# Forslag

# til

# Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau[1]

## Kapitel 1
*Anvendelsesområde, jurisdiktion, definitioner m.v.*

**§ 1.** Loven finder anvendelse på offentlige og private enheder, der er omfattet af anvendelsesområdet i artikel 2 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), jf. dog stk. 2-7 og § 2.

*Stk. 2.* Loven finder ikke anvendelse på enheder i energisektoren. Loven finder endvidere ikke anvendelse på enheder i det omfang, de er omfattet af lov om cybersikkerhed i telesektoren eller er udpeget i medfør af § 333, stk. 1, i lov om finansiel virksomhed. Dog gælder lovens § 17 for disse enheder.

*Stk. 3.* Vedkommende minister kan inden for sit område bestemme, at loven helt eller delvist 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.

*Stk. 4.* Vedkommende minister kan inden for sit område træffe afgørelse om at undtage specifikke enheder, såfremt enhederne udfører aktiviteter

[1] Loven gennemfører dele af Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen, om ændring af forordning (EU) nr. 910/2014 og direktiv (EU) 2018/1972 og om ophævelse af direktiv (EU) 2016/1148 (NIS 2-direktivet), EU-Tidende 2022, nr. L 333, side 80. Direktivet er medtaget som bilag 1 til loven.

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.

*Stk. 5.* Stk. 4 finder ikke anvendelse, hvor en enhed fungerer som tillidstjenesteudbyder.

*Stk. 6.* Offentlige og private enheder kan, uanset om de er omfattet af lovens anvendelsesområde, give frivillig underretning til CSIRT'en efter § 14 og deltage i den frivillige udveksling af oplysninger mellem enheder i cybersikkerhedsfællesskaber efter § 19.

*Stk. 7.* Vedkommende minister kan inden for sit område 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 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.

*Stk. 4.* Er en enhed omfattet af 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. Hvis der ikke er udpeget en repræsentant efter 1. pkt., anses enheden for at høre under jurisdiktionen i de medlemsstater, hvor tjenesterne udbydes.

*Stk. 5.* Modtages der en anmodning om gensidig bistand, jf. § 27, 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.

**§ 3.** I denne lov forstås ved:

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 eller 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) 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.
22) 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.
23) 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.
24) 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 CSIRT på enhedens sted for så vidt angår denne enheds forpligtelser i henhold til NIS 2-direktivet.
25) 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.

26) Sårbarhed: En svaghed, modtagelighed eller fejl ved IKT-produkter eller -tjenester, som kan udnyttes af en cybertrussel.
27) 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, eller
    b) generering, kontrol og validering af certifikater for websteds autentifikation, eller
    c) bevaring af elektroniske signaturer, segl eller certifikater relateret til disse tjenester.
28) Tillidstjenesteudbyder: En fysisk eller juridisk person, der udbyder en eller flere tillidstjenester, enten som en kvalificeret eller ikke-kvalificeret tillidstjenesteudbyder.
29) 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.
30) Udbyder af administrerede sikkerhedstjenester: En udbyder af administrerede tjenester, der udfører eller yder assistance til aktiviteter vedrørende styring af cybersikkerhedsrisici.
31) 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.
32) 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 materiel eller immateriel skade.

**§ 4.** Enheder af en type, som er omfattet af bilag 2, og som overskrider tærsklerne for mellemstore virksomheder, anses for at være væsentlige enheder.

*Stk. 2.* I det omfang kommuner eller regioner måtte udføre opgaver som udbydere af offentlige elektroniske kommunikationsnet eller udbydere af offentligt tilgængelige elektroniske kommunikationstjenester, og er af en størrelse, der svarer til tærsklerne for mellemstore virksomheder, anses de for at være væsentlige enheder.

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

1) Kvalificerede tillidstjenesteudbydere og topdomæneadministratorer samt DNS-tjenesteudbydere.
2) Statslige myndigheder.
3) Enheder, der er identificeret som kritiske enheder i henhold til lov om kritiske enheders modstandsdygtighed.
4) Enheder, der inden den 16. januar 2023 er blevet identificeret som operatører af væsentlige tjenester i overensstemmelse med den tidligere gældende regulering, der gennemførte 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.
5) Øvrige enheder af en type, som er omfattet af bilag 2 og 3, 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.
   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 inden for sit område fastsætte nærmere regler om kriterier for, hvornår enheder er omfattet af stk. 3, nr. 5.

**§ 5.** Enheder, der ikke opfylder kriterierne for at være væsentlige enheder i medfør af § 4, stk. 1-3, anses for at være vigtige enheder.

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

*Stk. 3.* Enheder der leverer domænenavnsregistreringstjenester anses hverken for at være væsentlige eller vigtige enheder.

## 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 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.
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 finder, at den ikke overholder krav til foranstaltningerne i stk. 1 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 inden for sit område efter forhandling med forsvarsministeren fastsætte nærmere regler om krav til foranstaltninger efter stk. 1.

**§ 7.** 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 og sikrer, at foranstaltningerne har den fornødne effekt.

*Stk. 2.* Medlemmerne af en væsentlig eller vigtig enheds ledelsesorgan skal deltage i relevante kurser om styring af cybersikkerhedsrisici og overveje at tilbyde tilsvarende kurser til sine ansatte.

**§ 8.** Vedkommende minister kan inden for sit område efter forhandling med forsvarsministeren 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. Produktet kan

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

## Kapitel 3
*Registrerings- og underretningspligter*

### *Registreringspligter*

**§ 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) 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. bilag 2 eller 3.
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.
5) De medlemsstater i Den Europæiske Union, hvor enheden leverer tjenester.

*Stk. 2.* Oplysningerne efter stk. 1 skal indgives senest den 17. januar 2025. En enhed, der omfattes af lovens anvendelsesområde efter denne dato, skal indgive oplysningerne 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:

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. bilag 2 og 3.
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.

*Stk. 2.* Oplysningerne efter stk. 1 skal indgives senest den 17. april 2025. En enhed, der omfattes af lovens anvendelsesområde efter denne dato, skal indgive oplysningerne 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:

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 uden unødigt ophold og under alle omstændigheder 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.* Digitaliserings- og ligestillingsministeren kan fastsætte regler om krav til politikker og procedurer efter stk. 3.

*Underretningspligter og frivillig underretning*

**§ 12.** Væsentlige og vigtige enheder skal uden unødigt ophold underrette den relevante kompetente myndighed og CSIRT'en 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

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 materiel eller immateriel skade.

*Stk. 3.* Vedkommende minister kan inden for sit område efter forhandling med forsvarsministeren fastsætte nærmere regler om, hvornår en hændelse anses for at være væsentlig.

**§ 13.** 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.
   d) De eventuelle grænseoverskridende virkninger af hændelsen.
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.

*Stk. 2.* Tillidstjenesteudbydere skal i tilfælde af væsentlige hændelser afgive underretningen efter stk. 1, nr. 2, uden unødigt ophold og under alle

omstændigheder 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, 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.

**§ 14.** Offentlige og private enheder kan 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 § 12. CSIRT'en kan prioritere håndteringen af underretninger, der er modtaget i medfør af § 12.

*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.** I relevant omfang underretter væsentlige og vigtige enheder 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 på den pågældende trussel. Hvor det er relevant, skal enhederne også informere de pågældende modtagere om den væsentlige cybertrussel.

**§ 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 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, kræve, at den relevante enhed informerer offentligheden om den væsentlige hændelse.

*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 givet fald 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.* Forsvarsministeren kan fastsætte nærmere regler om rapportering efter stk. 1.

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

*Stk. 2.* Væsentlige og vigtige enheder, der indgår i eller udtræder af cybersikkerhedsfællesskaber efter stk. 1, skal underrette CSIRT'en herom.

## Kapitel 6
*Tilsyn og håndhævelse*

### *Kompetente myndigheder*

**§ 20.** Vedkommende minister fastsætter inden for sit område regler om hvilken myndighed, der skal varetage funktionen som kompetent myndighed inden for en given sektor eller delsektor, jf. lovens bilag 2 og 3.

*Stk. 2.* For at sikre operationel uafhængighed ved tilsyn med den offentlige forvaltning, kan digitaliserings- og ligestillingsministeren efter forhandling med en anden minister fastsætte regler om, at tilsyn med Digitaliserings- og Ligestillingsministeriet og underliggende myndigheder helt eller delvist overlades til den pågældende minister.

*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 ud fra en konkret vurdering af omstændighederne i hver enkelt sag anvende følgende tilsynsforanstaltninger over for en væsentlig enhed:

1) Foretage kontrol på stedet og foretage 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 ad hoc.
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 med kravet og præcisere, hvilke oplysninger der kræves udleveret.

*Stk. 3.* Den kompetente myndighed kan stille nærmere krav om, hvordan og i hvilken form oplysningerne eller materialet nævnt i stk. 1, nr. 5-7, skal afgives.

**§ 22.** En kompetent myndighed kan ud fra en konkret vurdering af omstændighederne i hver enkelt sag anvende følgende håndhævelsesforanstaltninger over for en væsentlig enhed:

1) Påbyde enheden at træffe foranstaltninger, der er nødvendige for at forhindre eller afhjælpe en hændelse.
2) Meddele enheden påbud og forbud for at sikre overholdelsen af de krav, der er fastsat i loven eller regler udstedt i medfør af loven.
3) 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 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.
4) Påbyde enheden at gennemføre de anbefalinger, der er fremsat i forbindelse med en gennemført sikkerhedsaudit.

5) Påbyde enheden at udpege en person med ansvar for i en nærmere fastsat periode at føre tilsyn med enhedens overholdelse af §§ 6, 12, 13, 15 og 16, samt regler udstedt i medfør heraf.
6) 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 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 suspendere en certificering eller godkendelse vedrørende dele af eller alle de relevante tjenester, 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.* Midlertidige 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 af enheden eller den fysiske person, afgørelsen vedrører, forlanges indbragt for domstolene. Den myndighed, som vedkommende minister bemyndiger hertil, anlægger i givet fald sag inden for rammerne af den civile retspleje mod den enhed eller person, som har forlangt sagen indbragt.

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

*Stk. 5.* Vedkommende minister kan efter forhandling med forsvarsministeren fastsætte nærmere regler om, hvilke certificeringer og godkendelser der er omfattet af stk. 1, nr. 1.

*Vigtige enheder*

**§ 24.** De kompetente myndigheder fører på deres respektive områder reaktivt tilsyn med vigtige enheders overholdelse af denne lov og regler udstedt i medfør af loven. En kompetent myndighed kan som led i sit tilsyn, hvis der er indikationer på, at en vigtig enhed ikke overholder eller ikke har overholdt denne lov eller regler udstedt i medfør af loven, ud fra en konkret vurdering af omstændighederne i hver enkelt sag anvende følgende tilsynsforanstaltninger:

1) Foretage kontrol på stedet.

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.

*Stk. 3.* Den kompetente myndighed kan stille nærmere krav om, hvordan og i hvilken form oplysningerne eller materialet nævnt i stk. 1, nr. 4-6, skal afgives.

**§ 25.** En kompetent myndighed kan ud fra en konkret vurdering af omstændighederne i hver enkelt sag anvende følgende håndhævelsesforanstaltninger over for en vigtig enhed:

1) Meddele enheden påbud og forbud for at sikre overholdelsen af de krav, der er fastsat i loven eller regler udstedt i medfør af loven.
2) 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 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.
3) Påbyde enheden at gennemføre de anbefalinger, der er fremsat i forbindelse med en gennemført sikkerhedsaudit.
4) 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, at:

1) De kompetente myndigheder via det centrale kontaktpunkt underretter 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.
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.

## Kapitel 8
*Videregivelse af oplysninger, digital kommunikation, gennemførelsesretsakter og operativ uafhængighed*

**§ 28.** De relevante 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 NIS 2-direktivet.

**§ 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 inden for sit område fastsætte regler, som er nødvendige for at gennemføre retsakter udstedt af Europa-Kommissionen i medfør af NIS 2-direktivet.

**§ 31.** Vedkommende minister kan inden for sit område efter forhandling med forsvarsministeren 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, §§ 7, 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.
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 m.v. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.

*Stk. 3.* Hvis der er pålagt en bøde for overtrædelse af Databeskyttelsesforordningen eller databeskyttelsesloven, kan der ikke pålægges en bøde for overtrædelse af denne lov eller regler udstedt i medfør af loven, hvis overtrædelsen skyldes den samme adfærd som den, der var genstand for bøden i medfør af nævnte forordning eller databeskyttelsesloven.

*Stk. 4.* Digitaliserings- og ligestillingsministeren kan fastsætte regler om, at offentlige myndigheder og institutioner m.v., som er omfattet af forvaltningslovens § 1, stk. 1 eller 2, uanset straffelovens § 27, stk. 2, kan straffes i anledning af overtrædelser, der begås ved udøvelse af virksomhed, der ikke svarer til eller kan sidestilles med virksomhed udøvet af private.

*Stk. 5.* Digitaliserings- og ligestillingsministeren kan fastsætte regler om bødeniveauer for offentlige myndigheders overtrædelse af loven.

*Stk. 6.* I regler udstedt i medfør af loven kan der fastsættes straf i form af bøde for overtrædelse af regler udstedt i medfør af loven.

## Kapitel 10
*Ikrafttrædelse*

**§ 33.** Loven træder i kraft den 1. marts 2025.

## Kapitel 11
*Ændringer i anden lovgivning*

**§ 34.** Lov nr. 436 af 8. maj 2018 om net- og informationssikkerhed for domænenavnssystemer og visse digitale tjenester ophæves.

**§ 35.** Lov nr. 437 af 8. maj 2018 om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudviklingspunkter m.v. ophæves.

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

**§ 37.** Lov nr. 441 af 8. maj 2018 om sikkerhed i net- og informationssystemer i transportsektoren ophæves.

## Kapitel 12
*Territorialbestemmelser*

**§ 38.** 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 henholdsvis færøske og grønlandske forhold tilsiger.

**Bilag 1**

# 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)**

**(EØS-relevant tekst)**

EUROPA-PARLAMENTET OG RÅDET FOR DEN EUROPÆISKE UNION HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel 114,

under henvisning til forslag fra Europa-Kommissionen,

efter fremsendelse af udkast til lovgivningsmæssig retsakt til de nationale parlamenter,

under henvisning til udtalelse fra Den Europæiske Centralbank ([1]),

under henvisning til udtalelse fra Det Europæiske Økonomiske og Sociale Udvalg ([2]),

efter høring af Regionsudvalget,

efter den almindelige lovgivningsprocedure ([3]), og

ud fra følgende betragtninger:

(1) Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 ([4]) tog sigte på at opbygge cybersikkerhedskapaciteter i hele Unionen, afbøde trusler mod net- og informationssystemer, der anvendes til at levere væsentlige tjenester i nøglesektorer, og sikre kontinuiteten af sådanne tjenester, når de står over for hændelser, og dermed bidrage til Unionens sikkerhed og til, at dens økonomi og samfund kan fungere effektivt.

(2) Siden ikrafttrædelsen af direktiv (EU) 2016/1148 er der gjort betydelige fremskridt med hensyn til at øge Unionens niveau af cyberrobusthed. Evalueringen af nævnte direktiv har vist, at det har fungeret som katalysator for den institutionelle og lovgivningsmæssige tilgang til cybersikkerhed i Unionen og har banet vejen for en betydelig holdningsændring. Nævnte direktiv har sikret færdiggørelsen af nationale rammer for sikkerheden i net- og informationssystemer ved at fastlægge nationale stra-

tegier for sikkerheden i net- og informationssystemer og etablere nationale kapaciteter og ved at gennemføre lovgivningsmæssige foranstaltninger, der omfatter væsentlige infrastrukturer og enheder, som hver medlemsstat har identificeret. Direktiv (EU) 2016/1148 har også bidraget til samarbejdet på EU-plan gennem oprettelsen af samarbejdsgruppen og netværket af nationale enheder, der håndterer IT-sikkerhedshændelser. Uanset disse resultater har evalueringen af direktiv (EU) 2016/1148 afsløret iboende mangler, der forhindrer det i effektivt at tackle aktuelle og nye cybersikkerhedsudfordringer.

(3) Net- og informationssystemer har udviklet sig til et centralt element i hverdagen med den hurtige digitale omstilling og forbundethed i samfundet, herunder i forbindelse med grænseoverskridende udvekslinger. Denne udvikling har ført til en udvidelse af antallet og typen af cybertrusler og skabt nye udfordringer, som kræver tilpassede, koordinerede og innovative svar i alle medlemsstater. Antallet, omfanget, den avancerede karakter, hyppigheden og virkningen af hændelser er stigende og udgør en alvorlig trussel mod net- og informationssystemernes funktion. Som følge heraf kan hændelser hindre udøvelsen af økonomiske aktiviteter i det indre marked, medføre økonomiske tab, underminere brugernes tillid og forårsage store skader på Unionens økonomi og samfund. Cybersikkerhedsberedskab og -effektivitet er derfor mere afgørende for et velfungerende indre marked end nogensinde før. Cybersikkerhed er desuden en vigtig katalysator for, at mange kritiske sektorer kan tage den digitale omstilling til sig med et positivt resultat og fuldt ud kan udnytte de økonomiske, sociale og bæredygtige fordele ved digitalisering.

(4) Retsgrundlaget for direktiv (EU) 2016/1148 var artikel 114 i traktaten om Den Europæiske Unions funktionsmåde (TEUF), hvis formål er det indre markeds oprettelse og funktion ved at styrke foranstaltninger til indbyrdes tilnærmelse af de nationale regler. De cybersikkerhedskrav, der pålægges enheder, som leverer tjenester eller som udfører aktiviteter, der er økonomisk betydningsfulde, varierer betydeligt fra medlemsstat til medlemsstat med hensyn til typen af krav, detaljeringsgrad og tilsynsmetode. Disse forskelle medfører yderligere omkostninger og skaber vanskeligheder for enheder, der udbyder varer eller tjenester på tværs af grænserne. Krav, der stilles af en medlemsstat, og som er forskellige fra eller endog i konflikt med dem, der er pålagt af en anden medlemsstat, kan påvirke sådanne grænseoverskridende aktiviteter i væsentlig grad. Desuden har muligheden for en utilstrækkelig udformning eller gennemførelse af cybersikkerhedskravene i én medlemsstat sandsynligvis konsekvenser for cybersikkerhedsniveauet i andre medlemsstater, navnlig i betragtning af intensiteten af grænseoverskridende udvekslinger. Evalueringen af direktiv (EU) 2016/1148 har vist, at der er store forskelle i medlemsstaternes gennemførelse af det, herunder med hensyn til dets anvendelsesom-

råde, hvis afgrænsning i vid udstrækning blev overladt til medlemsstaternes skøn. Direktiv (EU) 2016/1148 gav også medlemsstaterne meget vide skønsbeføjelser med hensyn til gennemførelsen af de sikkerheds- og hændelsesrapporteringsforpligtelser, der er fastsat deri. Disse forpligtelser blev derfor gennemført på vidt forskellige måder på nationalt plan. Der er lignende forskelle i gennemførelsen af bestemmelserne i direktiv (EU) 2016/1148 om tilsyn og håndhævelse.

(5) Alle disse forskelle medfører en fragmentering af det indre marked og kan have en negativ indvirkning på dets funktion og navnlig påvirke den grænseoverskridende levering af tjenester og cyberrobustheden som følge af anvendelsen af forskellige foranstaltninger. Disse forskelle 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. Dette direktiv sigter mod at fjerne sådanne store forskelle mellem medlemsstaterne, navnlig ved at fastsætte minimumsregler for, hvordan en koordineret reguleringsramme fungerer, ved at fastlægge mekanismer for effektivt samarbejde mellem de ansvarlige myndigheder i hver medlemsstat, ved at ajourføre listen over sektorer og aktiviteter, der er omfattet af cybersikkerhedsforpligtelser, og ved at tilvejebringe effektive retsmidler og håndhævelsesforanstaltninger, der er afgørende for effektiv håndhævelse af disse forpligtelser. Derfor bør direktiv (EU) 2016/1148 ophæves og erstattes af nærværende direktiv.

(6) Med ophævelsen af direktiv (EU) 2016/1148 bør anvendelsesområdet for de enkelte sektorer udvides til at omfatte en større del af økonomien for at give en omfattende dækning af sektorer og tjenester af vital betydning for vigtige samfundsmæssige og økonomiske aktiviteter i det indre marked. Nærværende direktiv sigter navnlig mod at afhjælpe manglerne i differentieringen mellem operatører af væsentlige tjenester og udbydere af digitale tjenester, som har vist sig at være forældet, da den ikke afspejler sektorernes eller tjenesternes betydning for de samfundsmæssige og økonomiske aktiviteter i det indre marked.

(7) I henhold til direktiv (EU) 2016/1148 havde medlemsstaterne ansvaret for at identificere de enheder, der opfyldte kriterierne for at blive betragtet som operatører af væsentlige tjenester. For at fjerne de store forskelle mellem medlemsstaterne i denne henseende og garantere retssikkerhed for så vidt angår foranstaltningerne til styring af cybersikkerhedsrisici og rapporteringsforpligtelserne for alle relevante enheder bør der fastsættes et ensartet kriterium for, hvilke enheder der er omfattet af nærværende direktivs anvendelsesområde. Dette kriterium bør bestå i anvendelsen af en regel om størrelsesloft, ifølge hvilken alle enheder, der udgør mellemstore virksomheder i henhold til artikel 2 i bilaget til Kommissionens henstilling 2003/361/EF ([5]), eller overskrider tærsklerne for mellemstore virksomheder fastsat i nævnte artikels stk. 1, og som opererer inden for

de sektorer og leverer de typer tjenester eller udfører de aktiviteter, der er omfattet af nærværende direktiv, er omfattet af dets anvendelsesområde. Medlemsstaterne bør også sørge for, at visse små virksomheder og mikrovirksomheder, som defineret i nævnte bilags artikel 2, stk. 2 og 3, der opfylder specifikke kriterier, der tyder på en central rolle for samfundet eller økonomien eller bestemte sektorer eller typer af tjenester, omfattes af nærværende direktivs anvendelsesområde.

(8) 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.

(9) Medlemsstaterne bør kunne træffe de nødvendige foranstaltninger for at sikre beskyttelsen af væsentlige nationale sikkerhedsinteresser, opretholde den offentlige orden og sikkerhed samt tillade forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger. Med henblik herpå bør medlemsstater kunne undtage specifikke enheder, der udfører aktiviteter inden for national sikkerhed, offentlig sikkerhed, forsvar eller retshåndhævelse, herunder forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger, fra visse forpligtelser, der er fastsat i dette direktiv, for så vidt angår disse aktiviteter. Hvor en enhed udelukkende leverer tjenester til en offentlig forvaltningsenhed, der er udelukket fra dette direktivs anvendelsesområde, bør medlemsstater kunne undtage denne enhed fra visse forpligtelser, der er fastsat i dette direktiv, for så vidt angår disse tjenester. Endvidere bør ingen medlemsstat 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. 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 begræns-

ninger 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.

(10) Selv om dette direktiv finder anvendelse på enheder, der beskæftiger sig med produktion af elektricitet fra kernekraftværker, kan nogle af disse aktiviteter være knyttet til den nationale sikkerhed. Hvor det er tilfældet, bør en medlemsstat kunne udøve sit ansvar for at beskytte sin nationale sikkerhed med hensyn til disse aktiviteter, herunder aktiviteter inden for den nukleare værdikæde, i overensstemmelse med traktaterne.

(11) Nogle enheder udfører aktiviteter inden for national sikkerhed, offentlig sikkerhed, forsvar eller retshåndhævelse, herunder forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger, og leverer samtidig tillidstjenester. Tillidstjenesteudbydere, der er omfattet af anvendelsesområdet for Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 ([6]), bør være omfattet af dette direktivs anvendelsesområde for at sikre samme niveau af sikkerhedskrav og tilsyn som det, der tidligere var fastsat i nævnte forordning, for så vidt angår tillidstjenesteudbydere. I overensstemmelse med udelukkelsen af visse specifikke tjenester fra forordning (EU) nr. 910/2014 bør dette direktiv ikke finde anvendelse på levering af tillidstjenester, der udelukkende anvendes i lukkede systemer i henhold til national ret eller aftaler mellem et defineret sæt deltagere.

(12) Postbefordrende virksomheder som defineret i Europa-Parlamentets og Rådets direktiv 97/67/EF ([7]), herunder udbydere af kurertjenester, bør være omfattet af nærværende direktiv, hvis de leverer mindst ét led i postbefordringskæden, navnlig indsamling, sortering, transport eller omdeling, herunder afhentning, samtidig med at der tages hensyn til omfanget af deres afhængighed af net- og informationssystemer. Transporttjenester, der ikke udføres i forbindelse med et af disse trin, bør udelukkes fra anvendelsesområdet for posttjenester.

(13) I betragtning af intensiveringen og den stadig mere sofistikerede karakter af cybertrusler bør medlemsstaterne bestræbe sig på at sikre, at enheder, der er udelukket fra dette direktivs anvendelsesområde, opnår et højt cybersikkerhedsniveau, og på at støtte gennemførelsen af tilsvarende foranstaltninger til styring af cybersikkerhedsrisici, der afspejler disse enheders følsomme karakter.

(14) EU-retten om databeskyttelse og privatlivets fred finder anvendelse på enhver behandling af personoplysninger i henhold til dette direktiv. Navnlig berører dette direktiv ikke Europa-Parlamentets og Rådets direktiv (EU) 2016/679 ([8]) og Europa-Parlamentets og Rådets direktiv 2002/58/EF ([9]). Nærværende direktiv bør derfor ikke berøre bl.a. de opgaver og beføjelser, der påhviler de myndigheder, der har kompetence

til at overvåge overholdelsen af gældende EU-ret om databeskyttelse og om privatlivets fred.

(15) Enheder, der er omfattet af dette direktiv med henblik på overholdelse af foranstaltninger til styring af cybersikkerhedsrisici og rapporteringsforpligtelser, bør inddeles i to kategorier, væsentlige enheder og vigtige enheder, der afspejler, i hvilket omfang de er kritiske for så vidt angår deres sektor eller den type tjenester, de leverer, samt deres størrelse. I den henseende bør der tages behørigt hensyn til eventuelle relevante sektorspecifikke risikovurderinger eller vejledning fra de kompetente myndigheder, hvor det er relevant. Tilsyns- og håndhævelsesordningerne for disse to kategorier af enheder bør differentieres for at sikre en fair balance mellem risikobaserede krav og forpligtelser på den ene side og den administrative byrde, der følger af tilsynet med overholdelsen, på den anden side.

