæves den 1. juli 2025.

Det foreslås i *stk. 5,* at lov nr. 437 af 8. maj 2018 om

sikkerhed i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter mv. ophæves.

Bestemmelsen vil indebære, at loven ophæves den 1. januar 2025. Med lovens ophævelse bortfalder bekendtgørelse nr. 454 af 8. maj 2018 om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter.

Det foreslås i *stk. 6,* at lov nr. 440 af 8. maj 2018 om krav til sikkerhed i net- og informationssystemer inden for sundhedssektoren ophæves.

Bestemmelsen vil indebære, at loven ophæves den 1. januar 2025. Med lovens ophævelse bortfalder de bekendtgørelser, der er udstedt i medfør af loven.

Det foreslås i *stk. 7,* at lov nr. 441 af 8. maj 2018 om sikkerhed i net- og informationssystemer i transportsektoren ophæves.

Bestemmelsen vil indebære, at loven ophæves den 1. januar 2025.

Til § 34

Det foreslås i *§ 34,* at loven ikke gælder for Færøerne og Grønland, men kan ved kongelig anordning helt eller delvist sættes i kraft for Færøerne og Grønland med de ændringer, som de henholdsvis færøske og grønlandske forhold tilsiger. Lovens bestemmelser kan sættes i kraft på forskellige tidspunkter.

Bestemmelsen vedrører lovens territoriale gyldighed og indebærer, at loven ikke gælder for Færøerne og Grønland, men at loven ved kongelig anordning helt eller delvist kan sættes i kraft for Færøerne og Grønland med de ændringer, som de henholdsvis færøske og grønlandske forhold tilsiger.

Loven vil alene kunne sættes helt eller delvist i kraft for Færøerne og Grønland for så vidt angår sektorer og delsektorer, som dækker områder, der ikke er overtagne af de færøske og grønlandske myndigheder.

Lovens bestemmelser vil kunne sættes i kraft på forskellige tidspunkter.