(16) For at undgå, at enheder, der har partnervirksomheder eller er tilknyttede virksomheder, betragtes som væsentlige eller vigtige enheder, hvor dette ville være uforholdsmæssigt, kan medlemsstaterne tage hensyn til den grad af uafhængighed, som en enhed har i forhold til sine partnervirksomheder eller tilknyttede virksomheder, når artikel 6, stk. 2, i bilaget til henstilling 2003/361/EF anvendes. Medlemsstaterne kan navnlig tage hensyn til, at en enhed er uafhængig af sine partnervirksomheder eller tilknyttede virksomheder med hensyn til de net- og informationssystemer, som enheden anvender i forbindelse med leveringen af sine tjenester, og med hensyn til de tjenester, som enheden leverer. På dette grundlag kan medlemsstaterne, hvor det er hensigtsmæssigt, anse en sådan enhed for ikke at udgøre en mellemstor virksomhed i henhold til artikel 2, i bilaget til henstilling 2003/361/EF, eller for ikke at overskride tærsklerne for en mellemstor virksomhed fastsat i nævnte artikels stk. 1, hvis den pågældende enhed i betragtning af dennes grad af uafhængighed ikke ville være blevet anset for at udgøre en mellemstor virksomhed eller at overskride disse tærskler, hvis kun dens egne data var blevet taget i betragtning. Dette berører ikke forpligtelserne fastsat i dette direktiv for partnervirksomheder og tilknyttede virksomheder, som er omfattet af dette direktivs anvendelsesområde.

(17) Medlemsstaterne bør kunne bestemme, at enheder, der inden dette direktivs ikrafttræden er identificeret som operatører af væsentlige tjenester i overensstemmelse med direktiv (EU) 2016/1148, skal betragtes som væsentlige enheder.

(18) For at sikre et klart overblik over de enheder, der er omfattet af dette direktivs anvendelsesområde, bør medlemsstaterne udarbejde en liste over væsentlige og vigtige enheder samt enheder, der leverer domænenavnsregistreringstjenester. Med henblik herpå bør medlemsstaterne

kræve, at enheder mindst indgiver følgende oplysninger til de kompetente myndigheder: navn, adresse og ajourførte kontaktoplysninger, herunder e-mailadresser, IP-intervaller og telefonnumre for enheden, og i givet fald den relevante sektor og delsektor omhandlet i bilagene samt i givet fald en liste over de medlemsstater, hvor de leverer tjenester, der er omfattet af dette direktivs anvendelsesområde. Med henblik herpå bør Kommissionen med bistand fra Den Europæiske Unions Agentur for Cybersikkerhed (ENISA) uden unødigt ophold fastlægge retningslinjer og skabeloner vedrørende forpligtelsen til at indgive oplysninger. For at lette udarbejdelsen og ajourføringen af listen over væsentlige og vigtige enheder samt enheder, der leverer domænenavnsregistreringstjenester, bør medlemsstaterne kunne indføre nationale mekanismer, hvorigennem enheder kan registrere sig selv. Hvor der findes registre på nationalt plan, kan medlemsstaterne træffe afgørelse om passende mekanismer, der gør det muligt at identificere enheder, der er omfattet af dette direktivs anvendelsesområde.

(19) Medlemsstaterne bør være ansvarlige for mindst at oplyse Kommissionen om antallet af væsentlige og vigtige enheder for hver sektor og delsektor omhandlet i bilagene, samt give relevante oplysninger om antallet af identificerede enheder og den bestemmelse blandt dem, der er fastsat i dette direktiv, på grundlag af hvilken de blev identificeret og den type tjeneste de leverer. Medlemsstaterne opfordres til at udveksle oplysninger med Kommissionen om væsentlige og vigtige enheder og, i tilfælde af en omfattende cybersikkerhedshændelse, relevante oplysninger såsom navnet på den berørte enhed.

(20) Kommissionen bør i samarbejde med samarbejdsgruppen og efter høring af de relevante interessenter fastlægge retningslinjer for gennemførelsen af de kriterier, der gælder for mikrovirksomheder og små virksomheder, for vurderingen af, om de er omfattet af dette direktivs anvendelsesområde. Kommissionen bør også sikre, at der gives passende vejledning til mikrovirksomheder og små virksomheder, som hører under dette direktivs anvendelsesområde. Kommissionen bør med bistand fra medlemsstaterne stille oplysninger til rådighed for mikrovirksomheder og små virksomheder i denne henseende.

(21) Kommissionen vil kunne yde vejledning med henblik på at bistå medlemsstaterne med gennemførelse af dette direktivs bestemmelser om anvendelsesområde og evaluering af proportionaliteten af de foranstaltninger, der skal træffes i henhold til dette direktiv, navnlig for så vidt angår enheder med komplekse forretningsmodeller eller driftsmiljøer, hvorved en enhed samtidig kunne opfylde de kriterier, der er tildelt både væsentlige og vigtige enheder, eller samtidig kunne udføre aktiviteter, hvoraf nogle falder inden for og nogle uden for dette direktivs anvendelsesområde.

(22) Dette direktiv fastsætter referencescenariet for foranstaltninger til styring af cybersikkerhedsrisici og rapporteringsforpligtelser på tværs af de sektorer, der er omfattet af dets anvendelsesområde. For at undgå fragmentering af EU-retsakters cybersikkerhedsbestemmelser bør Kommissionen, hvor yderligere sektorspecifikke EU-retsakter vedrørende foranstaltninger til styring af cybersikkerhedsrisici og rapporteringsforpligtelser vedrørende cybersikkerhed anses for nødvendige for at sikre et højt cybersikkerhedsniveau i hele Unionen, vurdere, hvorvidt sådanne yderligere bestemmelser vil kunne fastsættes i en gennemførelsesretsakt til dette direktiv. Er sådan en gennemførelsesretsakt ikke egnede til dette formål, vil sektorspecifikke EU-retsakter kunne bidrage til at sikre et højt cybersikkerhedsniveau i hele Unionen, samtidig med at der fuldt ud tages hensyn til de berørte sektorers specificiteter og kompleksiteter. Med henblik herpå er dette direktiv ikke til hinder for, at der vedtages yderligere sektorspecifikke EU-retsakter, der omhandler foranstaltninger til styring af cybersikkerhedsrisici og rapporteringsforpligtelser, der tager behørigt hensyn til behovet for en omfattende og sammenhængende ramme for cybersikkerhed. Dette direktiv berører ikke de eksisterende gennemførelsesbeføjelser, der er tillagt Kommissionen inden for en række sektorer, herunder transport og energi.

(23) Hvor en sektorspecifik EU-retsakt indeholder bestemmelser, der 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 dette direktiv, bør de pågældende bestemmelser, herunder om tilsyn og håndhævelse, finde anvendelse på sådanne enheder. Hvis en sektorspecifik EU-retsakt ikke omfatter alle enheder i en specifik sektor, der er omfattet af dette direktivs anvendelsesområde, bør de relevante bestemmelser i dette direktiv fortsat finde anvendelse på de enheder, der ikke er omfattet af nævnte retsakt.

(24) Hvor bestemmelser i en sektorspecifik EU-retsakt kræver, at væsentlige eller vigtige enheder overholder rapporteringsforpligtelser med en virkning, der mindst svarer til de rapporteringsforpligtelser, der er fastsat i dette direktiv, bør der sikres sammenhæng og effektivitet i håndteringen af hændelsesunderretninger. Med henblik herpå bør bestemmelserne vedrørende hændelsesunderretninger i den sektorspecifikke EU-retsakt give CSIRT'erne, de kompetente myndigheder eller de centrale kontaktpunkter for cybersikkerhed (det centrale kontaktpunkt) i henhold til dette direktiv øjeblikkelig adgang til de hændelsesunderretninger, der indgives i overensstemmelse med den sektorspecifikke EU-retsakt. En sådan øjeblikkelig adgang kan navnlig sikres, hvis hændelsesunderretninger uden unødigt ophold sendes til CSIRT'en, den kompetente myn-

dighed eller det centrale kontaktpunkt i henhold til dette direktiv. Medlemsstaterne bør, hvor det er hensigtsmæssigt, indføre en automatisk og direkte rapporteringsmekanisme, der sikrer systematisk og øjeblikkelig udveksling af oplysninger med CSIRT'er, de kompetente myndigheder eller de centrale kontaktpunkter vedrørende håndtering af sådanne hændelsesunderretninger. Med henblik på at forenkle rapporteringen og gennemføre den automatiske og direkte rapporteringsmekanisme vil medlemsstaterne i overensstemmelse med den sektorspecifikke EU-retsakt kunne anvende et enkelt indgangspunkt.

(25) Sektorspecifikke EU-retsakter, der kræver foranstaltninger til styring af cybersikkerhedsrisici eller rapporteringsforpligtelser med en virkning, der mindst svarer til dem, der er fastsat i dette direktiv, vil kunne fastsætte, at de kompetente myndigheder i henhold til sådanne retsakter udøver deres tilsyns- og håndhævelsesbeføjelser i forbindelse med sådanne foranstaltninger eller forpligtelser med bistand fra de kompetente myndigheder i henhold til dette direktiv. De berørte kompetente myndigheder vil kunne etablere samarbejdsordninger med henblik herpå. Sådanne samarbejdsordninger vil bl.a. kunne præcisere procedurerne for koordinering af tilsynsaktiviteter, herunder procedurerne for undersøgelser og kontrol på stedet i overensstemmelse med national ret og en mekanisme for udveksling af relevante oplysninger om tilsyn og håndhævelse mellem de kompetente myndigheder, herunder adgang til cyberrelaterede oplysninger, som de kompetente myndigheder i henhold til dette direktiv anmoder om.

(26) Hvor sektorspecifikke EU-retsakter kræver eller skaber incitamenter for enheder til at underrette om væsentlige cybertrusler, bør medlemsstaterne også tilskynde til udveksling af væsentlige cybertrusler med CSIRT'erne, de kompetente myndigheder eller de centrale kontaktpunkter i henhold til dette direktiv for at sikre, at disse organer i højere grad er opmærksomme på cybertrusselsbilledet, og for at sætte dem i stand til at reagere effektivt og rettidigt, såfremt de væsentlige cybertrusler bliver til virkelighed.

(27) Fremtidige sektorspecifikke EU-retsakter bør tage behørigt hensyn til de definitioner og tilsyns- og håndhævelsesrammer, der er fastsat i dette direktiv.

(28) Europa-Parlamentets og Rådets forordning (EU) 2022/2554 ([10]) bør betragtes som en sektorspecifik EU-retsakt i forbindelse med dette direktiv for så vidt angår finansielle enheder. Bestemmelserne i forordning (EU) 2022/2554 om risikostyring inden for informations- og kommunikationsteknologi (IKT), styring af IKT-relaterede hændelser og navnlig indberetning af større IKT-relaterede hændelser, samt om test af digital operationel modstandsdygtighed, ordninger for udveksling af oplysnin-

ger og IKT-tredjepartsrisiko bør finde anvendelse i stedet for bestemmelserne i dette direktiv. Medlemsstaterne bør derfor ikke anvende bestemmelserne i dette direktiv om risikostyrings- og rapporterings forpligtelser vedrørende cybersikkerhed samt tilsyn og håndhævelse på finansielle enheder, der er omfattet af forordning (EU) 2022/2554. Samtidig er det vigtigt at opretholde stærke forbindelser og udveksle oplysninger med den finansielle sektor i henhold til dette direktiv. Med henblik herpå giver forordning (EU) 2022/2554 de europæiske tilsynsmyndigheder (ESA'erne) og de kompetente myndigheder i henhold til nævnte forordning mulighed for at deltage i samarbejdsgruppens aktiviteter samt udveksle oplysninger og samarbejde med de centrale kontaktpunkter såvel som CSIRT'erne og de kompetente myndigheder i henhold til dette direktiv. De kompetente myndigheder i henhold til forordning (EU) 2022/2554 bør også fremsende oplysninger om større IKT-relaterede hændelser og, hvor det er relevant, væsentlige cybertrusler til CSIRT'erne, de kompetente myndigheder eller de centrale kontaktpunkter i henhold til dette direktiv. Dette kan opnås ved at sikre øjeblikkelig adgang til hændelsesunderretninger og videresende af dem enten direkte eller via et enkelt indgangspunkt. Desuden bør medlemsstaterne fortsat medtage den finansielle sektor i deres cybersikkerhedsstrategier, og CSIRT'er kan dække den finansielle sektor i deres aktiviteter.

(29) For at undgå huller mellem eller overlapning af cybersikkerhedsforpligtelser, der pålægges enheder i luftfartssektoren, bør nationale myndigheder i henhold til Europa-Parlamentets og Rådets forordning (EF) nr. 300/2008 ([11]) og (EU) 2018/1139 ([12]), og de kompetente myndigheder i henhold til dette direktiv samarbejde om gennemførelsen af foranstaltninger til styring af cybersikkerhedsrisici og tilsynet med overholdelsen af disse foranstaltninger på nationalt plan. En enheds overholdelse af sikkerhedskravene i forordning (EF) nr. 300/2008 og (EU) 2018/1139 og i de relevante delegerede retsakter og gennemførelsesretsakter, der er vedtaget i henhold til nævnte forordninger, vil af de kompetente myndigheder i henhold til dette direktiv kunne anses for at udgøre opfyldelse af de tilsvarende krav, der er fastsat i dette direktiv.

(30) I betragtning af de indbyrdes forbindelser mellem cybersikkerhed og enheders fysiske sikkerhed bør der sikres en sammenhængende tilgang mellem Europa-Parlamentets og Rådets direktiv (EU) 2022/2557 ([13]) og nærværende direktiv. Med henblik herpå bør enheder identificeret som kritiske enheder i henhold til direktiv (EU) 2022/2557 betragtes som væsentlige enheder i henhold til nærværende direktiv. Endvidere bør hver medlemsstat sikre, at dens nationale cybersikkerhedsstrategi skaber en politisk ramme for øget koordinering i nævnte medlemsstat mellem dens kompetente myndigheder i henhold til nærværende direktiv og dem i henhold til direktiv (EU) 2022/2557 i forbindelse med udveksling

af oplysninger om risici, cybertrusler og hændelser samt om ikke-cyberrelaterede risici, trusler og hændelser samt om udøvelse af tilsynsopgaver. De kompetente myndigheder i henhold til nærværende direktiv og de i henhold til direktiv (EU) 2022/2557 bør samarbejde og udveksle oplysninger uden unødigt ophold, navnlig vedrørende identifikation af kritiske enheder, om risici, cybertrusler og hændelser samt om ikke-cyberrelaterede risici, trusler og hændelser, der påvirker kritiske enheder, herunder cybersikkerhedsforanstaltninger og fysiske foranstaltninger, der træffes af kritiske enheder, såvel som resultaterne af tilsynsaktiviteter, der udføres med hensyn til sådanne enheder.

For at strømline tilsynsaktiviteterne mellem de kompetente myndigheder i henhold til nærværende direktiv og i henhold til direktiv (EU) 2022/2557 og for at mindske den administrative byrde mest muligt for de berørte enheder bør disse kompetente myndigheder desuden bestræbe sig på at harmonisere modeller til hændelsesunderretning og tilsynsprocesser. Hvor det er hensigtsmæssigt, bør de kompetente myndigheder i henhold til direktiv (EU) 2022/2557 kunne anmode de kompetente myndigheder i henhold til nærværende direktiv om at udøve deres tilsyns- og håndhævelsesbeføjelser med hensyn til en enhed, som er identificeret som en kritisk enhed i henhold til direktiv (EU) 2022/2557. De kompetente myndigheder i henhold til nærværende direktiv og de i henhold til direktiv (EU) 2022/2557 bør samarbejde og udveksle oplysninger, om muligt i realtid, med henblik herpå.

(31) Enheder, der tilhører sektoren for digital infrastruktur, er i det væsentlige baseret på net- og informationssystemer, og derfor bør de forpligtelser, der pålægges disse enheder i medfør af dette direktiv, på en omfattende måde omhandle sådanne systemers fysiske sikkerhed som led i deres foranstaltninger til styring af cybersikkerhedsrisici og rapporteringsforpligtelser. Da disse spørgsmål er omfattet af dette direktiv, finder forpligtelserne i kapitel III, IV og VI i direktiv (EU) 2022/2557 ikke anvendelse på sådanne enheder.

(32) Opretholdelse og bevarelse af et pålideligt, modstandsdygtigt og sikkert domænenavnesystem (DNS) er afgørende faktorer for at bevare internettets integritet og er afgørende for dets fortsatte og stabile drift, som den digitale økonomi og det digitale samfund afhænger af. Derfor bør dette direktiv finde anvendelse på topdomænenavneadministratorer og DNS-tjenesteudbydere, der skal forstås som enheder, der leverer offentligt tilgængelige rekursive domænenavnsoversættelsestjenester til internetslutbrugere eller autoritative domænenavnsoversættelsestjenester til tredjepartsbrug. Dette direktiv bør ikke finde anvendelse på rodnavneservere.

(33) Cloudcomputingtjenester bør omfatte digitale tjenester, der giver mulighed for on demand-administration og bred fjernadgang til en skalerbar og elastisk pulje af delbare computerressourcer, herunder hvor sådanne ressourcer er fordelt mellem flere lokaliteter. Computerressourcer omfatter ressourcer såsom netværk, servere og anden infrastruktur, operativsystemer, software, lagring, applikationer og tjenester. Tjenestemodellerne for cloudcomputing omfatter bl.a. infrastruktur som en service (IaaS), platform som en service (PaaS), software som en service (SaaS) og netværk som en service (NaaS). Ibrugtagningsmodellerne for cloudcomputing bør omfatte privat, samfundsmæssig, offentlig og hybrid cloud. Cloudcomputingtjeneste- og ibrugtagningsmodellerne har samme betydning som de tjeneste- og ibrugtagningsmodeller, der er defineret i ISO/IEC 17788: 2014-standarden. Cloudcomputing-brugerens mulighed for ensidigt selvforsynende databehandlingskapacitet såsom servertid eller netlagring uden nogen menneskelig interaktion fra udbyderen af cloudcomputingtjenesters side kan beskrives som on demand-administration.

Udtrykket »bred fjernadgang« anvendes til at beskrive, at cloudkapaciteten leveres over nettet og tilgås gennem mekanismer, der fremmer brugen af heterogene tynde eller tykke klientplatforme, herunder mobiltelefoner, tablets, bærbare computere og arbejdsstationer. Udtrykket »skalerbar« henviser til databehandlingsressourcer, der fordeles fleksibelt af udbyderen af cloudcomputingtjenester, uanset ressourcernes geografiske placering, med henblik på at håndtere udsving i efterspørgslen. Udtrykket »elastisk pulje« bruges til at beskrive IT-ressourcer, der tilvejebringes og stilles til rådighed alt efter efterspørgslen for hurtigt at øge eller mindske de tilgængelige ressourcer alt efter arbejdsbyrden. Udtrykket »delbar« bruges til at beskrive IT-ressourcer, der leveres til flere brugere, som deler en fælles adgang til tjenesten, men hvor databehandlingen foretages særskilt for hver bruger, selv om tjenesten leveres fra samme elektroniske udstyr. Udtrykket »distribueret« anvendes til at beskrive databehandlingsressourcer, der befinder sig på forskellige netforbundne computere eller enheder, og som kommunikerer og koordinerer indbyrdes ved at sende meddelelser.

(34) I lyset af fremkomsten af innovative teknologier og nye forretningsmodeller forventes nye cloudcomputingtjeneste- og ibrugtagningsmodeller at dukke op på markedet som reaktion på nye kundebehov. I den forbindelse kan cloudcomputingtjenester leveres i en meget distribueret form, endnu tættere på de steder, hvor dataene genereres eller indsamles, hvorved man bevæger sig væk fra den traditionelle model og i retning af en meget distribueret model (»edge computing«).

(35) Tjenester, der udbydes af datacentertjenesteudbydere, leveres ikke altid i form af cloudcomputingtjenester. Datacentre udgør derfor ikke altid

en del af cloudcomputing-infrastrukturen. For at styre alle de risici, der er forbundet med sikkerheden i net- og informationssystemer, bør dette direktiv derfor omfatte udbydere af datacentertjenester, som ikke er cloudcomputingtjenester. I dette direktiv bør begrebet »datacentertjeneste« omfatte levering af en tjeneste, der omfatter strukturer eller grupper af strukturer, der er beregnet til central opbevaring, sammenkobling og drift af informationsteknologi (IT) og netværksudstyr, der leverer datalagrings-, -behandlings- og -transporttjenester, samt alle faciliteter og infrastrukturer til energidistribution og miljøkontrol. Begrebet »datacentertjeneste« bør ikke finde anvendelse på interne datacentre, der ejes og drives af den berørte enhed til dets egne formål.

(36) Forskningsaktiviteter spiller en central rolle i udviklingen af nye produkter og processer. Mange af disse aktiviteter udføres af enheder, der deler, udbreder eller udnytter resultaterne af deres forskning til kommercielle formål. Disse enheder kan derfor være vigtige led i værdikæder, hvilket gør sikkerheden af deres net- og informationssystemer til en integreret del af det indre markeds overordnede cybersikkerhed. 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 Frascati-manual fra 2015 (»Guidelines for Collecting and Reporting Data on 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.

(37) Den voksende indbyrdes afhængighed er resultatet af et stadig mere grænseoverskridende og indbyrdes afhængigt net af tjenester, der anvender centrale infrastrukturer i hele Unionen inden for sektorer såsom energi, transport, digital infrastruktur, drikkevand og spildevand, sundhed, visse aspekter af offentlig forvaltning samt rummet, for så vidt angår levering af visse tjenester, der er afhængige af jordbaserede infrastrukturer, som ejes, forvaltes og drives enten af medlemsstaterne eller af private parter, men ikke infrastruktur, der ejes, forvaltes eller drives af eller på vegne af Unionen som en del af dens rumprogram. Disse indbyrdes afhængighedsforhold betyder, at enhver afbrydelse, selv en, der oprindeligt var begrænset til én enhed eller én sektor, kan have kaskadevirkninger mere generelt, hvilket potentielt kan føre til vidtrækkende og langvarige negative virkninger for leveringen af tjenester i hele det indre marked. De intensiverede cyberangreb under covid-19-pandemien har vist stadig mere indbyrdes afhængige samfunds sårbarhed over for risici med lav sandsynlighed.

(38) I betragtning af forskellene i de nationale forvaltningsstrukturer og for at beskytte allerede eksisterende sektorspecifikke ordninger eller Unionens tilsyns- og kontrolorganer bør medlemsstaterne kunne udpege eller oprette én eller flere nationale kompetente myndigheder med ansvar for cybersikkerhed og for tilsynsopgaverne i henhold til dette direktiv.

(39) For at lette grænseoverskridende samarbejde og kommunikation mellem myndigheder og muliggøre en effektiv gennemførelse af dette direktiv er det nødvendigt, at hver medlemsstat udpeger et centralt kontaktpunkt med ansvar for koordinering af spørgsmål vedrørende sikkerheden i net- og informationssystemer og grænseoverskridende samarbejde på EU-plan.

(40) De centrale kontaktpunkter bør sikre et effektivt grænseoverskridende samarbejde med andre medlemsstaters relevante myndigheder og, hvor det er relevant, med Kommissionen og ENISA. De centrale kontaktpunkter bør derfor efter anmodning fra CSIRT'en eller den kompetente myndighed have til opgave at videresende underretninger om væsentlige hændelser med grænseoverskridende virkninger til de centrale kontaktpunkter i andre berørte medlemsstater. På nationalt plan bør de centrale kontaktpunkter muliggøre et gnidningsløst tværsektorielt samarbejde med andre kompetente myndigheder. De centrale kontaktpunkter kan også være adressaterne for relevante oplysninger om hændelser vedrørende finansielle enheder fra de kompetente myndigheder i henhold til forordning (EU) 2022/2554, som de i givet fald bør kunne fremsende til CSIRT'erne eller de kompetente myndigheder i henhold til dette direktiv.

(41) Medlemsstaterne bør være tilstrækkelig udstyret med både teknisk og organisatorisk kapacitet til at forebygge, opdage, reagere på og reetablere sig efter hændelser og risici og afbøde deres virkninger. Medlemsstaterne bør derfor oprette eller udpege en eller flere CSIRT'er i henhold til dette direktiv og sikre, at de har tilstrækkelige ressourcer og tekniske kapaciteter. CSIRT'erne bør opfylde kravene, der er fastsat i dette direktiv, med henblik på at sikre effektive og kompatible kapaciteter til at håndtere hændelser og risici og til at sikre et effektivt samarbejde på EU-plan. Medlemsstaterne bør kunne udpege eksisterende IT-beredskabsenheder (CERT'er) som CSIRT'er. Med henblik på at styrke tillidsforholdet mellem enhederne og CSIRT'erne bør medlemsstaterne, hvor en CSIRT er en del af en kompetent myndighed, kunne overveje en funktionel adskillelse mellem CSIRT'ernes operationelle opgaver, navnlig i forbindelse med udveksling af oplysninger og støtte til enhederne, og de kompetente myndigheders tilsynsaktiviteter.

(42) CSIRT'erne har til opgave at håndtere hændelser. Dette omfatter behandling af store mængder til tider følsomme oplysninger. Medlemssta-

terne bør sikre, at CSIRT'erne har en infrastruktur til udveksling og behandling af oplysninger samt veludstyrede medarbejdere, hvilket sikrer fortroligheden og pålideligheden af deres operationer. CSIRT'erne vil også kunne vedtage adfærdskodekser i den henseende.

(43) For så vidt angår personoplysninger bør CSIRT'erne i overensstemmelse med forordning (EU) 2016/679 efter anmodning fra en væsentlig eller vigtig enhed være i stand til at foretage en proaktiv scanning af de net- og informationssystemer, der anvendes til levering af enhedens tjenester. I givet fald bør medlemsstaterne tilstræbe at sikre et ensartet niveau af teknisk kapacitet for alle sektorspecifikke CSIRT'er. Medlemsstaterne bør kunne anmode ENISA om bistand til at udvikle deres CSIRT'er.

(44) CSIRT'erne bør være i stand til på anmodning fra en væsentlig eller vigtig enhed at overvåge de af enhedens aktiver, der har internetopkobling, både i og uden for enhedens lokaler, for at kortlægge, forstå og styre enhedens samlede organisatoriske risici hvad angår nyopdagede trusler fra forsyningskæden eller kritiske sårbarheder. Enheden bør tilskyndes til at meddele CSIRT'en, hvorvidt den driver en privilegeret forvaltningsgrænseflade, da dette vil kunne påvirke hastigheden af gennemførelsen af afbødende foranstaltninger.

(45) I betragtning af betydningen af internationalt samarbejde om cybersikkerhed bør CSIRT'erne kunne deltage i internationale samarbejdsnetværk i tillæg til det CSIRT-netværk, der oprettes ved dette direktiv. Med henblik på udførelsen af deres opgaver bør CSIRT'erne og de kompetente myndigheder derfor kunne udveksle oplysninger, herunder personoplysninger, med nationale enheder i tredjelande, der håndterer IT-sikkerhedshændelser, eller tredjelandes kompetente myndigheder, forudsat at betingelserne i henhold til EU-databeskyttelsesretten for overførsel af personoplysninger til tredjelande, bl.a. betingelserne i artikel 49 i forordning (EU) 2016/679, er opfyldt.

(46) Det er afgørende at sikre tilstrækkelige ressourcer til at opfylde målene i dette direktiv og gøre det muligt for de kompetente myndigheder og CSIRT'erne udføre opgaverne heri. Medlemsstaterne kan på nationalt plan indføre en finansieringsmekanisme til dækning af de nødvendige udgifter i forbindelse med udførelsen af opgaver, der påhviler offentlige enheder med ansvar for cybersikkerhed i medlemsstaten i henhold til dette direktiv. En sådan mekanisme bør overholde EU-retten og bør være forholdsmæssig og ikkediskriminerende og bør tage hensyn til forskellige tilgange til levering af sikre tjenester.

(47) CSIRT-netværket bør fortsat bidrage til at styrke fortroligheden og tilliden og til at fremme hurtigt og effektivt operationelt samarbejde mellem medlemsstaterne. For at styrke det operationelle samarbejde på EU-

plan bør CSIRT-netværket overveje at indbyde EU-organer og -agenturer, der er involveret i cybersikkerhedspolitikken, såsom Europol, til at deltage i sit arbejde.

(48) Med henblik på at opnå og opretholde et højt cybersikkerhedsniveau bør de nationale cybersikkerhedsstrategier, der kræves i henhold til dette direktiv, bestå af sammenhængende rammer med strategiske mål og prioriteter på cybersikkerhedsområdet og den styring, der skal til for at nå dem. Disse strategier kan bestå af et eller flere lovgivningsmæssige eller ikkelovgivningsmæssige instrumenter.

(49) Cyberhygiejnepolitikker danner grundlaget for beskyttelse af net- og informationssysteminfrastrukturer, sikkerheden af hardware, software og onlineapplikationer samt virksomheds- eller slutbrugerdata, som enhederne er afhængige af. Cyberhygiejnepolitikker med et fælles grundsæt af praksisser, herunder software- og hardwareopdateringer, ændringer af passwords, styring af nye installeringer, begrænsning af adgangskonti på administratorniveau og backup af data, fremmer en proaktiv ramme for beredskab og generel sikkerhed i tilfælde af hændelser eller cybertrusler. ENISA bør overvåge og analysere medlemsstaternes cyberhygiejne politikker.

(50) Bevidsthed om cybersikkerhed og cyberhygiejne er afgørende for at forbedre cybersikkerhedsniveauet i Unionen, navnlig i lyset af det stigende antal forbundne enheder, der i stigende grad anvendes til cyberangreb. Der bør gøres en indsats for at øge den generelle bevidsthed om risici i forbindelse med sådant udstyr, mens vurderinger på EU-plan vil kunne bidrage til at sikre en fælles forståelse af sådanne risici inden for det indre marked.

(51) Medlemsstaterne bør tilskynde til anvendelse af enhver form for innovativ teknologi, herunder kunstig intelligens, hvis anvendelse kan forbedre opdagelsen og forebyggelsen af cyberangreb og gøre det muligt at omdirigere ressourcer til cyberangreb mere effektivt. Medlemsstaterne bør derfor i deres nationale cybersikkerhedsstrategi tilskynde til aktiviteter inden for forskning og udvikling for at lette anvendelsen af sådanne teknologier, navnlig dem, der vedrører automatiserede eller halvautomatiske værktøjer inden for cybersikkerhed, og, hvor det er relevant, deling af data, der er nødvendige for at uddanne brugerne af en sådan teknologi og forbedre den. Anvendelsen af enhver innovativ teknologi, herunder kunstig intelligens, bør overholde EU-databeskyttelsesretten, herunder databeskyttelsesprincipperne om datanøjagtighed, dataminimering, rimelighed og gennemsigtighed samt datasikkerhed såsom kryptering på det aktuelle teknologiske stade. Kravene om databeskyttelse gennem design og gennem standardindstillinger, der er fastsat i forordning (EU) 2016/679, bør udnyttes fuldt ud.

(52) Open source-cybersikkerhedsværktøjer og -applikationer kan bidrage til en højere grad af åbenhed og kan have en positiv indvirkning på effektiviteten af industriel innovation. Åbne standarder fremmer interoperabiliteten mellem sikkerhedsværktøjer, hvilket gavner industrielle interessenters sikkerhed. Open source-cybersikkerhedsværktøjer og -applikationer kan fungere som løftestang for det bredere udviklersamfund og give mulighed for leverandørdiversificering. Open source kan føre til en mere gennemsigtig proces for kontrol af cybersikkerhedsrelaterede værktøjer og en brugerdrevet proces for opdagelse af sårbarheder. Medlemsstaterne bør derfor kunne fremme anvendelsen af open source-software og åbne standarder ved at føre politikker vedrørende brugen af åbne data og open source som en del af konceptet »sikkerhed gennem gennemsigtighed«. Politikker, der fremmer indførelse og bæredygtig anvendelse af open source-cybersikkerhedsværktøjer, er af særlig betydning for små og mellemstore virksomheder, der står med høje gennemførelsesomkostninger, som kan reduceres ved at mindske behovet for bestemte applikationer eller værktøjer.

(53) Forsyningsselskaberne er i stigende grad forbundet med digitale netværk i byerne med henblik på at forbedre byernes transportnet, opgradere vandforsynings- og affaldsbortskaffelsesfaciliteter og øge effektiviteten af belysning og opvarmning af bygninger. Disse digitaliserede forsyningsvirksomheder er sårbare over for cyberangreb og risikerer i tilfælde af et vellykket cyberangreb at skade borgerne i stor skala på grund af deres indbyrdes forbundethed. Medlemsstaterne bør som led i deres nationale cybersikkerhedsstrategi udvikle en politik, der tager højde for udviklingen af sådanne forbundne eller intelligente byer og deres potentielle indvirkning på samfundet.

(54) I de senere år har Unionen oplevet en eksponentiel stigning i antallet af ransomwareangreb, hvor malware krypterer data og systemer og kræver betaling af løsepenge for at dekryptere dem. Den stigende hyppighed og alvor af ransomware-angreb kan være drevet af flere faktorer såsom forskellige angrebsmønstre, kriminelle forretningsmodeller omkring »ransomware som en service« og kryptovalutaer, krav om løsepenge og stigningen i angreb i forsyningskæden. Medlemsstaterne bør som led i deres nationale cybersikkerhedsstrategi udvikle en politik til håndtering af stigningen i antallet af ransomware-angreb.

(55) Offentlig-private partnerskaber (OPP'er) inden for cybersikkerhed kan skabe en passende ramme for udveksling af viden, deling af bedste praksis og etablering af et fælles forståelsesniveau blandt interessenter. Medlemsstaterne bør fremme politikker til støtte for oprettelsen af cybersikkerhedsspecifikke OPP'er. Disse politikker bør bl.a. klarlægge anvendelsesområdet og de involverede interessenter, styringsmodellen, de

tilgængelige finansieringsmuligheder og samspillet mellem de deltagende interessenter med hensyn til OPP'er. OPP'er kan udnytte ekspertisen i enheder inden for den private sektor med henblik på at bistå de kompetente myndigheder i udviklingen af tjenester og processer på det aktuelle teknologiske stade, herunder udveksling af oplysninger, tidlig varsling, cybertrussels- og -hændelsesøvelser, krisestyring og planlægning af modstandsdygtighed.

(56) Medlemsstaterne bør i deres nationale cybersikkerhedsstrategier tackle små og mellemstore virksomheders specifikke cybersikkerhedsbehov. Små og mellemstore virksomheder udgør på tværs af Unionen en stor procentdel af industri- og forretningsmarkedet og kæmper ofte med at tilpasse sig nye forretningspraksisser i en mere forbundet verden og til det digitale miljø, hvor medarbejdere arbejder hjemmefra, og forretning i stigende grad drives online. Nogle små og mellemstore virksomheder står over for specifikke cybersikkerhedsudfordringer, såsom ringe cyberbevidsthed, manglende IT-sikkerhed i forbindelse med fjernarbejde, de store omkostninger forbundet med cybersikkerhedsløsninger og et øget trusselsniveau, som f.eks. ransomware, som de bør modtage vejledning i og assistance til. Små og mellemstore virksomheder er i stigende grad mål for angreb i forsyningskæden på grund af deres mindre strenge foranstaltninger til styring af cybersikkerhedsrisici og angrebsstyring, samt det faktum at de har begrænsede sikkerhedsressourcer. Sådanne angreb i forsyningskæden har ikke kun indvirkning på små og mellemstore virksomheder og deres aktiviteter isoleret set, men kan også have en kaskadevirkning på større angreb på enheder, som de leverede varer til. Medlemsstaterne bør gennem deres nationale cybersikkerhedsstrategier hjælpe små og mellemstore virksomheder med at tackle de udfordringer, de står over for i deres forsyningskæder. Medlemsstaterne bør have et kontaktpunkt for små og mellemstore virksomheder på nationalt eller regionalt plan, som enten yder vejledning og bistand til små og mellemstore virksomheder eller retter dem mod de relevante organer med henblik på vejledning og bistand med hensyn til cybersikkerhedsrelaterede spørgsmål. Medlemsstaterne tilskyndes også til at tilbyde tjenester såsom webstedskonfigurering og muliggørelse af logning til mikrovirksomheder og små virksomheder, der mangler disse kapaciteter.

(57) Medlemsstaterne bør som led i deres nationale cybersikkerhedsstrategier vedtage politikker til fremme af aktiv cyberbeskyttelse som led i en bredere defensiv strategi. Snarere end at svare reaktivt består aktiv cyberbeskyttelse i forebyggelse, opdagelse, overvågning, analyse og afbødning af brud på netsikkerheden på en aktiv måde kombineret med anvendelse af kapaciteter i og uden for det net, der angribes. Dette vil kunne omfatte medlemsstater, der tilbyder gratis tjenester eller værktø-

jer til visse enheder, herunder selvbetjeningskontrol, opdagelsesværktøjer og fjernelsestjenester. Evnen til hurtigt og automatisk at udveksle og forstå trusselsoplysninger og -analyser, cyberaktivitetsalarmer og reaktionsforanstaltninger er helt afgørende for at muliggøre en forenet indsats med hensyn til på vellykket vis at forebygge, opdage, imødegå og blokere angreb på net- og informationssystemer. Aktiv cyberbeskyttelse er baseret på en defensiv strategi, der udelukker offensive foranstaltninger.

(58) Eftersom udnyttelsen af sårbarheder i net- og informationssystemer kan forårsage betydelige forstyrrelser og skader, er hurtig identifikation og afhjælpning af sådanne sårbarheder en vigtig faktor med hensyn til at reducere risici. Enheder, der udvikler eller administrerer net- og informationssystemer, bør derfor indføre passende procedurer til håndtering af sårbarheder, når de opdages. Da sårbarheder ofte opdages og offentliggøres af tredjeparter, bør producenten eller udbyderen af IKT-produkter eller -tjenester også indføre de nødvendige procedurer for at modtage sårbarhedsoplysninger fra tredjeparter. I den forbindelse indeholder de internationale standarder ISO/IEC 30111 og ISO/IEC 29147 vejledning om henholdsvis håndtering af sårbarheder og offentliggørelse af sårbarheder. Styrkelse af koordineringen mellem de underrettende fysiske og juridiske personer og producenter eller udbydere af IKT-produkter eller -tjenester er særlig vigtig med henblik på at lette den frivillige ramme for offentliggørelse af sårbarheder. Koordineret offentliggørelse af sårbarheder angiver en struktureret proces, hvorigennem sårbarheder rapporteres til producenten eller leverandøren af potentielt sårbare IKT-produkter eller -tjenester på en måde, der gør det muligt for den at diagnosticere og afhjælpe sårbarheden, inden detaljerede sårbarhedsoplysninger offentliggøres for tredjeparter eller offentligheden. Koordineret offentliggørelse af sårbarheder bør også omfatte koordinering mellem den rapporterende fysiske eller juridiske person og producenten eller leverandøren af de potentielt sårbare IKT-produkter eller -tjenester med hensyn til tidspunktet for afhjælpning og offentliggørelse af sårbarheder.

(59) Kommissionen, ENISA og medlemsstaterne bør fortsat fremme tilpasning til internationale standarder og industriens eksisterende bedste praksis på området for styring af cybersikkerhedsrisici, f.eks. inden for sikkerhedsvurderinger af forsyningskæden, udveksling af oplysninger og offentliggørelse af sårbarheder.

(60) Medlemsstaterne bør i samarbejde med ENISA træffe foranstaltninger til at fremme koordineret offentliggørelse af sårbarheder ved at fastlægge en relevant national politik. Som led i deres nationale politik bør medlemsstaterne så vidt muligt tackle de udfordringer, som sårbarheds-

forskere står over for, herunder deres potentielle strafansvar, i overensstemmelse med nationale ret. Eftersom fysiske og juridiske personer, der forsker i sårbarheder, i nogle medlemsstater vil kunne blive udsat for strafferetligt og civilretligt ansvar, opfordres medlemsstaterne til at vedtage retningslinjer for ikke-retsforfølgelse af informationssikkerhedsforskere og en fritagelse for civilretligt ansvar for deres aktiviteter.

(61) Medlemsstaterne bør udpege en af deres CSIRT'er som koordinator med henblik på at fungere som betroet formidler mellem de rapporterende fysiske eller juridiske personer og producenterne eller udbyderne af IKT-produkter eller -tjenester, som sandsynligvis vil blive berørt af sårbarheden, hvor det er nødvendigt. Den CSIRT, der er udpeget som koordinator, bør bl.a. have til opgave at identificere og kontakte de berørte enheder, at bistå de fysiske eller juridiske personer, der rapporterer en sårbarhed, at forhandle tidsfrister for offentliggørelse og at håndtere sårbarheder, der påvirker flere enheder (koordineret offentliggørelse af sårbarheder med flere parter). Hvor den rapporterede sårbarhed vil kunne have væsentlig indvirkning på enheder i mere end én medlemsstat, bør de CSIRT'er, der er udpeget som koordinatorer, i givet fald samarbejde inden for CSIRT-netværket.

(62) Adgang til korrekte og rettidige oplysninger om sårbarheder, der påvirker IKT-produkter og -tjenester, bidrager til en forbedret styring af cybersikkerhedsrisici. Kilder til offentligt tilgængelige oplysninger om sårbarheder er et vigtigt redskab for enhederne og for brugerne af deres tjenester, men også for de kompetente myndigheder og CSIRT'erne. Derfor bør ENISA oprette en europæisk sårbarhedsdatabase, hvor enheder, uanset om de er omfattet af dette direktiv, og deres leverandører af net- og informationssystemer samt de kompetente myndigheder og CSIRT'erne på frivillig basis kan offentliggøre og registrere offentligt kendte sårbarheder med henblik på at give brugerne mulighed for at træffe passende afbødende foranstaltninger. Formålet med denne database er at tackle de unikke udfordringer, som risiciene udgør for enheder i Unionen. ENISA bør desuden fastlægge en passende procedure for offentliggørelsesprocessen for at give enhederne tid til at træffe afbødende foranstaltninger med hensyn til deres sårbarhed og anvende foranstaltninger på det aktuelle teknologiske stade til styring af cybersikkerhedsrisici samt maskinlæsbare datasæt og tilhørende grænseflader. For at fremme en kultur med offentliggørelse af sårbarheder bør offentliggørelse ikke have nogen negativ effekt for den rapporterende fysiske eller juridiske person.

(63) Selv om der findes lignende sårbarhedsregistre eller -databaser, hostes og vedligeholdes disse af enheder, der ikke er etableret i Unionen. En europæisk sårbarhedsdatabase, der vedligeholdes af ENISA, vil give

større gennemsigtighed med hensyn til offentliggørelsesprocessen, inden sårbarheden offentliggøres, og modstandsdygtighed i tilfælde af en forstyrrelse eller en afbrydelse af leveringen af tilsvarende tjenester. For i videst muligt omfang at undgå dobbeltarbejde og tilstræbe komplementaritet bør ENISA undersøge muligheden for at indgå strukturerede samarbejdsaftaler med lignende registre eller databaser, der henhører under tredjelandes jurisdiktioner. ENISA bør navnlig undersøge muligheden for et tæt samarbejde med operatørerne af det fælles sårbarheds- og eksponeringssystem (CVE).

(64) Samarbejdsgruppen bør støtte og lette strategisk samarbejde og udvekslingen af oplysninger samt styrke tilliden og fortroligheden blandt medlemsstaterne. Samarbejdsgruppen bør udarbejde et arbejdsprogram hvert andet år. Arbejdsprogrammet bør omfatte de foranstaltninger, som samarbejdsgruppen skal gennemføre for at nå sine mål og udføre sine opgaver. Tidsrammen for fastlæggelsen af det første arbejdsprogram i henhold til dette direktiv bør tilpasses tidsrammen for det sidste arbejdsprogram, der blev fastlagt i henhold til direktiv (EU) 2016/1148, for at undgå potentielle forstyrrelser af samarbejdsgruppens arbejde.

(65) Når samarbejdsgruppen udarbejder vejledningsdokumenter, bør den konsekvent kortlægge nationale løsninger og erfaringer, vurdere virkningen af samarbejdsgruppens resultater på nationale tilgange, drøfte gennemførelsesudfordringer og formulere specifikke anbefalinger, navnlig om at lette harmonisering af gennemførelsen af dette direktiv blandt medlemsstaterne, som skal håndteres gennem bedre gennemførelse af eksisterende regler. Samarbejdsgruppen vil også kunne kortlægge de nationale løsninger for at fremme foreneligheden af de cybersikkerhedsløsninger, der anvendes i hver enkelt specifik sektor i hele Unionen. Dette er særligt relevant for sektorer med en international eller grænseoverskridende karakter.

(66) Samarbejdsgruppen bør fortsat være et fleksibelt forum og være i stand til at reagere på skiftende og nye politiske prioriteter og udfordringer, samtidig med at der tages hensyn til de disponible ressourcer. Den vil kunne tilrettelægge regelmæssige fælles møder med relevante private interessenter fra hele Unionen for at drøfte samarbejdsgruppens aktiviteter og indsamle data og input om nye politiske udfordringer. Derudover bør samarbejdsgruppen foretage en regelmæssig vurdering af situationen med hensyn til cybertrusler eller hændelser såsom ransomware. For at styrke samarbejdet på EU-plan bør samarbejdsgruppen overveje at indbyde de relevante EU-institutioner, -organer, -kontorer og -agenturer, der er involveret i cybersikkerhedspolitikken, såsom Europa-Parlamentet, Europol, Det Europæiske Databeskyttelsesråd, Den Europæiske Unions Luftfartssikkerhedsagentur, oprettet ved forordning (EU) 2018/1139, og Den Europæiske Unions Agentur for Rumprogrammet,

oprettet ved Europa-Parlamentets og Rådets forordning (EU) 2021/696 ([14]), til at deltage i sit arbejde.

(67) De kompetente myndigheder og CSIRT'erne bør kunne deltage i udvekslingsordninger for embedsmænd fra andre medlemsstater inden for specifikke rammer og i givet faldmed forbehold for den påkrævede sikkerhedsgodkendelse af embedsmænd, der deltager i sådanne udvekslingsordninger, med henblik på at forbedre samarbejdet og styrke tilliden medlemsstaterne imellem. De kompetente myndigheder bør træffe de foranstaltninger, der er nødvendige for at sætte embedsmænd fra andre medlemsstater i stand til at spille en effektiv rolle i den kompetente myndigheds eller CSIRT-værtens aktiviteter.

(68) Medlemsstaterne bør bidrage til oprettelsen af EU-krisereaktionsrammen for cybersikkerhed som fastsat i Kommissionens henstilling (EU) 2017/1584 ([15]) gennem de eksisterende samarbejdsnetværk, navnlig det europæiske netværk af forbindelsesorganisationer for cyberkriser (EU-CyCLONe), CSIRT-netværket og samarbejdsgruppen. EU-CyCLONe og CSIRT-netværket bør samarbejde på grundlag af proceduremæssige ordninger, der fastlægger den nærmere udformning af dette samarbejde, og undgå dobbeltarbejde. EU-CyCLONe's forretningsorden bør yderligere præcisere, hvordan dette netværk bør fungere, herunder netværkets roller, metoder for samarbejde, interaktion med andre relevante aktører og skabeloner for udveksling af oplysninger samt kommunikationsmidler. Med hensyn til krisestyring på EU-plan bør de relevante parter støtte sig til EU's integrerede ordninger for politisk kriserespons i henhold til Rådets gennemførelsesafgørelse (EU) 2018/1993 ([16]) (IPCR-ordningerne). Kommissionen bør anvende den tværsektorielle krisekoordinationsproces på højt niveau, ARGUS, til dette formål. Hvis krisen har en vigtig ekstern dimension eller berører den fælles sikkerheds- og forsvarspolitik, bør EU-Udenrigstjenestens krisereaktionsmekanisme aktiveres.

(69) I overensstemmelse med bilaget til henstilling (EU) 2017/1584 bør en omfattende cybersikkerhedshændelse forstås som en hændelse, der forårsager en forstyrrelse på et niveau, der overstiger en medlemsstats kapacitet til at reagere på den, eller som har en betydelig indvirkning på mindst to medlemsstater. Alt efter årsag og virkning kan omfattende cybersikkerhedshændelser eskalere og udvikle sig til fuldgyldige kriser, der forhindrer det indre markeds korrekte funktion eller udgør alvorlige risici for den offentlige sikkerhed for enheder eller borgere i flere medlemsstater eller for Unionen som helhed. I betragtning af sådanne begivenheders vidtrækkende omfang og i de fleste tilfælde grænseoverskridende karakter bør medlemsstaterne og de relevante EU-institutioner, -organer, -kontorer og -agenturer samarbejde på teknisk, operationelt og politisk plan for at koordinere indsatsen i hele Unionen.

(70) Omfattende cybersikkerhedshændelser og kriser på EU-plan kræver en koordineret indsats for at sikre en hurtig og effektiv reaktion på grund af den store indbyrdes afhængighed mellem sektorer og medlemsstater. Tilgængeligheden af cybermodstandsdygtige net- og informationssystemer og tilgængeligheden, fortroligheden og integriteten af data er afgørende for Unionens sikkerhed og for beskyttelsen af dens borgere, virksomheder og institutioner mod hændelser og cybertrusler samt for at øge enkeltpersoners og organisationers tillid til Unionens evne til at fremme og beskytte et globalt, åbent, frit, stabilt og sikkert cyberspace baseret på menneskerettigheder, grundlæggende frihedsrettigheder, demokrati og retsstatsprincippet.

(71) EU-CyCLONe bør fungere som en formidler mellem det tekniske og det politiske niveau under omfattende cybersikkerhedshændelser og kriser og bør styrke samarbejdet på operationelt plan og støtte beslutningstagningen på politisk plan. I samarbejde med Kommissionen og under hensyntagen til Kommissionens kompetence på krisestyringsområdet bør EU-CyCLONe bygge videre på CSIRT-netværkets resultater og anvende sin egen kapacitet til at udarbejde konsekvensanalyser af omfattende cybersikkerhedshændelser og kriser.

(72) Cyberangreb er af grænseoverskridende karakter, og en væsentlig hændelse kan forstyrre og skade kritiske informationsinfrastrukturer, som det indre markeds funktion afhænger af. Henstilling (EU) 2017/1584 omhandler alle relevante aktørers rolle. Desuden er Kommissionen inden for rammerne af EU-civilbeskyttelsesmekanismen, der blev oprettet ved Europa-Parlamentets og Rådets afgørelse 1313/2013/EU ([17]), ansvarlig for generelle beredskabstiltag, herunder forvaltning af katastrofeberedskabskoordinationscentret og det fælles varslings- og informationssystem, opretholdelse og videreudvikling af situationsbevidsthed og analysekapacitet, og tilvejebringelse og forvaltning af kapaciteten til at mobilisere og udsende eksperthold i tilfælde af en anmodning om bistand fra en medlemsstat eller et tredjeland. Kommissionen er også ansvarlig for at udarbejde analytiske rapporter om IPCR-ordningerne i henhold til gennemførelsesafgørelse (EU) 2018/1993, herunder i forbindelse med situationsbevidsthed og beredskab vedrørende cybersikkerhed samt for situationsbevidsthed og kriserespons inden for landbrug, ugunstige vejrforhold, konfliktkortlægning og -prognoser, systemer for tidlig varsling i forbindelse med naturkatastrofer, sundhedskriser, overvågning af infektionssygdomme, plantesundhed, kemiske hændelser, fødevare- og fodersikkerhed, dyresundhed, migration, told, nukleare og radiologiske kriser og energi.

(73) Unionen kan, hvor det er hensigtsmæssigt, i overensstemmelse med artikel 218 i TEUF indgå internationale aftaler med tredjelande eller internationale organisationer, som giver mulighed for og tilrettelægger

disses deltagelse i bestemte aktiviteter, der foretages af samarbejdsgruppen, CSIRT-netværket og EU-CyCLONe. Sådanne aftaler bør sikre Unionens interesser og tilstrækkelig databeskyttelse. Dette bør ikke udelukke medlemsstaternes ret til at samarbejde med tredjelande om håndtering af sårbarheder og styring af cybersikkerhedsrisici og lette rapportering og generel udveksling af oplysninger i overensstemmelse med EU-retten.

(74) For at lette en effektiv gennemførelse af dette direktiv, herunder med hensyn til håndtering af sårbarheder, foranstaltninger til styring af cybersikkerhedsrisici, rapporteringsforpligtelser og ordninger for udveksling af cybersikkerhedsoplysninger, kan medlemsstaterne samarbejde med tredjelande og gennemføre aktiviteter, der anses for hensigtsmæssige til dette formål, herunder udveksling af oplysninger om cybertrusler, hændelser, sårbarheder, værktøjer og metoder, taktikker, teknikker og procedurer, beredskab og øvelser i forbindelse med styring af cybersikkerhedskriser, uddannelse, tillidsskabende tiltag og strukturerede ordninger til udveksling af oplysninger.

(75) Der bør indføres peerevalueringer for at gøre det lettere at lære af fælles erfaringer, styrke gensidig tillid og opnå et højt fælles cybersikkerhedsniveau. Peerevalueringer kan føre til værdifuld indsigt og anbefalinger, der kan styrke de overordnede cybersikkerhedskapaciteter, skabe en ny funktionel kanal for udveksling af bedste praksis på tværs af medlemsstaterne og bidrage til at højne medlemsstaternes modenhedsniveauer for så vidt angår cybersikkerhed. Desuden bør peerevalueringer tage hensyn til resultaterne af lignende mekanismer, såsom CSIRT-netværkets peerevalueringssystem, og bør tilføre merværdi og undgå dobbeltarbejde. Gennemførelsen af peerevalueringer bør ikke berøre EU-retten eller national ret om beskyttelse af fortrolige eller klassificerede oplysninger.

(76) Samarbejdsgruppen bør fastlægge en selvevalueringsmetode for medlemsstaterne med henblik på at dække faktorer såsom graden af gennemførelse af foranstaltninger til styring af cybersikkerhedsrisici og rapporteringsforpligtelser, kapacitetsniveauet og effektiviteten af udførelsen af de kompetente myndigheders opgaver, CSIRT'ernes operationelle kapacitet, graden af gennemførelse af gensidig bistand, graden af gennemførelse af ordningerne for udveksling af cybersikkerhedsoplysninger eller specifikke spørgsmål af grænseoverskridende eller tværsektoriel karakter. Medlemsstaterne bør tilskyndes til at foretage selvevalueringer regelmæssigt og til at fremlægge og drøfte resultaterne heraf i samarbejdsgruppen.

(77) Ansvaret for at sikre sikkerheden i net- og informationssystemer ligger i vid udstrækning hos væsentlige og vigtige enheder. En risikostyrings-

kultur, der indbefatter risikovurderinger og gennemførelse af foranstaltninger til styring af cybersikkerhedsrisici, som står i forhold til de foreliggende risici, bør fremmes og udvikles.

(78) Foranstaltningerne til styring af cybersikkerhedsrisici bør tage hensyn til den væsentlige eller vigtige enheds grad af afhængighed af net- og informationssystemer og omfatte foranstaltninger til at identificere alle risici for hændelser, til at forebygge, opdage, reagere på og reetablere sig efter hændelser og til at afbøde deres indvirkning. Sikkerheden i net- og informationssystemer bør omfatte lagrede, overførte og behandlede datas sikkerhed. Foranstaltningerne til styring af cybersikkerhedsrisici bør omfatte en systemisk analyse, som tager højde for den menneskelige faktor, for at få et fuldstændigt billede af sikkerheden af net- og informationssystemet.

(79) Da trusler mod sikkerheden i net- og informationssystemer kan have forskellig oprindelse, bør foranstaltninger til styring af cybersikkerhedsrisici bygge på en tilgang, der omfatter alle farer og sigter på at beskytte net- og informationssystemer og disse 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 til styring af cybersikkerhedsrisici bør derfor også adressere den fysiske og miljømæssige sikkerhed i net- og informationssystemerne ved at inkludere foranstaltninger til beskyttelse af sådanne systemer mod systemsvigt, menneskelige fejl, ondsindede handlinger eller naturfænomener i overensstemmelse med europæiske og internationale standarder såsom dem, der indgår i ISO/IEC 27000-serien. Væsentlige og vigtige enheder bør med henblik herpå som led i deres foranstaltninger til styring af cybersikkerhedsrisici også adressere sikkerheden vedrørende menneskelige ressourcer og indføre passende adgangskontrolpolitikker. Disse foranstaltninger bør være forenelige med direktiv (EU) 2022/2557.

(80) Med henblik på at påvise overensstemmelse med foranstaltninger til styring af cybersikkerhedsrisici og i mangel af passende europæiske cybersikkerhedscertificeringsordninger vedtaget i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) 2019/881 ([18]) bør medlemsstaterne i samråd med samarbejdsgruppen og Den Europæiske Cybersikkerhedscertificeringsgruppe fremme væsentlige og vigtige enhe-

ders anvendelse af relevante europæiske og internationale standarder eller kan eventuelt kræve, at enhederne anvender certificerede IKT-produkter, -tjenester og -processer.

(81) Med henblik på at undgå, at operatører af væsentlige og vigtige enheder pålægges en uforholdsmæssig stor økonomisk og administrativ byrde, 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.

(82) 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.

(83) Væsentlige og vigtige enheder bør garantere sikkerheden af de net- og informationssystemer, som de anvender i forbindelse med deres aktiviteter. Disse systemer er primært private net- og informationssystemer, der forvaltes af de væsentlige og vigtige enheders interne IT-personale, eller hvis sikkerhed er blevet outsourcet. De foranstaltninger til styring af cybersikkerhedsrisici og rapporteringsforpligtelser, der er fastsat i dette direktiv, bør finde anvendelse på de relevante væsentlige og vigtige enheder, uanset om disse enheder selv vedligeholder deres net- og informationssystemer eller outsourcer vedligeholdelsen deraf.

(84) DNS-tjenesteudbydere, topdomænenavneadministratorer og udbydere af cloudcomputingtjenester, af datacentertjenester, af indholdsleveringsnetværk, af administrerede tjenester, af administrerede sikkerhedstjenester, af onlinemarkedspladser, af onlinesøgemaskiner, af platforme for sociale netværkstjenester og af tillidstjenester bør i betragtning af deres grænseoverskridende karakter være underlagt en høj grad af harmonisering på EU-plan. Gennemførelsen af foranstaltninger til styring af cybersikkerhedsrisici med hensyn til disse enheder bør derfor lettes ved hjælp af en gennemførelsesretsakt.

(85) 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.

(86) Blandt tjenesteudbydere spiller udbydere af administrerede sikkerhedstjenester på områder såsom reaktion på hændelser, penetrationstest, sikkerhedsaudits og konsulentbistand en særlig vigtig rolle med hensyn til at bistå enheder i deres bestræbelser på at forebygge, opdage, reagere på eller reetablere sig efter hændelser. Udbydere af administrerede sikkerhedstjenester har imidlertid også selv været mål for cyberangreb og udgør på grund af deres høje grad af integration i enheders operationer en særlig risiko. Væsentlige og vigtige enheder bør derfor udvise forøget omhu ved udvælgelsen af en udbyder af administrerede sikkerhedstjenester.

(87) De kompetente myndigheder kan i forbindelse med deres tilsynsopgaver også drage fordel af cybersikkerhedstjenester såsom sikkerhedsaudits, penetrationstest eller reaktion på hændelser.

(88) Væsentlige og vigtige enheder bør også tage højde for risici hidrørende fra deres samspil og relationer med andre interessenter inden for et bredere økosystem, herunder i forbindelse med bekæmpelse af industrispionage og beskyttelse af forretningshemmeligheder. Navnlig bør disse enheder træffe passende foranstaltninger til at sikre, at deres samarbejde med akademiske institutioner og forskningsinstitutioner finder sted i overensstemmelse med deres cybersikkerhedspolitikker og følger god praksis med hensyn til sikker adgang til og formidling af oplysninger generelt og beskyttelse af intellektuel ejendom i særdeleshed. På samme måde bør væsentlige og vigtige enheder i betragtning af datas betydning og værdi for deres aktiviteter træffe alle passende foranstaltninger til styring af cybersikkerhedsrisici, når disse enheder benytter sig af datatransformations- og dataanalysetjenester fra tredjeparter.

(89) Væsentlige og vigtige enheder bør indføre en bred vifte af grundlæggende cyberhygiejnepraksisser såsom »zero trust«-principper, softwareopdateringer, enhedskonfiguration, netværkssegmentering, identitets- og adgangsstyring eller brugerbevidsthed, arrangere kurser for deres personale og højne bevidstheden om cybertrusler, phishing og social

engineering-teknikker. Disse enheder bør desuden evaluere deres egne cybersikkerhedskapaciteter og, hvor det er hensigtsmæssigt, stræbe efter at integrere cybersikkerhedsforstærkende teknologier, såsom systemer baseret på kunstig intelligens eller maskinlæring, for at forstærke deres kapaciteter og sikkerheden i net- og informationssystemerne.

(90) For yderligere at håndtere centrale risici i forsyningskæden og bistå væsentlige og vigtige enheder, der opererer i sektorer, som er omfattet af dette direktiv, med at håndtere forsyningskæde- og leverandørrelaterede risici på en hensigtsmæssig måde, bør samarbejdsgruppen, i samarbejde med Kommissionen og ENISA og, hvor det er hensigtsmæssigt, efter høring af relevante interessenter, herunder fra industrien, foretage koordinerede sikkerhedsrisikovurderinger af kritiske forsyningskæder som dem, der er foretaget for 5G-net efter Kommissionens henstilling (EU) 2019/534 ([19]), med henblik på inden for hver enkelt sektor at identificere de kritiske IKT-tjenester, -systemer eller -produkter, relevante trusler og sårbarheder Sådanne koordinerede sikkerhedsrisikovurderinger bør identificere foranstaltninger, afbødningsplaner og bedste praksisser for modvirkning af kritiske afhængigheder, potentielle enkelte fejlpunkter, trusler, sårbarheder og andre risici knyttet til forsyningskæden og bør undersøge, hvordan væsentlige og vigtige enheder yderligere kan tilskyndes til at indføre disse. Potentielle ikketekniske risikofaktorer såsom et tredjelands utilbørlige påvirkning af leverandører og tjenesteudbydere, navnlig i forbindelse med alternative styringsmodeller, omfatter skjulte sårbarheder eller bagdøre og potentielle systemiske forsyningsforstyrrelser, navnlig i tilfælde af teknologisk fastlåsning eller udbyderafhængighed.

(91) Ved koordinerede sikkerhedsrisikovurderinger af kritiske forsyningskæder bør der i lyset af kendetegnene ved den pågældende sektor tages hensyn til både tekniske og, hvor det er relevant, ikketekniske faktorer, herunder dem, der er defineret i henstilling (EU) 2019/534, i den EU-koordinerede risikovurdering af cybersikkerheden af 5G-net og i EU-værktøjskassen til 5G-cybersikkerhed, som samarbejdsgruppen er nået til enighed om. For at identificere de forsyningskæder, der bør gøres til genstand for en koordineret sikkerhedsrisikovurdering, bør følgende kriterier tages i betragtning: i) i hvilket omfang væsentlige og vigtige enheder anvender og er afhængige af specifikke kritiske IKT-tjenester, -systemer eller -produkter, ii) relevansen af specifikke kritiske IKT-tjenester, -systemer eller -produkter til udførelse af kritiske eller følsomme funktioner, herunder behandling af personoplysninger, iii) tilgængeligheden af alternative IKT-tjenester, -systemer eller -produkter, iv) modstandsdygtigheden af den samlede forsyningskæde for IKT-tjenester, -systemer eller -produkter i hele deres livscyklus over for forstyrrelser og v) for nye IKT-tjenester, -systemer eller -produkter, deres potentielle

fremtidige betydning for enhedernes aktiviteter. Endvidere bør der lægges særlig vægt på IKT-tjenester, -systemer eller -produkter, der er underlagt specifikke krav hidrørende fra tredjelande.

(92) For at strømline de forpligtelser, der pålægges udbydere af offentlige elektroniske kommunikationsnet eller af offentligt tilgængelige elektroniske kommunikationstjenester og tillidstjenesteudbydere med hensyn til sikkerheden af deres net- og informationssystemer, og for at gøre det muligt for de pågældende enheder og de kompetente myndigheder, i henhold til henholdsvis Europa-Parlamentets og Rådets direktiv (EU) 2018/1972 ([20]) og forordning (EU) nr. 910/2014, at drage fordel af de retlige rammer, der er fastsat i dette direktiv, herunder udpegelsen af en CSIRT med ansvar for håndteringen af hændelser, deltagelsen af de berørte kompetente myndigheder i samarbejdsgruppens aktiviteter og CSIRT-netværket, bør de pågældende enheder være omfattet af dette direktivs anvendelsesområde. De tilsvarende bestemmelser i forordning (EU) nr. 910/2014 og direktiv (EU) 2018/1972 vedrørende indførelse af sikkerhedskrav og underretningspligt for disse typer enheder bør derfor udgå. Reglerne om rapporteringsforpligtelser, der er fastsat i nærværende direktiv, bør ikke berøre forordning (EU) 2016/679 og direktiv 2002/58/EF.

(93) Cybersikkerhedsforpligtelserne, der er fastsat i dette direktiv, bør betragtes som et supplement til de krav, der pålægges tillidstjenesteudbydere i henhold til forordning (EU) nr. 910/2014. Tillidstjenesteudbydere bør være forpligtet til at træffe alle passende og forholdsmæssige foranstaltninger for at styre de risici, der er forbundet med deres tjenester, herunder i forhold til kunder og tilknyttede tredjeparter, og til at rapportere hændelser i henhold til dette direktiv. Sådanne cybersikkerheds- og rapporteringsforpligtelser bør også vedrøre den fysiske beskyttelse af de udbudte tjenester. Kravene til kvalificerede tillidstjenesteudbydere i artikel 24 i forordning (EU) nr. 910/2014 finder fortsat anvendelse.

(94) Medlemsstaterne kan tildele rollen som de kompetente myndigheder for tillidstjenester til de i forordning (EU) nr. 910/2014 omhandlede tilsynsorganer for at sikre videreførelsen af den nuværende praksis og bygge videre på den viden og erfaring, der er opnået i forbindelse med anvendelsen af nævnte forordning. I sådanne tilfælde bør de kompetente myndigheder i henhold til dette direktiv arbejde tæt sammen med disse tilsynsorganer ved rettidigt at udveksle relevante oplysninger for at sikre effektivt tilsyn med tillidstjenesteudbyderne og sikre deres overholdelse af kravene i dette direktiv og i forordning (EU) nr. 910/2014. I givet fald bør CSIRT'en eller den kompetente myndighed i henhold til dette direktiv straks informere tilsynsorganet i henhold til forordning (EU) nr. 910/2014 om enhver underretning om en væsentlig cybertrussel eller

hændelse, der berører tillidstjenester samt om ethvert tilfælde af en tillidstjenesteudbyders overtrædelser af dette direktiv. Medlemsstaterne kan i rapporteringsøjemed i givet fald anvende det enkelte indgangspunkt, der er oprettet for at opnå en fælles og automatisk rapportering af hændelser til både tilsynsorganet i henhold til forordning (EU) nr. 910/2014 og CSIRT eller den kompetente myndighed i henhold til dette direktiv.

(95) Hvor det er hensigtsmæssigt og for at undgå unødige forstyrrelser, bør eksisterende nationale retningslinjer der er vedtaget med henblik på gennemførelse af reglerne vedrørende sikkerhedsforanstaltninger i artikel 40 og 41 i direktiv (EU) 2018/1972, tages i betragtning ved gennemførelsen af nærværende direktiv, så der kan bygges videre på den viden og de færdigheder, der allerede er erhvervet i forbindelse med direktiv (EU) 2018/1972 med hensyn til sikkerhedsforanstaltninger og hændelsesunderretninger. ENISA kan også udvikle vejledning om sikkerhedskrav og om rapporteringsforpligtelser for udbydere af offentlige elektroniske kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester for at lette harmonisering og omstilling og minimere forstyrrelser. Medlemsstaterne kan tildele de nationale tilsynsmyndigheder rollen som de kompetente myndigheder for elektronisk kommunikation i henhold til direktiv (EU) 2018/1972 for at sikre videreførelsen af den nuværende praksis og bygge videre på den viden og erfaring, der er opnået som et resultat af gennemførelsen af nævnte direktiv.

(96) I betragtning af den stigende betydning af nummeruafhængige interpersonelle kommunikationstjenester som defineret i direktiv (EU) 2018/1972 er det nødvendigt at sikre, at sådanne tjenester også er omfattet af passende sikkerhedskrav i lyset af deres særlige karakter og økonomiske betydning. Eftersom angrebsfladen bliver stadig større, bliver nummeruafhængige interpersonelle kommunikationstjenester såsom meddelelsestjenester stadig mere udbredte angrebsvektorer. Ondsindede gerningspersoner anvender platforme til at kommunikere med og lokke ofre til at gå ind på kompromitterede websider, hvilket øger sandsynligheden for hændelser, der involverer udnyttelse af personoplysninger og, som følge deraf, sikkerheden i net- og informationssystemer. Udbydere af nummeruafhængige interpersonelle kommunikationstjenester bør sikre et sikkerhedsniveau i net- og informationssystemer, der står i forhold til risiciene. Da udbydere af nummeruafhængige interpersonelle kommunikationstjenester normalt ikke udøver egentlig kontrol over transmissionen af signaler via net, kan risikoniveauet for sådanne tjenester i visse henseender anses for at være lavere end for traditionelle elektroniske kommunikationstjenester. Det samme gælder interpersonelle kommunikationstjenester, som defineret i direktiv (EU)

2018/1972, der anvender numre, og som ikke udøver faktisk kontrol over signaltransmission.

(97) Det indre marked er mere end nogensinde afhængigt af internettets funktionsdygtighed. Næsten alle væsentlige og vigtige enheders tjenester er afhængige af tjenester, der leveres over internettet. For at sikre en problemfri levering af tjenester, der udbydes af væsentlige og vigtige enheder, er det vigtigt, at alle udbydere af offentlige elektroniske kommunikationsnet har indført passende foranstaltninger til styring af cybersikkerhedsrisici og rapporterer om væsentlige hændelser i forbindelse hermed. Medlemsstaterne bør sørge for, at sikkerheden af de offentlige elektroniske kommunikationsnet opretholdes, og at deres vitale sikkerhedsinteresser beskyttes mod sabotage og spionage. Eftersom international konnektivitet styrker og fremskynder den konkurrencedygtige digitalisering af Unionen og dens økonomi, bør hændelser, der påvirker undersøiske kommunikationskabler, rapporteres til CSIRT eller i givet fald til den kompetente myndighed. Den nationale cybersikkerhedsstrategi bør, hvor det er relevant, tage hensyn til undersøiske kommunikationskablers cybersikkerhed og omfatte en kortlægning af potentielle cybersikkerhedsrisici og afbødende foranstaltninger for at sikre dem det højeste beskyttelsesniveau.

(98) For at beskytte sikkerheden af offentlige elektroniske kommunikationsnet og offentligt tilgængelige elektroniske kommunikationstjenester bør brugen af krypteringsteknologier, navnlig end-to-end-kryptering samt datacentrerede sikkerhedskoncepter såsom kartografi, segmentering, tagging, adgangspolitik og adgangsstyring samt automatiserede adgangsbeslutninger fremmes. Om nødvendigt bør anvendelsen af kryptering, navnlig end-to-end-kryptering, være obligatorisk for udbydere af offentlige elektroniske kommunikationsnet eller af offentligt tilgængelige elektroniske kommunikationstjenester i overensstemmelse med principperne om sikkerhed og privatlivsbeskyttelse gennem standardindstillinger og gennem design med henblik på dette direktiv. Brugen af end-to-end-kryptering bør forliges med medlemsstaternes beføjelser til at sikre beskyttelsen af deres væsentlige sikkerhedsinteresser og offentlig sikkerhed og til at tillade forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger i overensstemmelse med EU-retten. Dette bør dog ikke svække end-to-end-kryptering, som er en teknologi af kritisk betydning for den effektive data- og privatlivsbeskyttelse og for kommunikationssikkerheden.

(99) For at beskytte sikkerheden af og forhindre misbrug af og manipulation med offentlige elektroniske kommunikationsnet og offentligt tilgængelige elektroniske kommunikationstjenester bør brugen af sikre routing-

standarder fremmes for at sikre integriteten og robustheden af routingfunktionerne i hele økosystemet af udbydere af internetadgangstjenester.

(100) For at beskytte internettets funktionalitet og integritet og fremme DNS'ens sikkerhed og modstandsdygtighed bør relevante interessenter, herunder enheder i Unionens private sektor, udbydere af offentligt tilgængelige elektroniske kommunikationstjenester, navnlig udbydere af internetadgangstjenester, og udbydere af onlinesøgemaskiner tilskyndes til at vedtage en diversificeringsstrategi for DNS-oversættelse. Endvidere bør medlemsstaterne tilskynde til udvikling og brug af en offentlig og sikker europæisk DNS-oversættelsestjeneste.

(101) I dette direktiv fastlægges en flertrinstilgang for underretning om væsentlige hændelser med henblik på at finde den rette balance mellem på den ene side hurtig underretning, der bidrager til at afbøde den potentielle spredning af væsentlige hændelser og giver væsentlige og vigtige enheder mulighed for at søge assistance, og på den anden side dybdegående underretning, der gør det muligt at høste værdifulde erfaringer af individuelle hændelser og over tid forbedre individuelle virksomheders og hele sektorers cyberrobusthed. Direktivet bør i den henseende 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.

(102) Hvor væsentlige og vigtige enheder bliver opmærksomme på en væsentlig hændelse, bør de være forpligtet til at indgive en tidlig varsling uden unødigt ophold og under alle omstændigheder inden for 24 timer. Denne tidlige varsling bør efterfølges af en hændelsesunderretning. De pågældende enheder bør indgive en hændelsesunderretning uden unødigt ophold og under alle omstændigheder inden for 72 timer efter, at have fået kendskab til den væsentlige hændelse, navnlig med henblik på at ajourføre de oplysninger, der blev indgivet ved den tidlige varsling, og give en indledende vurdering af den væsentlige hændelse, herunder dens alvor og indvirkning, samt kompromitteringsindikatorer,

hvor sådanne foreligger. En endelig rapport bør indgives senest en måned efter hændelsesunderretningen. Den tidlige varsling bør kun indeholde de oplysninger, der er nødvendige for at gøre CSIRT'en eller i givet fald den kompetente myndighed opmærksom på den væsentlige hændelse og give den pågældende enhed mulighed for om nødvendigt at søge assistance. En sådan tidlige varsling bør, 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. Medlemsstaterne bør sikre, at forpligtelsen til at indgive den tidlige varsling eller den efterfølgende hændelsesunderretning ikke medfører, at den underrettende enhed bruger færre ressourcer på aktiviteter vedrørende håndtering af hændelser, idet disse bør 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. I tilfælde af, at en hændelse pågår på tidspunktet for indgivelsen af den endelige rapport, bør medlemsstaterne sikre, at berørte enheder forelægger en statusrapport på det pågældende tidspunkt og en endelig rapport senest en måned efter deres håndtering af den væsentlige hændelse.

(103) De væsentlige og vigtige enheder bør i givet fald og uden unødigt ophold underrette deres tjenestemodtagere om enhver foranstaltning eller modforholdsregel, de kan træffe for at afbøde risici fra en væsentlig cybertrussel. Disse enheder bør, hvor det er hensigtsmæssigt, og navnlig hvor den væsentlige cybertrussel sandsynligvis vil materialisere sig, også informere deres tjenestemodtagere om selve truslen. Kravet om at informere modtagerne om væsentlige cybertrusler bør opfyldes efter bedste evne, men bør ikke fritage disse enheder for forpligtelsen til for egen regning at træffe passende og øjeblikkelige foranstaltninger til at forebygge eller afhjælpe enhver trussel af denne art og genoprette tjenestens normale sikkerhedsniveau. Sådanne oplysninger om væsentlige cybertrusler bør stilles gratis til rådighed for modtagerne i et let forståeligt sprog.

(104) Udbydere af offentlige elektroniske kommunikationsnet eller af offentligt tilgængelige elektroniske kommunikationstjenester bør indføre sikkerhed gennem design og gennem standardindstillinger samt informere deres tjenestemodtagere om væsentlige cybertrusler og om de foranstaltninger, de kan træffe for at beskytte deres enheder og kommunikation, f.eks. ved at anvende bestemte typer software eller krypteringsteknologier.

(105) En proaktiv tilgang til cybertrusler er et afgørende element i styring af cybersikkerhedsrisici, som bør sætte de kompetente myndigheder i stand til effektivt at forhindre cybertrusler i at blive til hændelser, der

kan forårsage betydelige materiel eller immateriel skade. Med henblik herpå er underretning om cybertrusler af afgørende betydning. Enhederne opfordres med dette for øje til på frivillig basis at rapportere cybertrusler.

(106) For at forenkle rapporteringen af de oplysninger, der kræves i henhold til dette direktiv, og for at mindske den administrative byrde for enhederne bør medlemsstaterne stille tekniske midler til rådighed såsom et enkelt indgangspunkt, automatiserede systemer, onlineformularer, brugervenlige grænseflader, skabeloner og dedikerede platforme, som enheder, uanset om de falder ind under dette direktivs anvendelsesområde, til indgivelsen af de relevante oplysninger, der skal rapporteres. Unionens støtte til gennemførelsen af dette direktiv, navnlig inden for programmet for et digitalt Europa, der er oprettet ved Europa-Parlamentets og Rådets forordning (EU) 2021/694 ([21]), vil kunne omfatte støtte til enkelte indgangspunkter. Endvidere befinder enheder sig ofte i en situation, hvor en bestemt hændelse på grund af dens karakteristika skal rapporteres til forskellige myndigheder som følge af underretningspligten i forskellige retsakter. Sådanne tilfælde medfører ekstra administrative byrder og kunne også føre til usikkerhed med hensyn til formatet af og procedurerne for sådanne underretninger. Hvor der er oprettet et enkelt indgangspunkt, opfordres medlemsstaterne til også at anvende dette til underretninger om sikkerhedshændelser, der kræves i henhold til anden EU-ret, såsom forordning (EU) 2016/679 og direktiv 2002/58/EF. Anvendelsen af et sådant enkelt indgangspunkt til rapportering af sikkerhedshændelser i henhold til forordning (EU) 2016/679 og direktiv 2002/58/EF bør ikke berøre anvendelsen af bestemmelserne i forordning (EU) 2016/679 og direktiv 2002/58/EF, navnlig bestemmelserne vedrørende uafhængigheden af de deri omhandlede myndigheder. ENISA bør i samarbejde med samarbejdsgruppen udvikle fælles underretningsmodeller ved hjælp af retningslinjer, der kan forenkle og strømline de oplysninger, der skal rapporteres, i henhold til EU-retten, og mindske den administrative byrde for de underrettende enheder.

(107) Hvor der er mistanke om, at en hændelse har forbindelse til alvorlige kriminelle aktiviteter i henhold til EU-retten eller national ret, bør medlemsstaterne opfordre væsentlige og vigtige enheder til på grundlag af gældende strafferetsplejeregler i overensstemmelse med EU-retten at rapportere hændelser af formodet alvorlig kriminel karakter til de relevante retshåndhævende myndigheder. Hvor det er relevant, og uden at det berører de regler om beskyttelse af personoplysninger, der gælder for Europol, er det ønskeligt, at Det Europæiske Center for Bekæmpelse af Cyberkriminalitet (EC3) og ENISA letter koordineringen mellem de kompetente myndigheder og de retshåndhævende myndigheder i forskellige medlemsstater.

(108)Personoplysninger bliver i mange tilfælde kompromitteret som følge af hændelser. I den forbindelse bør de kompetente myndigheder samarbejde og udveksle oplysninger om alle relevante spørgsmål med de myndigheder, der er omhandlet i forordning (EU) 2016/679 og direktiv 2002/58/EF.

(109)Det er afgørende at opretholde nøjagtige og fuldstændige databaser over domænenavnsregistreringsdata (»WHOIS-data«) og give lovlig adgang til sådanne data for at sikre DNS'ens sikkerhed, stabilitet og modstandsdygtighed, hvilket igen bidrager til et højt fælles cybersikkerhedsniveau i hele Unionen. Med henblik herpå bør topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester, være forpligtet til at behandle visse data, der er nødvendige for at opfylde dette formål. Denne behandling bør udgøre en retlig forpligtelse i den i artikel 6, stk. 1, litra c), i forordning (EU) 2016/679 anvendte betydning. Denne forpligtelse berører ikke muligheden for at indsamle domænenavnsregistreringsdata til andre formål, f.eks. på grundlag af kontraktlige arrangementer eller retlige krav, der er fastsat i anden EU-ret eller national ret. Denne forpligtelse har til formål at opnå et fuldstændigt og nøjagtigt sæt af registreringsdata og bør ikke medføre, at de samme data indsamles flere gange. Topdomænenavneadministratorerne og de enheder, der leverer domænenavnsregistreringstjenester, bør samarbejde med hinanden for at undgå dobbeltarbejde.

(110)Tilgængeligheden af og den rettidige adgang til domænenavnsregistreringsdata for legitime adgangssøgende er afgørende for at forebygge og bekæmpe DNS-misbrug samt for at forebygge, og opdage og reagere på, hændelser. Ved legitime adgangssøgende forstås enhver fysisk eller juridisk person, der fremsætter en anmodning i henhold til EU-retten eller national ret. De kan omfatte myndigheder, som er kompetente i henhold til dette direktiv, og myndigheder, som i henhold til EU-retten eller national ret er kompetente til at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger, samt CERT'er eller CSIRT'er. Topdomæneadministratorer og enheder, der leverer domænenavnsregistreringstjenester, bør være forpligtet til at give lovlig adgang til specifikke domænenavnsregistreringsdata, som er nødvendige for anmodningen om adgang, for legitime adgangssøgende i overensstemmelse med EU-retten og national ret. Anmodningen fra legitime adgangssøgende bør ledsages af en begrundelse, der gør det muligt at vurdere nødvendigheden af adgang til dataene.

(111)For at sikre, at nøjagtige og fuldstændige domænenavnsregistreringsdata er til rådighed, bør topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester, indsamle og garantere integriteten og tilgængeligheden af domænenavnsregistreringsdata.

Topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester, bør navnlig fastlægge politikker og procedurer for indsamling og vedligeholdelse af nøjagtige og fuldstændige domænenavnsregistreringsdata samt for forebyggelse og rettelse af unøjagtige registreringsdata, i overensstemmelse med EU-databeskyttelsesretten. Disse politikker og procedurer bør så vidt muligt tage hensyn til de standarder, der er udviklet af multiinteressentstyringsstrukturerne på internationalt plan. Topdomænenavneadministratorerne og de enheder, der leverer domænenavnsregistreringstjenester, bør fastlægge og indføre forholdsmæssige procedurer til verifikation af domænenavnsregistreringsdata. Disse procedurer bør afspejle den bedste praksis, der anvendes i industrien, 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.

(112) Topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester, bør i overensstemmelse med præamblen til forordning (EU) 2016/679 forpligtes til at offentliggøre oplysninger om registrering af domænenavne, der ikke er omfattet af anvendelsesområdet for EU-databeskyttelsesretten, såsom data, der vedrører juridiske personer. For så vidt angår juridiske personer bør topdomænenavneadministratorerne og de enheder, der leverer domænenavnsregistreringstjenester, mindst offentliggøre registrantens navn og kontakttelefonnummer. Kontaktmailadressen bør også offentliggøres, forudsat at den ikke indeholder personoplysninger, såsom ved brug af e-mail-aliasser or funktionsmailadresser. Topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester, bør også give legitime adgangssøgende lovlig adgang til specifikke domænenavnsregistreringsdata om fysiske personer i overensstemmelse med EU-databeskyttelsesretten. Medlemsstaterne bør pålægger topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester, uden unødigt ophold at besvare anmodninger om udlevering af domænenavnsregistreringsdata fra legitime adgangssøgende. Topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester, bør fastlægge politikker og procedurer for offentliggørelse og udlevering af registreringsdata, herunder serviceleveranceaftaler til behandling af anmodninger om adgang fra legitime adgangssøgende. Disse politikker og procedurer bør så vidt muligt tage hensyn til eventuel vejledning og til de standarder, der er udviklet af multiinteressentstyringsstrukturerne på internationalt plan. Adgangsproceduren vil også kunne omfatte brug af en grænseflade, en

portal eller et andet teknisk værktøj til at tilvejebringe et effektivt system til anmodning om og adgang til registreringsdata. Med henblik på at fremme en harmoniseret praksis i hele det indre marked kan Kommissionen, uden at det berører Det Europæiske Databeskyttelsesråds beføjelser, fastlægge retningslinjer for sådanne procedurer, som så vidt muligt tager hensyn til de standarder, der er udviklet af multiinteressentstyringsstrukturerne på internationalt plan. Medlemsstaterne bør sikre, at alle former for adgang til personlige og ikkepersonlige domænenavnsregistreringsdata er gratis.

(113) Enheder, der er omfattet af dette direktivs anvendelsesområde, bør anses for at henhøre under jurisdiktionen i den medlemsstat, hvor de er etableret. Dog bør udbydere af offentlige elektroniske kommunikationsnet eller af offentligt tilgængelige elektroniske kommunikationstjenester anses for at henhøre under jurisdiktionen i den medlemsstat, hvor de leverer deres tjenester. DNS-tjenesteudbydere, topdomænenavneadministratorer, enheder, der leverer domænenavnsregistreringstjenester til topdomæner, 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 anses for at henhøre under jurisdiktionen i den medlemsstat, hvor de har deres hovedforretningssted i Unionen. Offentlige forvaltningsenheder bør henhøre under jurisdiktionen i den medlemsstat, der har oprettet dem. Hvis enheden leverer tjenester eller er etableret i mere end én medlemsstat, bør den henhøre under hver af disse medlemsstaters særskilte og parallelle jurisdiktion. De kompetente myndigheder i disse medlemsstater bør samarbejde, yde hinanden gensidig bistand og, hvor det er hensigtsmæssigt, gennemføre fælles tilsynstiltag. Hvor medlemsstaterne udøver deres jurisdiktion, bør de ikke pålægge håndhævelsesforanstaltninger eller sanktioner mere end én gang for den samme adfærd i overensstemmelse med princippet ne bis in idem.

(114) 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. Jurisdiktionen bør tillægges den medlemsstat, hvor den pågældende enhed har sit hovedforretningssted i Unionen. For så vidt angår dette direktiv indebærer forretningsstedskriteriet i dette direktiv

en faktisk udøvelse af virksomhed gennem faste ordninger. De pågældende ordningers juridiske form — hvorvidt der er tale om en filial eller et datterselskab med status som juridisk person — er ikke den afgørende faktor i denne forbindelse. Opfyldelsen af det nævnte kriterium bør ikke 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 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.

(115) Hvor en offentligt tilgængelig rekursiv DNS-tjeneste udbydes af en udbyder af offentlige elektroniske kommunikationsnet eller af offentligt tilgængelige elektroniske kommunikationstjenester kun som en del af dennes internetadgangstjeneste, bør enheden anses for at henhøre under jurisdiktionen i alle de medlemsstater, hvor dens tjenester udbydes.

(116) Hvor 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 Unionen, udbyder tjenester i Unionen, bør denne udpege en repræsentant i Unionen. Med henblik på at afgøre, om en sådan enhed udbyder tjenester i Unionen, bør det fastslås, om enheden har til hensigt at udbyde tjenester til personer i en eller flere medlemsstater. Det blotte faktum, at der i Unionen er adgang til enhedens eller en formidlers websted eller til en e-mailadresse og andre kontaktoplysninger, eller at der benyttes et sprog, som almindeligvis benyttes i det tredjeland, hvor enheden er etableret, bør anses for utilstrækkeligt til at fastslå en sådan hensigt. Imidlertid vil faktorer såsom anvendelse af et sprog eller en valuta, der almindeligvis anvendes i en eller flere medlemsstater, muligheden for at bestille tjenester på det pågældende sprog eller omtale

af kunder eller brugere, der befinder sig i Unionen, kunne gøre det åbenbart, at enheden har til hensigt at udbyde tjenester i Unionen. Repræsentanten bør handle på vegne af enheden, og det bør være muligt for de kompetente myndigheder eller CSIRT'er at kontakte repræsentanten. Repræsentanten bør have et udtrykkeligt skriftligt mandat fra enheden til at handle på sidstnævntes vegne for så vidt angår sidstnævntes forpligtelser, der er fastsat i dette direktiv, herunder rapportering af hændelser.

(117) For at sikre et klart overblik over 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, der leverer tjenester i hele Unionen, som er omfattet af dette direktivs anvendelsesområde, bør ENISA oprette og føre et register over sådanne enheder på grundlag af de oplysninger, som medlemsstaterne modtager, i givet fald gennem nationale mekanismer oprettet for, at enheder kan registrere dem selv. De centrale kontaktpunkter bør sende ENISA oplysningerne og eventuelle ændringer heraf. Med henblik på at sikre, at de oplysninger, som skal optages i dette register, er nøjagtige og fuldstændige, kan medlemsstaterne tilsende ENISA de oplysninger, der findes om de pågældende enheder i nationale registre. ENISA og medlemsstaterne bør træffe foranstaltninger til at fremme interoperabiliteten mellem sådanne registre, samtidig med at beskyttelsen af fortrolige eller klassificerede oplysninger sikres. ENISA bør fastsætte passende protokoller for klassificering og forvaltning af oplysninger for at sikre, at de udleverede oplysningers sikkerhed og fortrolighed bevares, og at adgangen til, lagringen af og overførsel af sådanne oplysninger begrænses til de tiltænkte brugere.

(118) Hvor oplysninger, der er klassificeret i overensstemmelse med EU-retten eller national ret udveksles, rapporteres eller på anden måde deles i henhold til dette direktiv, bør de tilsvarende regler for håndtering af klassificerede oplysninger finde anvendelse. Endvidere bør ENISA have infrastruktur, procedurer og regler på plads til at håndtere følsomme og klassificerede oplysninger i overensstemmelse med de gældende regler for sikkerhedsbeskyttelse af EU's klassificerede informationer.

(119) I takt med at cybertrusler bliver mere komplekse og sofistikerede, er evnen til at opdage sådanne trusler og træffe effektive forebyggelsesforanstaltninger mod dem i høj grad afhængig af regelmæssig udveksling af trussels- og sårbarhedsefterretninger mellem enheder. Udveks-

ling af oplysninger bidrager til øget bevidsthed om cybertrusler, hvilket igen styrker enhedernes evne til at forhindre trusler i at blive til hændelser og sætter dem i stand til bedre at inddæmme virkningerne af hændelser og reetablere sig mere effektivt. I mangel af vejledning på EU-plan synes flere faktorer at have hæmmet en sådan udveksling af efterretninger, navnlig usikkerhed om foreneligheden med konkurrence- og ansvarsregler.

(120) Enhederne bør tilskyndes til, med bistand fra medlemsstaterne, i fællesskab at udnytte deres individuelle viden og praktiske erfaring på strategisk, taktisk og operationelt plan med henblik på at styrke deres 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 cybersikkerhedsoplysninger. Med henblik herpå bør medlemsstaterne aktivt bistå og tilskynde enheder, såsom dem der leverer cybersikkerhedstjenester og -forskning, samt relevante enheder, der ikke er omfattet af dette direktivs anvendelsesområde til at deltage i sådanne ordninger for udveksling af cybersikkerhedsoplysninger. Disse ordninger bør etableres i overensstemmelse med EU-konkurrencereglerne og EU-databeskyttelsesretten.

(121) Væsentlige og vigtige enheders behandling af personoplysninger vil i det omfang, det er nødvendigt og står i et rimeligt forhold til målet om at sikre sikkerheden i net- og informationssystemer, kunne anses for at være lovlig, når en sådan behandling overholder en retlig forpligtelse, som påhviler den dataansvarlige, i overensstemmelse med betingelserne i artikel 6, stk. 1, litra c), og artikel 6, stk. 3, i forordning (EU) 2016/679. Behandling af personoplysninger vil også kunne være nødvendig for, at væsentlige og vigtige enheder samt udbydere af sikkerhedsteknologier og -tjenester, der handler på de nævnte enheders vegne, kan forfølge legitime interesser i henhold til artikel 6, stk. 1, litra f), i forordning (EU) 2016/679, herunder når en sådan behandling er nødvendig for ordninger for udveksling af cybersikkerhedsoplysninger eller frivillig underretning om relevante oplysninger i overensstemmelse med dette direktiv. Foranstaltninger vedrørende forebyggelse, opdagelse, identifikation, inddæmning, analyse og reaktion på hændelser, foranstaltninger til at øge bevidstheden vedrørende specifikke cybertrusler, udveksling af oplysninger i forbindelse med afhjælpning af sårbarheder og koordineret offentliggørelse af sårbarheder, frivillig udveksling af oplysninger om disse hændelser samt cybertrusler og sårbarheder, kompromitteringsindikatorer, taktikker, teknikker og procedurer, cybersikkerhedsadvarsler og konfigurationsværktøjer vil kunne kræve behandling af visse kategorier af personoplysninger såsom IP-adresser, uniform resources locators (URL'er), do-

mænenavne, e-mailadresser og, hvor disse afslører personlige oplysninger, tidsstempler. De kompetente myndigheders, de centrale kontaktpunkters og CSIRT'ernes behandling af personoplysninger vil kunne udgøre en retlig forpligtelse eller anses for at være nødvendig for udførelsen af en opgave i samfundets interesse eller henhørende under offentlig myndighedsudøvelse, som den ansvarlige har fået pålagt, i henhold til artikel 6, stk. 1, litra c) eller e), og artikel 6, stk. 3, i forordning (EU) 2016/679, eller for forfølgelsen af væsentlige og vigtige enheders legitime interesser, som omhandlet i artikel 6, stk. 1, litra f), i forordning (EU) 2016/679. Desuden vil der i national ret kunne fastsættes regler, der gør det muligt for de kompetente myndigheder, de centrale kontaktpunkter og CSIRT'erne, i det omfang det er nødvendigt og forholdsmæssigt for at sikre sikkerheden i væsentlige og vigtige enheders net- og informationssystemer, at behandle særlige kategorier af personoplysninger i overensstemmelse med artikel 9 i forordning (EU) 2016/679, navnlig ved at fastsætte passende og specifikke foranstaltninger til beskyttelse af fysiske personers grundlæggende rettigheder og interesser, herunder tekniske begrænsninger for videreanvendelse af sådanne data og anvendelse af sikkerheds- og privatlivsbevarende foranstaltninger på det aktuelle teknologiske stade såsom pseudonymisering eller kryptering, hvor anonymisering i væsentlig grad kan påvirke det forfulgte formål.

(122) For at styrke de tilsynsbeføjelser og -foranstaltninger, der bidrager til at sikre effektiv overholdelse, bør dette direktiv indeholde en minimumsliste over tilsynsforanstaltninger og -midler, hvorigennem de kompetente myndigheder kan føre tilsyn med væsentlige og vigtige enheder. Desuden bør der ved dette direktiv 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.

(123) De kompetente myndigheders udførelse af tilsynsopgaver bør ikke unødigt hæmme den berørte enheds forretningsaktiviteter. Hvor de kompetente myndigheder udfører deres tilsynsopgaver vedrørende væsentlige enheder, herunder i form af kontrol på stedet og eksternt tilsyn, efterforskning overtrædelser af dette direktiv og udførelse af sikkerhedsaudits eller -scanninger, bør de minimere indvirkningen på den berørte enheds forretningsaktiviteter.

(124) Ved udøvelsen af efterfølgende tilsyn bør de kompetente myndigheder kunne træffe afgørelse om prioriteringen af de tilsynsforanstaltninger og -midler, som de har til rådighed, på en forholdsmæssig måde. Dette indebærer, at de kompetente myndigheder kan træffe afgørelse om en sådan prioritering på grundlag af tilsynsmetoder, som bør baseres på en risikobaseret tilgang. Mere specifikt vil sådanne metoder kunne omfatte kriterier eller benchmarks for klassificering af væsentlige enheder i risikokategorier og tilsvarende anbefalede tilsynsforanstaltninger og -midler pr. risikokategori, som f.eks. brugen, hyppigheden eller typerne af kontrol på stedet, målrettede sikkerhedsaudits eller -scanninger, typen af oplysninger, der skal anmodes om, og detaljeringsgraden af disse oplysninger. Sådanne tilsynsmetoder vil også kunne ledsages af arbejdsprogrammer og vurderes og revideres regelmæssigt, herunder vedrørende aspekter såsom ressourcefordeling og -behov. For så vidt angår offentlige forvaltningsorganer bør tilsynsbeføjelserne udøves i overensstemmelse med de nationale lovgivningsmæssige og institutionelle rammer.

(125) De kompetente myndigheder bør sikre, at deres tilsynsopgaver i forbindelse med væsentlige og vigtige enheder udføres af uddannede fagfolk, som bør have de nødvendige færdigheder til at udføre disse opgaver, navnlig med hensyn til at udføre kontrol på stedet og eksternt tilsyn, herunder identifikation af svagheder i databaser, hardware, firewalls, kryptering og netværk. Denne kontrol og sådant tilsyn bør udføres på en objektiv måde.

(126) Den kompetente myndighed bør i behørigt begrundede tilfælde, hvor den er blevet bekendt med en væsentlig cybertrussel eller en overhængende risiko, omgående kunne træffe håndhævelsesafgørelser med henblik på at forebygge eller reagere på en hændelse.

(127) For at gøre håndhævelse effektiv bør der fastlægges en minimumsliste over håndhævelsesbeføjelser, der kan udøves for overtrædelse af foranstaltningerne til styring af cybersikkerhedsrisici og rapporteringskravene i dette direktiv, som opstiller en klar og konsekvent ramme for sådan håndhævelse i hele Unionen. Der bør 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. Håndhævelsesforanstaltningerne, herunder administrative bøder, bør være forholdsmæssige, og pålæggelsen heraf bør være underlagt passende proceduremæssige garantier i overensstemmelse med de generelle principper i EU-retten og Den Europæiske Unions charter om grundlæggende rettigheder (chartret), herunder adgangen til effektive retsmidler og retten til en retfærdig rettergang, uskyldsformodningen og retten til et forsvar.

(128) Dette direktiv forpligter ikke medlemsstaterne til at pålægge strafferetligt eller civilretligt ansvar for fysiske personer, der er ansvarlige for at sikre, at en enhed overholder dette direktiv, for skader, som tredjemand påføres som følge af en overtrædelse af dette direktiv.

(129) For at sikre en effektiv håndhævelse af de forpligtelser, der er fastsat i dette direktiv, bør hver kompetent myndighed have beføjelse til at pålægge eller anmode om pålæggelse af administrative bøder.

(130) Hvor en administrative bøde pålægges en væsentlig eller vigtig enhed, der er en virksomhed, bør der ved virksomhed i denne forbindelse forstås en virksomhed i overensstemmelse med artikel 101 og 102 i TEUF. Hvor en administrativ 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. Det bør være op til medlemsstaterne at bestemme, om og i hvilket omfang de offentlige myndigheder bør kunne pålægges administrative bøder. Pålæggelse af en administrativ bøde berører ikke de kompetente myndigheders anvendelse af andre beføjelser eller andre sanktioner, der er fastsat i de nationale regler til gennemførelse af dette direktiv.

(131) Medlemsstaterne bør kunne fastsætte regler om strafferetlige sanktioner for overtrædelse af de nationale regler til gennemførelse af dette direktiv. Dog bør pålæggelse af strafferetlige sanktioner for overtrædelse af sådanne nationale regler og af tilknyttede administrative sanktioner ikke føre til et brud på princippet ne bis in idem som fortolket af Den Europæiske Unions Domstol.

(132) 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. Sanktionernes art, herunder om de skal være strafferetlige eller administrative, bør fastsættes ved national ret.

(133) For yderligere at styrke effektiviteten og den afskrækkende virkning af de håndhævelsesforanstaltninger, der finder anvendelse på overtrædelser af dette direktiv, bør de kompetente myndigheder have beføjelse til midlertidigt at suspendere eller anmode om en midlertidig suspension af en certificering eller godkendelse vedrørende dele af eller alle de relevante tjenester, der leveres, eller aktiviteter, der udføres, af en væsentlig enhed, og kræve, at der indføres et midlertidigt forbud mod udøvelsen af ledelsesfunktioner for enhver fysisk person, der har ledelsesansvar på direktionsniveau eller som juridisk repræsentant. I betragtning af deres alvor og indvirkning på enhedernes aktiviteter og i sidste ende på brugerne bør sådanne midlertidige suspensioner eller forbud kun anvendes proportionalt med overtrædelsens alvor og under hensyntagen til omstændighederne i hver enkelttilfælde, herunder i lyset af, om overtrædelsen var forsætlig eller uagtsom, og ethvert tiltag, der er iværksat til at forebygge eller afbøde den materielle eller immaterielle skade. Sådanne midlertidige suspensioner eller forbud bør kun anvendes som en sidste udvej, dvs. først efter at de øvrige relevante håndhævelsesforanstaltninger, der er fastsat i dette direktiv, er udtømt, og kun indtil den pågældende enhed iværksætter de nødvendige tiltag for at afhjælpe manglerne eller opfylde kravene fra den kompetente myndighed, for hvilken sådanne midlertidige suspensioner eller forbud blev anvendt. Pålæggelse af sådanne midlertidige suspensioner eller forbud bør være underlagt passende proceduremæssige garantier i overensstemmelse med de generelle principper i EU-retten og chartret, herunder adgangen til effektive retsmidler og retten til en retfærdig rettergang, uskyldsformodningen og retten til et forsvar.

(134) For at sikre, at enhederne overholder deres forpligtelser fastsat i dette direktiv, bør medlemsstaterne samarbejde med og bistå hinanden med hensyn til tilsyns- og håndhævelsesforanstaltninger, navnlig hvor en enhed leverer tjenester i mere end én medlemsstat, eller hvor dens net- og informationssystemer er beliggende i en anden medlemsstat end den, hvori den leverer tjenesterne. Når den anmodede kompetente myndighed yder bistand, bør den træffe tilsyns- eller håndhævelsesforanstaltninger i overensstemmelse med national ret. For at sikre, at den gensidige bistand i henhold til dette direktiv fungerer gnidningsløst, bør de kompetente myndigheder anvende samarbejdsgruppen som et forum til at drøfte sager og specifikke anmodninger om bistand.

(135) For at sikre effektivt tilsyn og effektiv håndhævelse, navnlig i en situation med en grænseoverskridende dimension, bør en medlemsstat, der har modtaget en anmodning om gensidig bistand, inden for rammerne

af denne anmodning træffe passende tilsyns- og håndhævelsesforanstaltninger over for den enhed, der er genstand for denne anmodning, og som leverer tjenester eller har et net- og informationssystem på denne medlemsstats område.

(136) Dette direktiv bør fastlægge samarbejdsregler mellem de kompetente myndigheder og tilsynsmyndighederne i henhold til forordning (EU) 2016/679 med henblik på behandling af overtrædelser af dette direktiv vedrørende personoplysninger.

(137) Dette direktiv bør sigte mod at sikre et højt ansvarsniveau for de væsentlige og vigtige enheders foranstaltninger til styring af cybersikkerhedsrisici og rapporteringsforpligtelser. Derfor bør de væsentlige og vigtige enheders ledelsesorganer godkende foranstaltningerne til styring af cybersikkerhedsrisici og føre tilsyn med deres gennemførelse.

(138) For at sikre et højt fælles cybersikkerhedsniveau i hele Unionen på grundlag af dette direktiv bør beføjelsen til at vedtage retsakter delegeres til Kommissionen i overensstemmelse med artikel 290 i TEUF for så vidt angår supplering af dette direktiv 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. Det er navnlig vigtigt, at Kommissionen gennemfører relevante høringer under sit forberedende arbejde, herunder på ekspertniveau, og at disse høringer gennemføres i overensstemmelse med principperne i den interinstitutionelle aftale af 13. april 2016 om bedre lovgivning ([22]). For at sikre lige deltagelse i forberedelsen af delegerede retsakter modtager Europa-Parlamentet og Rådet navnlig alle dokumenter på samme tid som medlemsstaternes eksperter, og deres eksperter har systematisk adgang til møder i Kommissionens ekspertgrupper, der beskæftiger sig med forberedelse af delegerede retsakter.

(139) For at sikre ensartede betingelser for gennemførelsen af dette direktiv bør Kommissionen tillægges gennemførelsesbeføjelser til at fastlægge de proceduremæssige ordninger, der er nødvendige for samarbejdsgruppens funktion og de tekniske og metodologiske samt sektorspecifikke krav vedrørende foranstaltninger til styring af cybersikkerhedsrisici og til yderligere at præcisere typen af oplysninger, formatet og proceduren for underretning om hændelser, cybertrusler og nærvedhændelser og for kommunikation om væsentlige cybertrusler samt de tilfælde, hvor en hændelse skal anses for at være væsentlig. Disse beføjelser bør udøves i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) nr. 182/2011 ([23]).

(140) Kommissionen bør regelmæssigt evaluere dette direktiv efter høring af interessenter, navnlig med henblik på at afgøre, om det er hensigtsmæssigt at foreslå ændringer i lyset af skiftende samfundsmæssige,

politiske eller teknologiske vilkår eller markedsvilkår. Som led i disse evalueringer bør Kommissionen vurdere relevansen af størrelsen af de berørte enheder, sektorerne, delsektorerne og typerne af enheder omhandlet i dette direktivs bilag for, hvordan økonomien og samfundet fungerer i relation til cybersikkerhed. Kommissionen bør bl.a. vurdere, hvorvidt udbydere, der er omfattet af dette direktivs anvendelsesområde og er udpeget som meget store onlineplatforme i den i artikel 33 i Europa-Parlamentets og Rådets forordning (EU) 2022/2065 ([24]) anvendte betydning, vil kunne identificeres som væsentlige enheder i henhold til dette direktiv.

(141) Dette direktiv tildeler ENISA nye opgaver og styrker derved dets rolle og vil også kunne resultere i, at ENISA vil skulle udføre sine eksisterende opgaver i henhold til forordning (EU) 2019/881 på et højere niveau end tidligere. For at sikre, at ENISA har de nødvendige finansielle og menneskelige ressourcer til at udføre eksisterende og nye opgaver samt til at opnå et højere gennemførelsesniveau for disse opgaver som følge af sin styrkede rolle, bør dets budget forhøjes tilsvarende. For at sikre en effektiv anvendelse af ressourcerne bør ENISA desuden gives større handlefrihed i sin interne ressourcefordeling for at sætte det i stand til at udføre sine opgaver effektivt og indfri forventningerne.

(142) Målene for dette direktiv, nemlig at opnå et højt, fælles cybersikkerhedsniveau i hele Unionen, kan ikke i tilstrækkelig grad opfyldes af medlemsstaterne, men kan på grund af handlingens virkninger bedre nås på EU-plan; Unionen kan derfor vedtage foranstaltninger i overensstemmelse med nærhedsprincippet, jf. artikel 5 i traktaten om Den Europæiske Union. I overensstemmelse med proportionalitetsprincippet, jf. nævnte artikel, går dette direktiv ikke videre, end hvad der er nødvendigt for at nå disse mål.

(143) Dette direktiv respekterer de grundlæggende rettigheder og overholder de principper, som anerkendes i chartret, navnlig retten til respekt for privatliv og kommunikation og retten til beskyttelse af personoplysninger, friheden til at oprette og drive egen virksomhed, ejendomsretten, adgangen til effektive retsmidler og retten til en retfærdig rettergang, uskyldsformodningen og retten til et forsvar. Adgangen til effektive retsmidler gælder også modtagere af tjenester, der leveres af væsentlige og vigtige enheder. Direktivet bør gennemføres i overensstemmelse med disse rettigheder og principper.

(144) Den Europæiske Tilsynsførende for Databeskyttelse er blevet hørt i overensstemmelse med artikel 42, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) 2018/1725 ([25]) og afgav en udtalelse den 11. marts 2021 ([26]) —

VEDTAGET DETTE DIREKTIV:

## KAPITEL I
## GENERELLE BESTEMMELSER

*Artikel 1*

**Genstand**

1. Dette direktiv fastlægger foranstaltninger, der sigter på at opnå et højt fælles cybersikkerhedsniveau i hele Unionen med henblik på at forbedre det indre markeds funktion.

2. Med henblik herpå fastlægger dette direktiv:

a) forpligtelser, der kræver, at medlemsstaterne vedtager nationale cybersikkerhedsstrategier og udpeger eller opretter kompetente myndigheder, cyberkrisestyringsmyndigheder, centrale kontaktpunkter for cybersikkerhed (centrale kontaktpunkter) og enheder, der håndterer IT-sikkerhedshændelser (CSIRT'er)

b) foranstaltninger til styring af cybersikkerhedsrisici og rapporteringsforpligtelser for enheder af den type, der er omhandlet i bilag I eller II, samt for enheder, der er udpeget som kritiske enheder i henhold til direktiv (EU) 2022/2557

c) regler og forpligtelser vedrørende udveksling af cybersikkerhedsoplysninger

d) tilsyns- og håndhævelsesforpligtelser for medlemsstaterne.

*Artikel 2*

**Anvendelsesområde**

1. Dette direktiv finder anvendelse på offentlige eller private enheder af den type, der er omhandlet i 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 nævnte artikels stk. 1, og som leverer deres tjenester eller udfører deres aktiviteter inden for Unionen.

Artikel 3, stk. 4, i bilaget til nævnte henstilling finder ikke anvendelse for så vidt angår dette direktiv.

2. Uanset deres størrelse finder dette direktiv også anvendelse på enheder af den type, der er omhandlet i bilag I eller II, hvor:

a) tjenester leveres af:

i) udbydere af offentlige elektroniske kommunikationsnet eller af offentligt tilgængelige elektroniske kommunikationstjenester

ii) tillidstjenesteudbydere

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

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.

3. Uanset deres størrelse, finder dette direktiv anvendelse på enheder, der er identificeret som kritiske enheder i henhold til direktiv (EU) 2022/2557.

4. Uanset deres størrelse, finder dette direktiv anvendelse på enheder, der leverer domænenavnsregistreringstjenester.

5. Medlemsstater kan fastsætte, at dette direktiv finder anvendelse på:

a) offentlige forvaltningsenheder på lokalt plan

b) uddannelsesinstitutioner, navnlig hvor de udfører kritiske forskningsaktiviteter.

6. Dette direktiv berører ikke medlemsstaternes ansvar for at beskytte national sikkerhed og deres beføjelse til at beskytte andre væsentlige statslige funktioner, herunder sikring af statens territoriale integritet og opretholdelse af lov og orden.

7. Dette direktiv finder ikke 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.

8. Medlemsstater 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 denne artikels stk. 7, fra forpligtelserne i artikel 21 eller 23 for så vidt angår disse aktiviteter eller tjenester. I så fald finder de i 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.

9. Stk. 7 og 8 finder ikke anvendelse, hvor en enhed fungerer som tillidstjenesteudbyder.

10. Dette direktiv finder ikke anvendelse på enheder, som medlemsstaterne har undtaget fra anvendelsesområdet for forordning (EU) 2022/2554 i overensstemmelse med artikel 2, stk. 4, i nævnte forordning.

11. De forpligtelser, der er fastsat i dette direktiv, omfatter ikke meddelelse af oplysninger, hvis videregivelse ville stride mod væsentlige interesser med hensyn til medlemsstaternes nationale sikkerhed, offentlige sikkerhed eller forsvar.

12. Dette direktiv berører ikke forordning (EU) 2016/679, direktiv 2002/58/EF, Europa-Parlamentets og Rådets direktiv 2011/93/EU ([27]) og 2013/40/EU ([28]) samt direktiv (EU) 2022/2557.

13. Uden at det berører artikel 346 i TEUF, udveksles oplysninger, der er fortrolige i henhold til EU-regler eller nationale regler, såsom regler om forretningshemmeligheder, kun med Kommissionen og andre relevante myndigheder i overensstemmelse med dette direktiv, hvor denne udveksling er nødvendig for anvendelsen af dette direktiv. De udvekslede oplysninger 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.

14. Enheder, de kompetente myndigheder, de centrale kontaktpunkter og CSIRT'erne behandler personoplysninger i det omfang, det er nødvendigt med henblik på dette direktiv og i overensstemmelse med forordning (EU) 2016/679, navnlig på grundlag af artikel 6 deri.

Når udbydere af offentlige elektroniske kommunikationsnet eller af offentligt tilgængelige elektroniske kommunikationstjenester behandler personoplysninger i medfør af dette direktiv, skal det ske i overensstemmelse med EU-databeskyttelsesret og EU-retten om privatlivets fred, navnlig direktiv 2002/58/EF.

*Artikel 3*

**Væsentlige og vigtige enheder**

1. Med henblik på dette direktiv anses følgende enheder for at være væsentlige enheder:

a) enheder af en type, som er omhandlet i bilag I og som overskrider tærsklerne for mellemstore virksomheder, der er fastsat i artikel 2, stk. 1, i bilaget til henstilling 2003/361/EF

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 i henhold til artikel 2, i bilaget til henstilling 2003/361/EF

d) offentlige forvaltningsenheder omhandlet i artikel 2, stk. 2, litra f), nr. i)

e) alle andre enheder af en type omhandlet i 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, jf. artikel 2, stk. 3, i nærværende direktiv

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.

2. Med henblik på dette direktiv anses enheder af en type omhandlet i bilag I eller II, der ikke opfylder kriterierne for at være væsentlige enheder i henhold til denne artikels stk. 1, 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).

3. Senest den 17. april 2025 udarbejder medlemsstaterne en liste over væsentlige og vigtige enheder samt enheder, der leverer domænenavnsregistreringstjenester. Medlemsstaterne reviderer og, hvor det er relevant, ajourfører derefter listen med jævne mellemrum, mindst hvert andet år.

4. Med henblik på udarbejdelsen af den i stk. 3 omhandlede liste pålægger medlemsstaterne de enheder, der er omhandlet i nævnte stykke, 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 dette direktivs anvendelsesområde.

De i stk. 3 omhandlede enheder skal i tilfælde af ændringer af de oplysninger, de har indgivet i henhold til nærværende stykkes første afsnit, straks give underretning herom og under alle omstændigheder senest to uger efter datoen for ændringen.

Kommissionen fastlægger med bistand fra Den Europæiske Unions Agentur for Cybersikkerhed (ENISA) uden unødigt ophold retningslinjer og skabeloner vedrørende de forpligtelser, der er fastsat i dette stykke.

Medlemsstaterne kan indføre nationale mekanismer, hvorigennem enheder kan registrere sig selv.

5. Senest den 17. april 2025 og derefter hvert andet år underretter de kompetente myndigheder:

a) Kommissionen og samarbejdsgruppen om antallet af væsentlige og vigtige enheder, der er opført på den i stk. 3 omhandlede liste for hver af de sektorer og delsektorer, der er omhandlet i bilag I eller II, samt

b) Kommissionen om relevante oplysninger med hensyn til antallet af væsentlige og vigtige enheder, der er identificeret i medfør af artikel 2, stk. 2, litra b)-e), hvilke af sektorerne og delsektorerne i bilag I eller II, som de tilhører, hvilken type tjeneste de leverer, og hvilken af bestemmelserne i artikel 2, stk. 2, litra b)-e), i medfør af hvilken de blev identificeret.

6. Indtil til den 17. april 2025 og efter anmodning fra Kommissionen kan medlemsstaterne underrette Kommissionen om navnene på de væsentlige og vigtige enheder, der er omhandlet i stk. 5, litra b).

*Artikel 4*

**Sektorspecifikke EU-retsakter**

1. 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 dette direktiv, finder de relevante bestemmelser i dette direktiv, herunder bestemmelserne om tilsyn og håndhævelse, der er fastsat i kapitel VII, ikke finde anvendelse på sådanne enheder. I tilfælde, hvor sektorspecifikke EU-retsakter ikke omfatter alle enheder i en specifik sektor, der er omfattet af dette direktivs anvendelsesområde, finder de relevante bestemmelser i dette direktiv fortsat anvendelse på de enheder, der ikke er omfattet af de nævnte sektorspecifikke EU-retsakter.

2. De i denne artikels stk. 1 omhandlede krav anses for at have samme virkning som de forpligtelser, der er fastsat i dette direktiv, hvor:

a) foranstaltningerne til styring af cybersikkerhedsrisici har mindst samme virkning som dem, der er fastsat i 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 dette direktiv 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 dette direktivs artikel 23, stk. 1-6.

3. Kommissionen fastlægger senest den 17. juli 2023 retningslinjer, der præciserer anvendelsen af stk. 1 og 2. Kommissionen reviderer regelmæssigt disse retningslinjer. Ved udarbejdelsen af disse retningslinjer tager Kommissionen hensyn til eventuelle bemærkninger fra samarbejdsgruppen og ENISA.

*Artikel 5*

**Minimumsharmonisering**

Dette direktiv er ikke til hinder for, at medlemsstaterne vedtager eller opretholder bestemmelser, der sikrer et højere cybersikkerhedsniveau, forudsat at sådanne bestemmelser er i overensstemmelse med medlemsstaternes forpligtelser, der er fastsat i EU-retten.

*Artikel 6*

**Definitioner**

I dette direktiv forstås ved:

1) »net- og informationssystem«:

a) et elektronisk kommunikationsnet som defineret i artikel 2, nr. 1), i direktiv (EU) 2018/1972

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, eller

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

2) »sikkerhed i net- og informationssystemer«: net- og informationssystemers evne til, på et givet sikkerhedsniveau, at modstå enhver begivenhed, der kan være til skade for tilgængeligheden, autenticiteten, integriteten eller fortroligheden af lagrede, overførte eller behandlede data eller af de tjenester, der tilbydes af eller er tilgængelige via disse net- og informationssystemer

3) »cybersikkerhed«: cybersikkerhed som defineret i artikel 2, nr. 1), i forordning (EU) 2019/881

4) »national cybersikkerhedsstrategi«: en medlemsstats sammenhængende ramme, der opstiller strategiske mål og prioriteter på cybersikkerhedsområdet og styringen for at nå dem i den pågældende medlemsstat

5) »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 i at materialisere sig, eller som ikke materialiserede sig

6) »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

7) »omfattende cybersikkerhedshændelse«: en hændelse, der forårsager en forstyrrelse på et niveau, som overstiger en medlemsstats kapacitet til at reagere på den, eller som har en betydelig indvirkning på mindst to medlemsstater

8) »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

9) »risiko«: 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

10) »cybertrussel«: en cybertrussel som defineret i artikel 2, nr. 8), i forordning (EU) 2019/881

11) »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 materiel eller immateriel skade

12) »IKT-produkt«: et IKT-produkt som defineret i artikel 2, nr. 12), i forordning (EU) 2019/881

13) »IKT-tjeneste«: en IKT-tjeneste som defineret i artikel 2, nr. 13), i forordning (EU) 2019/881

14) »IKT-proces«: en IKT-proces som defineret i artikel 2, nr. 14), i forordning (EU) 2019/881

15) »sårbarhed«: en svaghed, modtagelighed eller fejl ved IKT-produkter eller -tjenester, som kan udnyttes af en cybertrussel

16) »standard«: standard som defineret i artikel 2, nr. 1), i Europa-Parlamentets og Rådets forordning (EU) nr. 1025/2012 ([29])

17) »teknisk specifikation«: en teknisk specifikation som defineret i artikel 2, nr. 4), i forordning (EU) nr. 1025/2012

18) »internetudvekslingspunkt« en netfacilitet, som muliggør sammenkobling af mere end to uafhængige net (autonome systemer), hovedsageligt med henblik på at lette udvekslingen af internettrafik, som kun leverer sammenkobling til autonome systemer og som hverken kræver, at internettrafik, som bevæger sig mellem et givent par af deltagende autonome systemer, passerer gennem et eventuelt tredje autonomt system, eller ændrer eller på anden måde griber ind i en sådan trafik

19) »domænenavnesystem« eller »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

20) »DNS-tjenesteudbyder«: en enhed, der leverer:

    a)offentligt tilgængelige rekursive domænenavnsoversættelsestjenester til internetslutbrugere, eller

    b)autoritative domænenavnsoversættelsestjenester til tredjepartsbrug, med undtagelse af rodnavneservere

21) »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 hvorvidt nogen af disse operationer udføres af enheden selv eller outsources, men ikke situationer, hvor topdomænenavne kun anvendes af en administrator til eget brug

22) »enhed, der leverer domænenavnsregistreringstjenester«: en registrator eller en agent, der handler på vegne af registratorer, såsom en udbyder eller videresælger af privatlivs- eller proxyregistreringstjenester

23) »digital tjeneste«: en tjeneste som defineret i artikel 1, stk. 1, litra b), i Europa-Parlamentets og Rådets direktiv (EU) 2015/1535 ([30])

24) »tillidstjeneste«: en tillidstjeneste som defineret i artikel 3, nr. 16), i forordning (EU) nr. 910/2014

25) »tillidstjenesteudbyder«: en tillidstjenesteudbyder som defineret i artikel 3, nr. 19), i forordning (EU) nr. 910/2014

26) »kvalificeret tillidstjeneste«: en kvalificeret tillidstjeneste som defineret i artikel 3, nr. 17), i forordning (EU) nr. 910/2014

27) »kvalificeret tillidstjenesteudbyder«: en kvalificeret tillidstjenesteudbyder som defineret i artikel 3, nr. 20), i forordning (EU) nr. 910/2014

28) »onlinemarkedsplads«: en onlinemarkedsplads som defineret i artikel 2, litra n), i Europa-Parlamentets og Rådets direktiv 2005/29/EF ([31])

29) »onlinesøgemaskine«: en onlinesøgemaskine som defineret i artikel 2, nr. 5), i Europa-Parlamentets og Rådets forordning (EU) 2019/1150 ([32])

30) »cloudcomputingtjeneste«: en digital tjeneste, som muliggør on demand-administration og giver bred fjernadgang til en skalerbar og elastisk pulje af delbare computerressourcer, herunder hvor disse ressourcer er fordelt mellem flere lokaliteter

31) »datacentertjeneste«: en tjeneste, der omfatter strukturer eller grupper af strukturer, der er beregnet til central opbevaring, sammenkobling og drift af IT- og netværksudstyr, der leverer datalagrings-, -behandlings- og -transporttjenester samt alle faciliteter og infrastrukturer til energidistribution og miljøkontrol

32) »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

33) »platform for sociale netværkstjenester«: en platform, der sætter slutbrugere i stand til at komme i forbindelse, dele, opdage og kommunikere med hinanden på tværs af forskellige anordninger, navnlig via chats, opslag, videoer og anbefalinger

34) »repræsentant«: en fysisk eller juridisk person, der er etableret i Unionen, 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 Unionen, og som kan kontaktes af en kompetent myndighed eller en CSIRT på enhedens sted for så vidt angår denne enheds forpligtelser i henhold til dette direktiv

35) »offentlig forvaltningsenhed«: en enhed, der er anerkendt som sådan i en medlemsstat i overensstemmelse med national ret, med undtagelse af retsvæsenet, parlamenter og centralbanker, som opfylder følgende kriterier:

   a) den er oprettet med henblik på at opfylde almennyttige formål og har ikke industriel eller kommerciel karakter

b) den har status som juridisk person, eller den er ved lov berettiget til at handle på vegne af en anden enhed med status som juridisk person

c) den finansieres overvejende 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

d) den 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

36) »offentligt elektronisk kommunikationsnet«: et offentligt elektronisk kommunikationsnet som defineret i artikel 2, nr. 8), i direktiv (EU) 2018/1972

37) »elektronisk kommunikationstjeneste«: en elektronisk kommunikationstjeneste som defineret i artikel 2, nr. 4), i direktiv (EU) 2018/1972

38) »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

39) »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

40) »udbyder af administrerede sikkerhedstjenester«: en udbyder af administrerede tjenester, der udfører eller yder assistance til aktiviteter vedrørende styring af cybersikkerhedsrisici

41) »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, men som ikke indbefatter uddannelsesinstitutioner.

## KAPITEL II

## KOORDINEREDE RAMMER FOR CYBERSIKKERHED

*Artikel 7*

### National cybersikkerhedsstrategi

1. Hver medlemsstat vedtager en national cybersikkerhedsstrategi, der fastlægger de 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. Den nationale cybersikkerhedsstrategi skal omfatte:

a) mål og prioriteter for medlemsstatens cybersikkerhedsstrategi, navnlig for de sektorer, der er omhandlet i bilag I og II

b) en styringsramme med henblik på at nå de i dette stykkes litra a) omhandlede mål og prioriteter, herunder de politikker, der er omhandlet i stk. 2

c) en styringsramme, der præciserer de relevante interessenters roller og ansvarsområder på nationalt plan og understøtter samarbejdet og koordineringen på nationalt plan mellem de kompetente myndigheder, de centrale kontaktpunkter og CSIRT'erne i henhold til dette direktiv samt koordinering og samarbejde mellem disse organer og kompetente myndigheder i henhold til sektorspecifikke EU-retsakter

d) en mekanisme til at identificere relevante aktiver og en vurdering af risiciene i den pågældende medlemsstat

e) en identifikation af de foranstaltninger, der sikrer beredskabet for og evnen til at reagere på og reetablere sig efter hændelser, herunder samarbejde mellem den offentlige og den private sektor

f) en liste over de forskellige myndigheder og interessenter, der er involveret i gennemførelsen af den nationale cybersikkerhedsstrategi

g) en politisk ramme for øget koordinering mellem de kompetente myndigheder i henhold til dette direktiv og de kompetente myndigheder i henhold til direktiv (EU) 2022/2557 med henblik på udveksling af oplysninger om risici, cybertrusler og hændelser samt om ikke-cyberrelaterede risici, trusler og hændelser og udøvelse af tilsynsopgaver, alt efter hvad der er relevant.

h) en plan, herunder med de nødvendige foranstaltninger, for højnelse af borgernes generelle bevidsthed om cybersikkerhed.

2. Som led i den nationale cybersikkerhedsstrategi skal medlemsstaterne navnlig vedtage politikker for:

a) håndtering af cybersikkerhed i forsyningskæden for IKT-produkter og -tjenester, der anvendes af enheder til levering af deres tjenester

b) inklusion og specificering af cybersikkerhedsrelaterede krav til IKT-produkter og -tjenester i forbindelse med offentlige indkøb, herunder vedrørende cybersikkerhedscertificering, kryptering og brugen af open source-cybersikkerhedsprodukter

c) håndtering af sårbarheder, der omfatter fremme og facilitering af koordineret offentliggørelse af sårbarheder i henhold til artikel 12, stk. 1

d) opretholdelse af den generelle tilgængelighed, integritet og fortrolighed af den offentlige centrale del af det åbne internet, herunder, hvor det er relevant, undersøiske kommunikationskablers cybersikkerhed

e) fremme af udviklingen og integrationen af relevante avancerede teknologier, der har til formål at gennemføre foranstaltninger på det aktuelle teknologiske stade til styring af cybersikkerhedsrisici

f) fremme og udvikling af uddannelse i cybersikkerhed, cybersikkerhedsfærdigheder, -bevidstgørelse og -forskning og -udviklingsinitiativer samt vejledning om god praksis for og kontrol med cyberhygiejne rettet mod borgere, interessenter og enheder

g) støtte til akademiske institutioner og forskningsinstitutioner med henblik på at udvikle, forbedre og fremme udbredelsen af cybersikkerhedsværktøjer og sikker netinfrastruktur

h) indførelse af relevante procedurer og passende informationsdelingsværktøjer til støtte for frivillig udveksling af cybersikkerhedsoplysninger mellem enheder i overensstemmelse med EU-retten

i) styrkelse af den grundlæggende cyberrobusthed og cyberhygiejne i små og mellemstore virksomheder, navnlig dem, der er udelukket fra dette direktivs anvendelsesområde, ved at yde let tilgængelig vejledning og bistand til opfyldelse af deres specifikke behov

j) fremme af aktiv cyberbeskyttelse.

3. Medlemsstaterne underretter Kommissionen om deres nationale cybersikkerhedsstrategier senest tre måneder efter vedtagelsen deraf. Medlemsstaterne kan udelade oplysninger, der vedrører deres nationale sikkerhed, fra sådanne underretninger.

4. Regelmæssigt og mindst hvert femte år vurderer og om fornødent ajourfører medlemsstaterne deres nationale cybersikkerhedsstrategier på grundlag af centrale præstationsindikatorer. ENISA bistår på anmodning medlemsstaterne med at udvikle eller ajourføre en national strategi og nøgleresultatindikatorer til vurdering af denne strategi med henblik på at bringe den i overensstemmelse med de krav og forpligtelser, der er fastsat i dette direktiv.

*Artikel 8*

**Kompetente myndigheder og centrale kontaktpunkter**

1. Hver medlemsstat udpeger eller opretter en eller flere kompetente myndigheder med ansvar for cybersikkerhed og for de tilsynsopgaver, der er omhandlet i kapitel VII (kompetente myndigheder).

2. De i stk. 1 omhandlede kompetente myndigheder fører tilsyn med gennemførelsen af dette direktiv på nationalt plan.

3. Hver medlemsstat udpeger eller opretter et centralt kontaktpunkt. Hvor en medlemsstat kun udpeger eller opretter én kompetent myndighed i henhold til stk. 1, skal denne kompetente myndighed også være det centrale kontaktpunkt i den pågældende medlemsstat.

4. Hvert enkelt centrale kontaktpunkt udøver en forbindelsesfunktion for at sikre grænseoverskridende samarbejde mellem dets medlemsstats myndigheder og andre medlemsstaters relevante myndigheder og, hvor det er relevant, Kommissionen og ENISA, samt for at sikre tværsektorielt samarbejde med andre kompetente myndigheder i dets medlemsstat.

5. Medlemsstaterne sikrer, at deres kompetente myndigheder og centrale kontaktpunkter har tilstrækkelige ressourcer til på en effektiv måde at udføre de opgaver, som de pålægges, og dermed opfylde dette direktivs mål.

6. Hver medlemsstat underretter uden unødigt ophold Kommissionen om identiteten af den i stk. 1 omhandlede kompetente myndighed og af det i stk. 3 omhandlede centrale kontaktpunkt, om disse myndigheders opgaver og om enhver senere ændring heraf. Hver medlemsstat offentliggør sin kompetente myndigheds identitet. Kommissionen gør en liste over de centrale kontaktpunkter offentligt tilgængelig.

*Artikel 9*

**Nationale rammer for cyberkrisestyring**

1. Hver medlemsstat udpeger eller opretter en eller flere kompetente myndigheder med ansvar for styring af omfattende cybersikkerhedshændelser og kriser (cyberkrisestyringsmyndigheder). Medlemsstaterne sikrer, at disse myndigheder har tilstrækkelige ressourcer til at udføre de opgaver, de pålægges, på en virkningsfuld og effektiv måde. Medlemsstaterne sikrer sammenhængen med de eksisterende rammer for generel national krisestyring.

2. Hvor en medlemsstat udpeger eller opretter mere end én cyberkrisestyringsmyndighed i henhold til stk. 1, skal den klart angive, hvilken af disse myndigheder der skal fungere som koordinator for styringen af omfattende cybersikkerhedshændelser og kriser.

3. Hver medlemsstat identificerer kapaciteter, aktiver og procedurer, der kan indsættes i tilfælde af en krise inden for rammerne af dette direktiv.

4. Hver medlemsstat vedtager en national beredskabsplan for omfattende cybersikkerhedshændelser og kriser, hvor målene og ordningerne for håndtering af omfattende cybersikkerhedshændelser og kriser er fastsat. Denne plan skal navnlig fastlægge:

a) målene for de nationale beredskabsforanstaltninger og –aktiviteter

b) cyberkrisestyringsmyndighedernes opgaver og ansvarsområder

c) cyberkrisestyringsprocedurerne, herunder deres integration i den generelle nationale krisestyringsramme, og kanalerne for udveksling af oplysninger

d) nationale beredskabsforanstaltninger, herunder øvelses- og uddannelsesaktiviteter

e) de relevante involverede offentlige og private interessenter og infrastrukturer

f) nationale procedurer og ordninger mellem relevante nationale myndigheder og organer for at sikre medlemsstatens effektive deltagelse i og støtte til den koordinerede håndtering af omfattende cybersikkerhedshændelser og kriser på EU-plan.

5. Senest tre måneder efter udpegelsen eller oprettelsen af den i stk. 1 omhandlede cyberkrisestyringsmyndighed underretter hver medlemsstat Kommissionen om sin myndigheds identitet og om eventuelle senere ændringer heraf. Medlemsstaterne forelægger senest tre måneder efter vedtagelsen af deres nationale beredskabsplaner for omfattende cybersikkerhedshændelser og kriser Kommissionen og det europæiske netværk af cybersikkerhedsforbindelsesorganisationer (EU-CyCLONe) relevante oplysninger vedrørende de i stk. 4 indeholdte krav til disse planer. Medlemsstaterne kan udelade oplysninger, hvor og i det omfang en sådan udeladelse er nødvendig for deres nationale sikkerhed.

*Artikel 10*

**Enheder, der håndterer IT-sikkerhedshændelser (CSIRT'er)**

1. Hver medlemsstat udpeger eller opretter en eller flere CSIRT'er. CSIRT'erne kan udpeges eller oprettes inden for en kompetent myndighed. CSIRT'erne skal opfylde kravene i artikel 11, stk. 1, mindst dække de sektorer, delsektorer og typer af enheder, der er omhandlet i bilag I og II, og være ansvarlige for håndtering af hændelser i overensstemmelse med en nøje fastlagt proces.

2. Medlemsstaterne sikrer, at hver CSIRT har tilstrækkelige ressourcer til effektivt at udføre sine opgaver som fastsat i artikel 11, stk. 3.

3. Medlemsstaterne sikrer, at hver CSIRT råder over en passende, sikker og modstandsdygtig kommunikations- og informationsinfrastruktur til udveksling af oplysninger med væsentlige og vigtige enheder og andre relevante interessenter. Med henblik herpå sikrer medlemsstaterne, at hver CSIRT bidrager til udbredelsen af sikre værktøjer til udveksling af oplysninger.

4. CSIRT'erne samarbejder og, hvor det er relevant, udveksler relevante oplysninger i overensstemmelse med artikel 29 med sektorielle eller tværsektorielle fællesskaber af væsentlige og vigtige enheder.

5. CSIRT'erne deltager i peerevalueringer, der tilrettelægges i overensstemmelse med artikel 19.

6. Medlemsstaterne sikrer et effektivt og sikkert samarbejde mellem deres CSIRT'er i CSIRT-netværket.

7. CSIRT'erne kan etablere samarbejdsrelationer med tredjelandes nationale enheder, der håndterer IT-sikkerhedshændelser. Som led i sådanne samarbejdsrelationer skal medlemsstaterne lette effektiv og sikker udveksling af oplysninger med disse tredjelandes nationale enheder, der håndterer IT-sikkerhedshændelser, ved hjælp af relevante protokoller for udveksling af oplysninger, herunder Traffic Light Protocol. CSIRT'erne kan udveksle relevante oplysninger med tredjelandes nationale enheder, der håndterer IT-sikkerhedshændelser, herunder personoplysninger i overensstemmelse med EU-databeskyttelsesret.

8. CSIRT'erne kan samarbejde med tredjelandes nationale enheder, der håndterer IT-sikkerhedshændelser, eller tilsvarende organer i tredjelande, navnlig med henblik på at yde dem cybersikkerhedsbistand.

9. Hver medlemsstat underretter uden unødigt ophold Kommissionen om identiteten af den eller de i denne artikels stk. 1 omhandlede CSIRT'er og den CSIRT, der er udpeget som koordinator i henhold til artikel 12, stk. 1, om deres respektive opgaver i relation til væsentlige og vigtige enheder og om eventuelle efterfølgende ændringer heraf.

10. Medlemsstaterne kan anmode ENISA om bistand til at udvikle deres CSIRT'er.

*Artikel 11*

**Krav til CSIRT'er og deres tekniske kapaciteter og opgaver**

1. CSIRT'erne skal opfylde nedenstående krav:

a) CSIRT'erne skal sikre et højt tilgængelighedsniveau for deres kommunikationskanaler ved at undgå enkelte fejlpunkter og ved til enhver tid at have flere muligheder for at blive kontaktet og for at kontakte andre; de skal tydeligt angive kommunikationskanalerne og bringe dem til brugergruppers og samarbejdspartneres kundskab

b) CSIRT'ernes lokaler og de underliggende informationssystemer skal være placeret i sikrede lokaliteter

c) CSIRT'erne skal være udstyret med et passende system til at administrere og videresende anmodninger, navnlig med henblik på at lette effektive overdragelser

d) CSIRT'erne skal sikre fortroligheden og troværdigheden af deres operationer

e) CSIRT'erne skal have tilstrækkeligt personale til at sikre, at deres tjenester er tilgængelige på alle tidspunkter, og de skal sikre, at deres personale er behørigt uddannet

f) CSIRT'erne skal være udstyret med redundante systemer og backup-arbejdsplads for at sikre kontinuiteten af deres tjenester.

CSIRT'erne kan deltage i internationale samarbejdsnetværk.

2. Medlemsstaterne sikrer, at deres CSIRT'er i fællesskab har den tekniske kapacitet, der er nødvendig for at udføre de opgaver, der er omhandlet i stk. 3. Medlemsstaterne sikrer, at deres CSIRT'er har de fornødne ressourcer til at sikre et tilstrækkeligt personaleniveau, med henblik på at gøre det muligt, at CSIRT'erne kan udvikle deres tekniske kapacitet.

3. 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 og 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 at fungere som koordinator med henblik på den koordinerede offentliggørelse af sårbarheder i henhold til artikel 12, stk. 1

h) at bidrage til udbredelsen af sikre værktøjer til udveksling af oplysninger i henhold til artikel 10, stk. 3.

CSIRT'erne kan foretage proaktiv ikkeindgribende 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.

Ved udførelsen af de opgaver, der er omhandlet i første afsnit, kan CSIRT'erne prioritere særlige opgaver på grundlag af en risikobaseret tilgang.

4. CSIRT'erne etablerer samarbejdsrelationer med relevante interessenter i den private sektor med henblik på at nå dette direktivs mål.

5. For at lette det i stk. 4 omhandlede samarbejde fremmer CSIRT'erne vedtagelsen og anvendelsen af fælles eller standardiserede praksisser, klassificeringsordninger og taksonomier i forbindelse med:

a) procedurer for håndtering af hændelser

b) krisestyring og

c) koordineret offentliggørelse af sårbarheder i henhold til artikel 12, stk. 1.

*Artikel 12*

**Koordineret offentliggørelse af sårbarheder og en europæisk sårbarhedsdatabase**

1. Hver medlemsstat udpeger en af sine CSIRT'er som koordinator med henblik på koordineret offentliggørelse af sårbarheder. Den CSIRT, der er udpeget som koordinator, fungerer som betroet formidler, der, hvor det er nødvendigt, letter interaktionen mellem den fysiske eller juridiske person, der rapporterer en sårbarhed, og producenten eller udbyderen af de potentielt sårbare IKT-produkter eller -tjenester på anmodning fra en af parterne. Opgaverne for den CSIRT, der er udpeget som koordinator, omfatter:

a) identifikation af og kontakt til de berørte enheder

b) bistand til de fysiske eller juridiske personer, der rapporterer en sårbarhed og

c) forhandling af tidsfrister for offentliggørelse og håndtering af sårbarheder, der berører flere enheder.

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. Hvor en rapporteret sårbarhed vil kunne have en væsentlig indvirkning på enheder i mere end én medlemsstat, samarbejder den CSIRT, der er udpeget som koordinator for hver berørt medlemsstat, om nødvendigt med andre CSIRT'er, der er udpeget som koordinatorer, inden for CSIRT-netværket.

2. ENISA udvikler og vedligeholder efter høring af samarbejdsgruppen en europæisk sårbarhedsdatabase. Med henblik herpå opretter og vedligeholder

ENISA passende informationssystemer, -politikker og -procedurer og træffer de nødvendige tekniske og organisatoriske foranstaltninger til at garantere den europæiske sårbarhedsdatabases sikkerhed og integritet, navnlig med det formål at sætte enheder, uanset om de er omfattet af dettes direktivs anvendelsesområde, og deres leverandører af net- og informationssystemer, i stand til på frivillig basis at oplyse om og registrere offentligt kendte sårbarheder i IKT-produkter eller -tjenester. Alle interessenter skal have adgang til oplysningerne om sårbarhederne i den europæiske sårbarhedsdatabase. Denne database indeholder:

a) oplysninger, der beskriver sårbarheden

b) de berørte IKT-produkter eller -tjenester og sårbarhedens alvor med hensyn til de omstændigheder, hvorunder den kan udnyttes

c) tilgængeligheden af relaterede patches og, i mangel af tilgængelige patches, vejledning fastlagt af de kompetente myndigheder eller CSIRT'erne til brugere af sårbare IKT-produkter og -tjenester om, hvordan risiciene som følge af afslørede sårbarheder kan afbødes.

*Artikel 13*

**Samarbejde på nationalt plan**

1. Hvor de kompetente myndigheder, det centrale kontaktpunkt og CSIRT'erne i samme medlemsstat er adskilt fra hinanden, samarbejder de med hensyn til opfyldelsen af forpligtelserne, der er fastsat i dette direktiv.

2. Medlemsstaterne sikrer, at deres CSIRT'er eller i givet fald deres kompetente myndigheder modtager underretninger om væsentlige hændelser i henhold til artikel 23 og om hændelser, cybertrusler og nærvedhændelser i henhold til artikel 30.

3. Medlemsstaterne sikrer, at deres CSIRT'er eller i givet fald deres kompetente myndigheder oplyser deres centrale kontaktpunkter om underretninger om hændelser, cybertrusler og nærvedhændelser indgivet i henhold til dette direktiv.

4. For at sikre, at de kompetente myndigheders, de centrale kontaktpunkters og CSIRT'ernes opgaver og forpligtelser udføres effektivt, sikrer medlemsstaterne i muligt omfang et passende samarbejde mellem disse organer og retshåndhævende myndigheder, databeskyttelsesmyndigheder, de nationale myndigheder i henhold til forordning (EF) nr. 300/2008 og (EU) 2018/1139, tilsynsorganerne i henhold til forordning (EU) nr. 910/2014, de kompetente myndigheder i henhold til forordning (EU) 2022/2554, de nationale tilsynsmyndigheder i henhold til direktiv (EU) 2018/1972, de kompetente myndigheder i henhold til direktiv (EU) 2022/2557, samt de kompetente myndigheder i henhold til andre sektorspecifikke EU-retsakter, i den pågældende medlemsstat.

5. Medlemsstaterne sikrer, at deres kompetente myndigheder i henhold til dette direktiv og deres kompetente myndigheder i henhold til direktiv (EU) 2022/2557 regelmæssigt samarbejder og udveksler oplysninger vedrørende identifikation af kritiske enheder, om risici, cybertrusler og hændelser samt om ikke-cyberrelaterede risici, trusler og hændelser, som påvirker væsentlige enheder, der er identificeret som kritiske enheder i henhold til direktiv (EU) 2022/2557, og de foranstaltninger, der træffes som reaktion på sådanne risici, trusler og hændelser. Medlemsstaterne sikrer endvidere, at deres kompetente myndigheder i henhold til nærværende direktiv og deres kompetente myndigheder i henhold til forordning (EU) nr. 910/2014, forordning (EU) 2022/2554 og direktiv (EU) 2018/1972 regelmæssigt udveksler relevante oplysninger, herunder om relevante hændelser og cybertrusler.

6. Medlemsstaterne forenkler rapporteringen ved hjælp af tekniske midler for underretninger omhandlet i artikel 23 og 30.

## KAPITEL III
## SAMARBEJDE PÅ EU-PLAN OG INTERNATIONALT PLAN

*Artikel 14*

### Samarbejdsgruppe

1. For at støtte og lette strategisk samarbejde og udvekslingen af oplysninger mellem medlemsstaterne samt for at styrke tillid og fortrolighed nedsættes der en samarbejdsgruppe.

2. Samarbejdsgruppen udfører sine opgaver på grundlag af toårige arbejdsprogrammer omhandlet i stk. 7.

3. Samarbejdsgruppen består af repræsentanter fra medlemsstaterne, Kommissionen og ENISA. Tjenesten for EU's Optræden Udadtil deltager som observatør i samarbejdsgruppens aktiviteter. De europæiske tilsynsmyndigheder (ESA'er) og de kompetente myndigheder i henhold til forordning (EU) 2022/2554 kan deltage i samarbejdsgruppens aktiviteter i overensstemmelse med artikel 47, stk. 1, i nævnte forordning.

Samarbejdsgruppen kan, hvor det er relevant, indbyde Europa-Parlamentet og repræsentanter for relevante interessenter til at deltage i dens arbejde.

Sekretariatsopgaverne varetages af Kommissionen.

4. Samarbejdsgruppen har følgende opgaver:

a) at vejlede de kompetente myndigheder vedrørende omsætningen og gennemførelsen af dette direktiv

b) at vejlede de kompetente myndigheder vedrørende udviklingen og gennemførelsen af politikker for koordineret offentliggørelse af sårbarheder som omhandlet i artikel 7, stk. 2, litra c)

c) at udveksle bedste praksis og oplysninger vedrørende gennemførelsen af dette direktiv, herunder vedrørende cybertrusler, hændelser og sårbarheder, nærvedhændelser, bevidstgørelsesinitiativer, uddannelse, øvelser og færdigheder, kapacitetsopbygning, standarder og tekniske specifikationer samt identifikation af væsentlige og vigtige enheder i medfør af artikel 2, stk. 2, litra b)-e)

d) at udveksle rådgivning og samarbejde med Kommissionen om nye politiske initiativer inden for cybersikkerhed og den overordnede sammenhæng mellem sektorspecifikke cybersikkerhedskrav

e) at udveksle rådgivning og samarbejde med Kommissionen om udkast til delegerede retsakter eller gennemførelsesretsakter vedtaget i henhold til dette direktiv

f) at udveksle bedste praksis og oplysninger med relevante EU-institutioner, -organer, -kontorer og –agenturer

g) at drøfte gennemførelsen af sektorspecifikke EU-retsakter, der indeholder bestemmelser om cybersikkerhed

h) hvor det er relevant, at drøfte rapporter om den i artikel 19, stk. 9, omhandlede peerevaluering og udarbejde konklusioner og henstillinger

i) at foretage koordinerede sikkerhedsrisikovurderinger af kritiske forsyningskæder i overensstemmelse med artikel 22, stk. 1

j) at drøfte tilfælde af gensidig bistand, herunder erfaringer fra og resultater af grænseoverskridende fælles tilsynstiltag som omhandlet i artikel 37

k) på anmodning af en eller flere berørte medlemsstater at drøfte specifikke anmodninger om gensidig bistand som omhandlet i artikel 37

l) at yde strategisk vejledning til CSIRT-netværket og EU–CyCLONe om specifikke nye spørgsmål

m) at drøfte politikken for opfølgende foranstaltninger efter omfattende cybersikkerhedshændelser og kriser på grundlag af erfaringer fra CSIRT-netværket og EU-CyCLONe

n) at bidrage til cybersikkerhedskapaciteter i hele Unionen ved at lette udvekslingen af nationale embedsmænd gennem et kapacitetsopbygningsprogram, der omfatter personale fra kompetente myndigheder eller CSIRT'erne

o) at tilrettelægge regelmæssige fælles møder med relevante private interessenter fra hele Unionen for at drøfte samarbejdsgruppens aktiviteter og indsamle input om nye politiske udfordringer

p) at drøfte det arbejde, der udføres i forbindelse med cybersikkerhedsøvelser, herunder det arbejder, der udføres af ENISA

q) at fastlægge metodologien og de organisatoriske aspekter af de peerevalueringer, der er omhandlet i artikel 19, stk. 1, samt at fastlægge selvevalueringsmetoden for medlemsstaterne i overensstemmelse med artikel 19, stk. 5, med bistand fra Kommissionen og ENISA samt, i samarbejde med Kommissionen og ENISA, at udvikle adfærdskodekser, der understøtter de udpegede cybersikkerhedseksperters arbejdsmetoder, i overensstemmelse med artikel 19, stk. 6

r) at udarbejde rapporter med henblik på den evaluering, der er omhandlet i artikel 40, om de erfaringer, der er indhøstet på strategisk plan og fra peerevalueringer

s) regelmæssigt at drøfte og foretage en vurdering af situationen med hensyn til cybertrusler eller hændelser såsom ransomware.

Samarbejdsgruppen forelægger de i første afsnit, litra r), omhandlede rapporter for Kommissionen, Europa-Parlamentet og Rådet.

5. Medlemsstaterne sikrer effektivt og sikkert samarbejde mellem deres repræsentanter i samarbejdsgruppen.

6. Samarbejdsgruppen kan anmode CSIRT-netværket om en teknisk rapport om udvalgte emner.

7. Senest den 1. februar 2024 og derefter hvert andet år udarbejder samarbejdsgruppen et arbejdsprogram vedrørende tiltag, der skal iværksættes for at gennemføre dens mål og opgaver.

8. Kommissionen kan vedtage gennemførelsesretsakter, hvori der fastlægges proceduremæssige ordninger, som er nødvendige for samarbejdsgruppens funktion.

Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 39, stk. 2.

Kommissionen udveksler rådgivning og samarbejder med samarbejdsgruppen om de udkast til gennemførelsesretsakter, der er omhandlet i dette stykkes første afsnit, i overensstemmelse med stk. 4, litra e).

9. Samarbejdsgruppen mødes regelmæssigt og i hvert fald mindst en gang om året med gruppen for kritiske enheders modstandsdygtighed, der er nedsat i henhold til direktiv (EU) 2022/2557, for at fremme og lette strategisk samarbejde og udvekslingen af oplysninger.

*Artikel 15*

**CSIRT-netværket**

1. Med henblik på at bidrage til skabelsen af tillid mellem medlemsstaterne og fremme hurtigt og effektivt operationelt samarbejde mellem medlemsstaterne oprettes der et netværk af nationale CSIRT'er.

2. CSIRT-netværket består af repræsentanter for de CSIRT'er, der er udpeget eller oprettet i henhold til artikel 10, og IT-Beredskabsenheden for Unionens institutioner, organer og agenturer (CERT-EU). Kommissionen deltager i CSIRT-netværket som observatør. ENISA varetager sekretariatsopgaverne og bistår aktivt samarbejdet mellem CSIRT'erne.

3. CSIRT-netværket har følgende opgaver:

a) at udveksle oplysninger om CSIRT'ernes kapaciteter

b) at lette deling, overførsel og udveksling af teknologi og relevante foranstaltninger, politikker, værktøjer, processer, bedste praksisser og rammer mellem CSIRT'erne

c) at udveksle relevant information om hændelser, nærvedhændelser, cybertrusler, risici og sårbarheder

d) at udveksle information vedrørende cybersikkerhedspublikationer og –anbefalinger

e) at sikre interoperabilitet med hensyn til specifikationer og protokoller for informationsdeling

f) på anmodning af et medlem af CSIRT-netværket, der potentielt er berørt af en hændelse, at udveksle og drøfte oplysninger i forbindelse med denne hændelse og tilknyttede cybertrusler, risici og sårbarheder

g) på anmodning af et medlem af CSIRT-netværket at drøfte og, hvor det er muligt, gennemføre en samordnet reaktion på en hændelse, som er identificeret inden for den pågældende medlemsstats jurisdiktion

h) at yde medlemsstaterne bistand til håndtering af grænseoverskridende hændelser i henhold til dette direktiv

i) at samarbejde, udveksle bedste praksis og yde bistand til de CSIRT'er, der er udpeget som koordinatorer i henhold til artikel 12, stk. 1, med hensyn til forvaltningen af den koordinerede offentliggørelse af sårbarheder, som vil kunne have en væsentlig indvirkning på enheder i mere end én medlemsstat

j) at drøfte og identificere yderligere former for operationelt samarbejde, herunder i forhold til:

i) kategorier af cybertrusler og hændelser

ii) tidlig varsling

iii) gensidig bistand

iv) principper og ordninger for koordination som reaktion på grænseoverskridende risici og hændelser

v) bidrag til den nationale beredskabsplan for omfattende cybersikkerhedshændelser og kriser, der er omhandlet i artikel 9, stk. 4, efter anmodning fra en medlemsstat

k) at oplyse samarbejdsgruppen om sine aktiviteter og om yderligere former for operationelt samarbejde, som drøftes i henhold til litra j), og, hvor det er nødvendigt, anmode om vejledning i forbindelse hermed

l) at gøre status over cybersikkerhedsøvelser, herunder dem, der organiseres af ENISA

m) på anmodning af en individuel CSIRT at drøfte denne CSIRT's kapaciteter og beredskab

n) at samarbejde og udveksle information med regionale og EU-dækkende sikkerhedsoperationscentre (SOC'er) for at forbedre den fælles situationsbevidsthed om hændelser og cybertrusler i hele Unionen

o) hvor det er relevant, at drøfte de i artikel 19, stk. 9, omhandlede peerevalueringsrapporter

p) at fastlægge retningslinjer for at lette konvergensen mellem operationel praksis med hensyn til anvendelsen af bestemmelserne i denne artikel vedrørende operationelt samarbejde.

4. Med henblik på den i artikel 40 omhandlede evaluering vurderer CSIRT-netværket senest den 17. januar 2025 og derefter hvert andet år de fremskridt, der er gjort med hensyn til det operationelle samarbejde, og udarbejde en rapport. Rapporten indeholder navnlig konklusioner og henstillinger baseret på resultaterne af de i artikel 19 omhandlede peerevalueringer, der foretages vedrørende de nationale CSIRT'er. Rapporten skal forelægges for samarbejdsgruppen.

5. CSIRT-netværket vedtager sin forretningsorden.

6. CSIRT-netværket og EU-CyCLONe aftaler proceduremæssige ordninger og samarbejder på grundlag heraf.

*Artikel 16*

**Det europæiske netværk af forbindelsesorganisationer for cyberkriser (EU-CyCLONe)**

1. EU-CyCLONe oprettes for at støtte den koordinerede forvaltning af omfattende cybersikkerhedshændelser og kriser på operationelt plan og for at sikre regelmæssig udveksling af relevant information mellem medlemsstaterne og EU-institutioner, -organer, -kontorer og -agenturer.

2. EU-CyCLONe består af repræsentanter for medlemsstaternes cyberkrisestyringsmyndigheder samt, i tilfælde hvor en potentiel eller igangværende omfattende cybersikkerhedshændelse har eller sandsynligvis vil have en be-

tydelig indvirkning på tjenester og aktiviteter, der er omfattet af dette direktivs anvendelsesområde, Kommissionen. I andre tilfælde deltager Kommissionen i EU-CyCLONe's aktiviteter som observatør.

ENISA varetager sekretariatsfunktionen for EU-CyCLONe og støtter sikker udveksling af oplysninger samt stiller de nødvendige værktøjer til rådighed for samarbejdet mellem medlemsstaterne med henblik på sikker udveksling af oplysninger.

EU-CyCLONe kan, hvor det er hensigtsmæssigt, indbyde repræsentanter for relevante interessenter til at deltage i dets arbejde som observatører.

3. EU-CyCLONe har følgende opgaver:

a) at øge beredskabsniveauet i forbindelse med håndtering af omfattende cybersikkerhedshændelser og kriser

b) at udvikle en fælles situationsbevidsthed om omfattende cybersikkerhedshændelser og kriser

c) at vurdere konsekvenserne og indvirkningen af relevante omfattende cybersikkerhedshændelser og kriser og foreslå mulige afbødende foranstaltninger

d) at koordinere håndteringen af omfattende cybersikkerhedshændelser og kriser og støtte beslutningstagningen på politisk plan i forbindelse med sådanne hændelser og kriser

e) på anmodning af en berørt medlemsstat at drøfte nationale beredskabsplaner for omfattende cybersikkerhedshændelser og kriser, der er omhandlet i artikel 9, stk. 4.

4. EU-CyCLONe vedtager sin forretningsorden.

5. EU-CyCLONe aflægger regelmæssigt rapport til samarbejdsgruppen om håndteringen af omfattende cybersikkerhedshændelser og kriser samt tendenser med særlig fokus på deres indvirkning på væsentlige og vigtige enheder.

6. EU-CyCLONe samarbejder med CSIRT-netværket på grundlag af aftalte proceduremæssige ordninger, jf. artikel 15, stk. 6.

7. Senest den 17. juli 2024 og derefter hver 18. måned forelægger EU-CyCLONe Europa-Parlamentet og Rådet en rapport med en vurdering af sit arbejde.

*Artikel 17*

**Internationalt samarbejde**

Unionen kan, hvor det er hensigtsmæssigt, i overensstemmelse med artikel 218 i TEUF indgå internationale aftaler med tredjelande eller internati-

onale organisationer, der giver mulighed for og tilrettelægger disses deltagelse i bestemte aktiviteter, der foretages af samarbejdsgruppen, CSIRT-netværket og EU-CyCLONe. Sådanne aftaler skal overholde EU-databeskyttelsesretten.

*Artikel 18*

**Rapport om cybersikkerhedssituationen i Unionen**

1. ENISA udarbejder i samarbejde med Kommissionen og samarbejdsgruppen hvert andet år en rapport om cybersikkerhedssituationen i Unionen, som fremsendes til og fremlægges for Europa-Parlamentet. Rapporten skal bl.a. gøres tilgængelig i et maskinlæsbart format og indeholde følgende:

a) en cybersikkerhedsrisikovurdering på EU-plan, der tager cybertrusselsbilledet i betragtning

b) en vurdering af udviklingen af cybersikkerhedskapaciteter i den offentlige og den private sektor i hele Unionen

c) en vurdering af det generelle niveau af cybersikkerhedsbevidsthed og cyberhygiejne hos borgere og enheder, herunder små og mellemstore virksomheder

d) en samlet vurdering af resultaterne af de peerevalueringer, der er omhandlet i artikel 19

e) en samlet vurdering af modenhedsniveauet for cybersikkerhedskapaciteter og -ressourcer i hele Unionen, herunder på sektorniveau, samt af i hvilket omfang medlemsstaternes nationale cybersikkerhedsstrategier er afstemt med hinanden.

2. Rapporten skal indeholde særlige politiske anbefalinger med henblik på at afhjælpe mangler og øge cybersikkerhedsniveauet i hele Unionen og et sammendrag af resultaterne for den pågældende periode fra de tekniske EU-cybersikkerhedsrapporter om hændelser og cybertrusler, som udarbejdes af ENISA i overensstemmelse med artikel 7, stk. 6, i forordning (EU) 2019/881.

3. ENISA udformer i samarbejde med Kommissionen, samarbejdsgruppen og CSIRT-netværket metodologien, herunder de relevante variabler, såsom kvantitative og kvalitative indikatorer, for den samlede vurdering, der er omhandlet i stk. 1, litra e).

*Artikel 19*

**Peerevalueringer**

1. Samarbejdsgruppen fastlægger senest den 17. januar 2025 med bistand fra Kommissionen og ENISA samt, hvor det er relevant, CSIRT-netværket metodologien og de organisatoriske aspekter af peerevalueringerne med

henblik på at lære af fælles erfaringer, styrke gensidig tillid, opnå et højt fælles cybersikkerhedsniveau samt styrke medlemsstaternes cybersikkerhedskapaciteter og -politikker, der er nødvendige for at gennemføre dette direktiv. Deltagelse i peerevalueringer er frivillig. Peerevalueringerne foretages af cybersikkerhedseksperter. Cybersikkerhedseksperterne udpeges af mindst to medlemsstater, som skal være forskellige fra den medlemsstat, der evalueres.

Peerevalueringerne skal mindst omfatte et af følgende aspekter:

a) gennemførelsesniveauet for de foranstaltninger til styring af cybersikkerhedsrisici og de rapporteringsforpligtelser, der er fastsat i artikel 21 og 23

b) kapacitetsniveauet, herunder de finansielle, tekniske og menneskelige ressourcer, der er til rådighed, og effektiviteten af de kompetente myndigheders varetagelse af deres opgaver

c) CSIRT'ernes operationelle kapacitet

d) gennemførelsesniveauet for den gensidige bistand, der er omhandlet i artikel 37

e) gennemførelsesniveauet for de ordninger for udveksling af cybersikkerhedsoplysninger, der er omhandlet i artikel 29

f) specifikke spørgsmål af grænseoverskridende eller tværsektoriel karakter.

2. Den i stk. 1 omhandlede metodologi skal omfatte objektive, ikkediskriminerende, retfærdige og gennemsigtige kriterier, på grundlag af hvilke medlemsstaterne udpeger cybersikkerhedseksperter, der kan udføre peerevalueringerne. Kommissionen og ENISA deltager som observatører i peerevalueringerne.

3. Medlemsstaterne kan udvælge specifikke spørgsmål som omhandlet i stk. 1, litra f), med henblik på en peerevaluering.

4. Forud for indledningen af en peerevaluering som omhandlet i stk. 1 underretter medlemsstater de deltagende medlemsstater om dens omfang, herunder de specifikke spørgsmål, der er udvalgt i medfør af stk. 3.

5. Forud for indledningen af peerevalueringen kan medlemsstaterne foretage en selvevaluering af de pågældende aspekter og stille denne selvevaluering til rådighed for de udpegede cybersikkerhedseksperter. Samarbejdsgruppen fastlægger med bistand fra Kommissionen og ENISA metoden for medlemsstaternes selvevaluering.

6. Peerevalueringer omfatter fysiske eller virtuelle besøg på stedet og ekstern udveksling af oplysninger. I overensstemmelse med princippet om godt samarbejde giver den medlemsstat, der er genstand for peerevalueringen, de udpegede cybersikkerhedseksperter de oplysninger, der er nødvendige for vurderingen, uden at det berører national ret eller EU-retten vedrørende beskyttelse af fortrolige eller klassificerede informationer og varetagelsen af

væsentlige statslige funktioner såsom den nationale sikkerhed. Samarbejdsgruppen udarbejder i samarbejde med Kommissionen og ENISA passende adfærdskodekser, der understøtter de udpegede cybersikkerhedseksperters arbejdsmetoder. Alle oplysninger, der indhentes ved peerevalueringen, må kun anvendes til dette formål. De cybersikkerhedseksperter, der deltager i peerevalueringen, må ikke videregive følsomme eller fortrolige oplysninger, som er indhentet som led i denne peerevaluering, til tredjemand.

7. Aspekter, der været genstand for en peerevaluering i en medlemsstat, må ikke underkastes en yderligere peerevaluering i den pågældende medlemsstat i to år efter afslutningen af peerevalueringen, medmindre medlemsstaten anmoder om andet, eller der aftales andet på forslag af samarbejdsgruppen.

8. Medlemsstaterne sikrer, at enhver risiko for interessekonflikter vedrørende de udpegede cybersikkerhedseksperter meddeles de øvrige medlemsstater, samarbejdsgruppen, Kommissionen og ENISA, inden peerevalueringen indledes. Den medlemsstat, der er genstand for peerevalueringen, kan gøre indsigelse mod udpegelsen af bestemte cybersikkerhedseksperter af behørigt begrundede årsager, som meddeles den udpegende medlemsstat.

9. Cybersikkerhedseksperter, der deltager i peerevalueringer, udarbejder rapporter om resultaterne og konklusionerne af peerevalueringerne. Medlemsstater, der er genstand for en peerevaluering, kan fremsætte bemærkninger til udkast til rapporter, der vedrører dem, og sådanne bemærkninger vedføjes rapporterne. Rapporterne skal indeholde anbefalinger, der kan gøre det muligt at forbedre de aspekter, peerevalueringen vedrører. Rapporterne forelægges for samarbejdsgruppen og CSIRT-netværket, hvor det er relevant. En medlemsstat, der er genstand for peerevalueringen, kan beslutte at gøre sin rapport, eller en redigeret udgave heraf, offentligt tilgængelig.

## KAPITEL IV

## FORANSTALTNINGER TIL STYRING AF CYBERSIKKERHEDSRISICI OG RAPPORTERINGSFORPLIGTELSER

*Artikel 20*

### Styring

1. 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.

Anvendelsen af dette stykke berører 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.

2. Medlemsstaterne sikrer, 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.

*Artikel 21*

**Foranstaltninger til styring af cybersikkerhedsrisici**

1. Medlemsstaterne sikrer, 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.

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

2. De i stk. 1 omhandlede foranstaltninger 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

j) brug af løsninger med multifaktorautentificering eller kontinuerlig autentificering, sikret tale-, video- og tekstkommunikation og sikrede nødkommunikationssystemer internt i enheden, hvor det er relevant.

3. Medlemsstaterne sikrer, at enhederne, når de overvejer, hvilke foranstaltninger omhandlet i denne artikels stk. 2, litra d), 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. Medlemsstaterne sikrer også, at enhederne, når de overvejer, hvilke foranstaltninger omhandlet i nævnte litra, 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.

4. Medlemsstaterne sikrer, at en enhed, der finder, at den ikke overholder foranstaltningerne i stk. 2, uden unødigt ophold træffer alle nødvendige, passende og forholdsmæssige korrigerende foranstaltninger.

5. Senest 17. oktober 2024 vedtager Kommissionen gennemførelsesretsakter, der fastsætter de tekniske og metodologiske krav til de foranstaltninger, der er omhandlet i stk. 2, 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.

Kommissionen kan vedtage gennemførelsesretsakter, der fastsætter de tekniske og metodologiske, samt om nødvendigt sektorspecifikke, krav til de i stk. 2 omhandlede foranstaltninger for så vidt angår andre væsentlige og vigtige enheder end dem, der er omhandlet i nærværende stykkes første afsnit.

Ved udarbejdelsen af de gennemførelsesretsakter, der er omhandlet i nærværende stykkes første og andet afsnit, følger Kommissionen i videst muligt omfang europæiske og internationale standarder samt relevante tekniske specifikationer. Kommissionen udveksler rådgivning og samarbejder med samarbejdsgruppen og ENISA om udkastene til gennemførelsesretsakter i overensstemmelse med artikel 14, stk. 4, litra e).

Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 39, stk. 2.

*Artikel 22*

**Koordinerede sikkerhedsrisikovurderinger af kritiske forsyningskæder på EU-plan**

1. Samarbejdsgruppen kan i samarbejde med Kommissionen og ENISA foretage koordinerede sikkerhedsrisikovurderinger af specifikke kritiske IKT-tjenester, -systemer eller -produktforsyningskæder under hensyntagen til tekniske og, hvor det er relevant, ikketekniske risikofaktorer.

2. Kommissionen identificerer efter høring af samarbejdsgruppen og ENISA og, hvor det er nødvendigt, relevante interessenter de specifikke kritiske IKT-tjenester, -systemer eller -produkter, der kan være genstand for den i stk. 1 omhandlede koordinerede sikkerhedsrisikovurdering.

*Artikel 23*

**Rapporteringsforpligtelser**

1. Hver medlemsstat sikrer, at væsentlige og vigtige enheder uden unødigt ophold underretter dens CSIRT eller i givet fald dens kompetente myndighed i overensstemmelse med stk. 4 om enhver hændelse, der har en væsentlig indvirkning på leveringen af deres tjenester som omhandlet i stk. 3 (væsentlig hændelse). Hvor det er relevant, underretter de pågældende enheder uden unødigt ophold modtagerne af deres tjenester om væsentlige hændelser, der sandsynligvis vil påvirke leveringen af disse tjenester negativt. Hver medlemsstat sikrer, at disse enheder indberetter bl.a. alle oplysninger, der gør det muligt for CSIRT'en, eller i givet fald den kompetente myndighed, at fastslå eventuelle grænseoverskridende virkninger af hændelsen. Underretningen i sig selv medfører ikke et øget ansvar for den underrettende enhed.

Hvor de berørte enheder underretter den kompetente myndighed om en væsentlig hændelse i henhold til første afsnit, sikrer medlemsstaten, at den pågældende kompetente myndighed videresender underretningen til CSIRT'en på tidspunktet for modtagelsen.

I tilfælde af en grænseoverskridende eller tværsektoriel væsentlig hændelse sikrer medlemsstaterne, at deres centrale kontaktpunkter rettidigt forsynes med relevante oplysninger, som der er givet underretning om i overensstemmelse med stk. 4.

2. I givet fald sikrer medlemsstaterne, at væsentlige og vigtige enheder uden unødigt ophold meddeler modtagerne af deres tjenester, som potentielt er berørt af en væsentlig cybertrussel, eventuelle foranstaltninger eller mod-

forholdsregler, 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 cybertrussel.

3. En hændelse anses for at være væsentlig, hvis:

a) den har forårsaget eller er i stand til at forårsage alvorlige driftsforstyrrelser af tjenesterne eller økonomiske tab for den berørte enhed

b) den har påvirket eller er i stand til at påvirke andre fysiske eller juridiske personer ved at forårsage betydelig materiel eller immateriel skade.

4. Medlemsstaterne sikrer, at de berørte enheder med henblik på den i 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 i givet fald 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

   iv) i givet fald de grænseoverskridende virkninger af hændelsen.

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.

Uanset første afsnit, litra b), skal tillidstjenesteudbyderen for så vidt angår væsentlige hændelser, der har en virkning på leveringen af dens tillidstjenester, 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.

5. CSIRT'en eller den kompetente myndighed giver uden unødigt ophold og, hvor det er muligt, inden for 24 timer efter modtagelsen af den i stk. 4, litra a), omhandlede tidlige varsling 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. Hvor CSIRT'en ikke er den oprindelige modtager af den i stk. 1 omhandlede underretning, gives vejledningen af den kompetente myndighed i samarbejde med CSIRT'en. 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.

6. Hvor det er relevant, og navnlig hvor den væsentlige 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 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.

7. Hvor offentlighedens kendskab er nødvendig for at forebygge en væsentlig hændelse eller for at håndtere en igangværende væsentlig 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.

8. På CSIRT'ens eller den kompetente myndigheds anmodning videresender det centrale kontaktpunkt de underretninger, der er modtaget i henhold til stk. 1, til de centrale kontaktpunkter i andre berørte medlemsstater.

9. Det centrale kontaktpunkt forelægger en gang hver tredje måned en sammenfattende rapport for ENISA, herunder anonymiserede og aggregerede data om væsentlige hændelser, hændelser, cybertrusler og nærvedhændelser, der er indberettet i overensstemmelse med denne artikels stk. 1 og med artikel 30. For at bidrage til tilvejebringelsen af sammenlignelige oplysninger kan ENISA vedtage teknisk vejledning om parametrene for de oplysninger, der skal inkluderes i den sammenfattende rapport. ENISA underretter

samarbejdsgruppen og CSIRT-netværket om sine resultater vedrørende modtagne underretninger hver sjette måned.

10. CSIRT'erne eller i givet fald de kompetente myndigheder giver de kompetente myndigheder i henhold til direktiv (EU) 2022/2557, oplysninger om væsentlige hændelser, hændelser, cybertrusler og nærvedhændelser, der er indberettet i overensstemmelse med denne artikels stk. 1 og med artikel 30 af enheder, der er identificeret som kritiske enheder i henhold til direktiv (EU) 2022/2557.

11. Kommissionen kan vedtage gennemførelsesretsakter, der yderligere præciserer typen af oplysninger, formatet og proceduren for en underretning indgivet i henhold til denne artikels stk. 1 og til artikel 30 og for en meddelelse, der er indgivet i henhold til nærværende artikels stk. 2.

Senest den 17. oktober 2024 vedtager Kommissionen for så vidt angår 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 gennemførelsesretsakter, der yderligere præciserer de tilfælde, hvor en hændelse anses for at være væsentlig som omhandlet i stk. 3. Kommissionen kan vedtage sådanne gennemførelsesretsakter for så vidt angår andre væsentlige og vigtige enheder.

Kommissionen udveksler rådgivning og samarbejder med samarbejdsgruppen om de udkast til gennemførelsesretsakter, der er omhandlet i dette stykkes første og andet afsnit, i overensstemmelse med artikel 14, stk. 4, litra e).

Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 39, stk. 2.

*Artikel 24*

**Brug af europæiske cybersikkerhedscertificeringsordninger**

1. For at påvise overensstemmelse med bestemte krav i artikel 21 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 cybersikkerhedscertificeringsordning, der er vedtaget i henhold til artikel 49 i forordning (EU) 2019/881. Endvidere skal medlemsstaterne tilskynde væsentlige og vigtige enheder til at anvende kvalificerede tillidstjenester.

2. Kommissionen tillægges beføjelser til at vedtage delegerede retsakter i overensstemmelse med artikel 38 for at supplere dette direktiv 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 forordning (EU) 2019/881. Disse delegerede retsakter vedtages, når der er identificeret utilstrækkelige cybersikkerhedsniveauer, og skal indeholde en gennemførelsesperiode.

Inden vedtagelsen af sådanne delegerede retsakter foretager Kommissionen en konsekvensanalyse og gennemfører høringer i overensstemmelse med artikel 56 i forordning (EU) 2019/881.

3. I tilfælde, hvor der ikke findes en passende europæisk cybersikkerhedscertificeringsordning for så vidt angår denne artikels stk. 2, kan Kommissionen efter høring af samarbejdsgruppen og Den Europæiske Cybersikkerhedscertificeringsgruppe anmode ENISA om at udarbejde et forslag til ordning i henhold til artikel 48, stk. 2, i forordning (EU) 2019/881.

*Artikel 25*

**Standardisering**

1. 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.

2. ENISA udarbejder i samarbejde med medlemsstaterne og, hvor det er relevant, efter høring af relevante interessenter vejledning og retningslinjer om de tekniske områder, der skal overvejes vedrørende stk. 1, samt om allerede eksisterende standarder, herunder nationale standarder, som vil give mulighed for at dække disse områder.

## KAPITEL V
## JURISDIKTION OG REGISTRERING

*Artikel 26*

**Jurisdiktion og territorialitet**

1. Enheder, der er omfattet af dette direktivs anvendelsesområde, anses for at henhøre under jurisdiktionen i den medlemsstat, hvor de er etableret, med undtagelse af:

a) udbydere af offentlige elektroniske kommunikationsnet eller af offentligt tilgængelige elektroniske kommunikationstjenester, som anses for at henhøre under jurisdiktionen i den medlemsstat, hvor de leverer deres tjenester

b) 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, som anses for at henhøre under jurisdiktionen i den medlemsstat, hvor de har deres hovedforretningssted i Unionen i henhold til stk. 2

c) offentlige forvaltningsenheder, som anses for at henhøre under jurisdiktionen i den medlemsstat, der har oprettet dem.

2. Med henblik på dette direktiv anses en enhed som omhandlet i stk. 1, litra b), for at have sit hovedforretningssted i Unionen 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. 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 Unionen er beliggende.

3. Hvis en enhed som omhandlet i stk. 1, litra b), ikke er etableret i Unionen, men udbyder tjenester inden for Unionen, skal den udpege en repræsentant i Unionen. Repræsentanten skal være etableret i en af de medlemsstater, hvor tjenesterne tilbydes. En sådan enhed anses for at høre under den medlemsstats jurisdiktion, hvor repræsentanten er etableret. Hvis der ikke findes en repræsentant i Unionen, der er udpeget i henhold til dette stykke, kan enhver medlemsstat, hvor enheden leverer tjenester, tage retlige skridt mod enheden for overtrædelse af dette direktiv.

4. Det forhold, at en enhed som omhandlet i stk. 1, litra b), har udpeget en repræsentant, forhindrer ikke, at der kan tages retlige skridt mod enheden selv.

5. Medlemsstater, der har modtaget en anmodning om gensidig bistand vedrørende en enhed som omhandlet i stk. 1, litra b), kan inden for rammerne af denne anmodning træffe passende tilsyns- og håndhævelsesforanstaltninger over for den pågældende enhed, der leverer tjenester eller har et net- og informationssystem på deres område.

*Artikel 27*

**Register over enheder**

1. ENISA opretter og fører et register over DNS-tjenesteudbydere, topdomænenavneadministratorer, enheder, der leverer domænenavnsregistre-

ringstjenester, og udbydere af cloudcomputingtjenester, af datacentertjenester, af indholdsleveringsnetværk, af administrerede tjenester, af administrerede sikkerhedstjenester, af onlinemarkedspladser, af onlinesøgemaskiner og af platforme for sociale netværkstjenester på grundlag af de oplysninger, der modtages fra det centrale kontaktpunkt i overensstemmelse med stk. 4. Efter anmodning giver ENISA de kompetente myndigheder adgang til dette register, idet det i givet fald sikrer de nødvendige garantier til at beskytte fortroligheden af oplysninger.

2. Medlemsstaterne pålægger de i stk. 1, omhandlede enheder at indgive følgende oplysninger til de kompetente myndigheder senest den 17. januar 2025:

a) enhedens navn

b) den relevante sektor og delsektor og typen af enhed, som i givet fald er omhandlet i 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 artikel 26, stk. 3

d) ajourførte kontaktoplysninger, herunder e-mailadresser og telefonnumre på enheden og i givet fald dens repræsentant udpeget i henhold til artikel 26, stk. 3

e) de medlemsstater, hvor enheden leverer tjenester og

f) enhedens IP-intervaller.

3. Medlemsstaterne sikrer, at de i stk. 1 omhandlede 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 stk. 2.

4. Efter modtagelsen af oplysningerne omhandlet i stk. 2 og 3, med undtagelse af oplysningerne omhandlet i stk. 2, litra f), videresender den berørte medlemsstats centrale kontaktpunkt dem, til ENISA uden unødigt ophold.

5. De i denne artikels stk. 2 og 3 omhandlede oplysninger fremsendes i givet fald via den nationale mekanisme, der er omhandlet i artikel 3, stk. 4, fjerde afsnit.

*Artikel 28*

**Database over domænenavnsregistreringsdata**

1. Med henblik på at bidrage til DNS' sikkerhed, stabilitet og modstandsdygtighed pålægger medlemsstaterne topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester, 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.

2. Med henblik på stk. 1 stiller medlemsstaterne krav om, at databasen over domænenavnsregistreringsdata indeholder de fornødne oplysninger til at identificere og kontakte indehaverne af domænenavne og de kontaktpunkter, der forvalter domænenavne under topdomæner. Sådanne oplysninger omfatter:

a) Domænenavnet

b) Registreringsdatoen

c) registrantens navn, kontakt-e-mailadresse og telefonnummer

d) kontakt-e-mailadresse og telefonnummer på det kontaktpunkt, der administrerer domænenavnet, i det tilfælde at de er forskellige fra registrantens.

3. 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 stk. 1 omhandlede databaser indeholder nøjagtige og fuldstændige oplysninger. Medlemsstaterne kræver, at sådanne politikker og procedurer gøres offentligt tilgængelige.

4. 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.

5. 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.

6. Overholdelse af de forpligtelser, der er fastsat i stk. 1-5, må ikke føre til en gentagelse af indsamlingen af domænenavnsregistreringsdata. Med henblik herpå pålægger medlemsstaterne topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester, at samarbejde med hinanden.

## KAPITEL VI
## UDVEKSLING AF OPLYSNINGER

*Artikel 29*

### Ordninger for udveksling af cybersikkerhedsoplysninger

1. Medlemsstaterne sikrer, at enheder, der er omfattet af dette direktivs anvendelsesområde, og, hvor det er relevant, andre enheder, der ikke er omfattet af dette direktivs 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

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.

2. Medlemsstaterne sikrer, 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.

3. Medlemsstaterne fremmer etableringen af ordninger for udveksling af cybersikkerhedsoplysninger, der er omhandlet i denne artikels stk. 2. Sådanne ordninger kan specificere operationelle elementer, herunder brugen af særlige IKT-platforme og automatiseringsværktøjer, i, indholdet af og betingelserne for ordningerne for udveksling af oplysninger. Ved fastlæggelsen af de nærmere bestemmelser om inddragelse af offentlige myndigheder i sådanne ordninger kan medlemsstaterne indføre betingelser for de oplysninger, som de kompetente myndigheder eller CSIRT'erne stiller til rådighed. Medlemsstaterne yder bistand til anvendelsen af sådanne ordninger i overensstemmelse med deres politikker, der er omhandlet i artikel 7, stk. 2, litra h).

4. Medlemsstaterne sikrer, at væsentlige og vigtige enheder underretter de kompetente myndigheder om deres deltagelse i de i stk. 2 omhandlede ord-

ninger for udveksling af cybersikkerhedsoplysninger, når de indtræder i sådanne ordninger, eller, i givet faldt, om deres udtræden af sådanne ordninger, når denne udtræden træder i kraft.

5. ENISA yder bistand til oprettelsen af ordninger for udveksling af cybersikkerhedsoplysninger, der er omhandlet i stk. 2, ved at udveksle bedste praksis og give vejledning.

*Artikel 30*

**Frivillig meddelelse af relevante oplysninger**

1. Medlemsstaterne sikrer, at der, i tilgift til underretningsforpligtelsen i medfør af artikel 23 kan indgives underretninger til CSIRT'er eller i givet fald til de kompetente myndigheder på frivillig basis af:

a) væsentlige og vigtige enheder for så vidt angår hændelser, cybertrusler og nærvedhændelser

b) enheder, udover dem der omhandlet i litra a), uanset om de er omfattet af dette direktivs anvendelsesområde, for så vidt angår væsentlige hændelser, cybertrusler og nærvedhændelser.

2. Medlemsstaterne behandler de i denne artikels 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.

## KAPITEL VII
## TILSYN OG HÅNDHÆVELSE

*Artikel 31*

**Generelle aspekter vedrørende tilsyn og håndhævelse**

1. Medlemsstaterne sikrer, at deres kompetente myndigheder effektivt overvåger og træffer de nødvendige foranstaltninger til at sikre, at dette direktiv overholdes.

2. 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.

3. De kompetente myndigheder arbejder tæt sammen med tilsynsmyndigheder i henhold til forordning (EU) 2016/679, når de håndterer hændelser, der medfører brud på persondatasikkerheden, uden at det berører de kompetencer og opgaver, som tilsynsmyndighederne har i henhold til nævnte forordning.

4. 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.

*Artikel 32*

**Tilsyns- og håndhævelsesforanstaltninger vedrørende væsentlige enheder**

1. Medlemsstaterne sikrer, at de tilsyns- eller håndhævelsesforanstaltninger, der pålægges væsentlige enheder for så vidt angår forpligtelserne fastsat i dette direktiv er effektive, står i rimeligt forhold til overtrædelsen og har afskrækkende virkning under hensyntagen til omstændighederne i hver enkelt sag.

2. Medlemsstaterne sikrer, at de kompetente myndigheder, når de udfører deres tilsynsopgaver vedrørende væsentlige enheder, som minimum har beføjelse til at pålægge disse enheder:

a) kontrol på stedet og eksternt tilsyn, herunder stikprøvekontrol, som skal udføres af uddannede fagfolk

b) regelmæssige og målrettede sikkerhedsaudits udført af et kvalificeret uafhængigt organ eller en kompetent myndighed

c) ad hoc-audits, herunder hvor det er berettiget på grund af en væsentlig hændelse eller en overtrædelse af dette direktiv fra den væsentlige enheds side

d) sikkerhedsscanninger baseret på objektive, ikkediskriminerende, fair og gennemsigtige risikovurderingskriterier, hvor det er nødvendigt i samarbejde med den berørte enhed

e) anmodninger om oplysninger, der er nødvendige for at vurdere de foranstaltninger til styring af cybersikkerhedsrisici, som den berørte enhed har indført, herunder dokumenterede cybersikkerhedspolitikker, samt overholdelse af forpligtelsen til at indgive oplysninger til de kompetente myndigheder i henhold til artikel 27

f) anmodninger om adgang til data, dokumenter og oplysninger, der er nødvendige for udførelsen af deres tilsynsopgaver

g) anmodninger om dokumentation for gennemførelsen af cybersikkerhedspolitikker såsom resultaterne af sikkerhedsaudits udført af en kvalificeret revisor og den respektive underliggende dokumentation.

De målrettede sikkerhedsaudits, der er omhandlet i første afsnit, litra b), baseres 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.

3. Ved udøvelsen af deres beføjelser i henhold til stk. 2, litra e), f) eller g), angiver de kompetente myndigheder formålet med anmodningen og præciserer, hvilke oplysninger der anmodes om.

4. Medlemsstaterne sikrer, at deres kompetente myndigheder, når de udøver deres håndhævelsesbeføjelser over for væsentlige enheder, som mindst har beføjelse til at:

a) udstede advarsler om de pågældende enheders overtrædelser af dette direktiv

b) 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 dette direktiv

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

g) udpege en overvågningsansvarlig med veldefinerede opgaver til i en nærmere fastsat periode at føre tilsyn med de pågældende enheders overholdelse af artikel 21 og 23

h) pålægge de pågældende enheder at offentliggøre aspekter af overtrædelser af dette direktiv på en nærmere angivet måde

i) 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 dette stykkes litra a)-h).

5. Hvor håndhævelsesforanstaltninger vedtaget i henhold til stk. 4, litra a)-d) og f), er virkningsløse, sikrer medlemsstaterne, at deres kompetente myndigheder har beføjelse til at fastsætte en frist, inden for hvilken den væsentlige enhed anmodes om at tage de nødvendige tiltag for at afhjælpe manglerne eller opfylde disse myndigheders krav. Hvis de ønskede tiltag ikke tages inden for den fastsatte frist, sikrer medlemsstaterne, at de kompetente myndigheder har 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

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.

Midlertidige suspensioner eller forbud, som er pålagt i henhold til dette stykke, anvendes kun, indtil den pågældende enhed træffer de nødvendige foranstaltninger til at afhjælpe manglerne eller opfylde den kompetente myndighed krav, som gav anledning til, at disse håndhævelsesforanstaltninger blev anvendt. Pålæggelse af sådanne 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.

Håndhævelsesforanstaltningerne i dette stykke finder ikke anvendelse på offentlige forvaltningsenheder, der er omfattet af dette direktiv.

6. Medlemsstaterne sikrer, at enhver fysisk person, der er ansvarlig for eller optræder som juridisk repræsentant for en væsentlig enhed på grundlag af beføjelsen til at repræsentere den, beføjelsen til at træffe afgørelser på dennes vegne eller beføjelsen til at udøve kontrol over den, har beføjelse til at sikre, at den overholder dette direktiv. Medlemsstaterne sikrer, at det er muligt at drage sådanne fysiske personer til ansvar for tilsidesættelse af deres forpligtelser til at sikre overholdelse af dette direktiv.

Med hensyn til offentlige forvaltningsenheder berører dette stykke ikke national ret for så vidt angår ansvaret for embedsmænd og personer valgt eller udnævnt til offentlige hverv.

7. Når de kompetente myndigheder træffer håndhævelsesforanstaltninger omhandlet i stk. 4 eller 5, skal de overholde retten til forsvar og tage hensyn til omstændighederne i hver enkelt sag og som minimum tage behørigt hensyn til:

a) overtrædelsens grovhed og vigtigheden af de overtrådte bestemmelser, idet bl.a. følgende under alle omstændigheder skal betragtes som alvorlige overtrædelser:

   i) gentagne overtrædelser

   ii) manglende underretning om eller afhjælpning af væsentlige hændelser

   iii) manglende afhjælpning af mangler efter bindende instrukser fra kompetente myndigheder

   iv) hindringer for audits eller overvågningsaktiviteter beordret af den kompetente myndighed efter konstatering af en overtrædelse

   v) afgivelse af urigtige eller klart unøjagtige oplysninger vedrørende cybersikkerhedsrisikostyringsforanstaltninger eller rapporteringsforpligtelser, der er fastsat i artikel 21 og 23

b) overtrædelsens varighed

c) den pågældende enheds relevante tidligere overtrædelser

d) 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

e) hvorvidt gerningsmanden har begået overtrædelsen forsætligt eller uagtsomt

f) enhver foranstaltning truffet af enheden for at forebygge eller afbøde den materielle eller immaterielle skade

g) hvorvidt godkendte adfærdskodekser eller godkendte certificeringsmekanismer er overholdt

h) i hvilken udstrækning de fysiske eller juridiske personer, der holdes ansvarlige, samarbejder med de kompetente myndigheder.

8. De kompetente myndigheder giver en detaljeret begrundelse for deres håndhævelsesforanstaltninger. Inden de kompetente myndigheder træffer sådanne foranstaltninger, underretter 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.

9. Medlemsstaterne sikrer, at deres kompetente myndigheder i henhold til dette direktiv underretter de relevante kompetente myndigheder i samme medlemsstat i henhold til direktiv (EU) 2022/2557, når de udøver deres tilsyns- og håndhævelsesbeføjelser med det formål at sikre, at en enhed, der er identificeret som en kritisk enhed i henhold til direktiv (EU) 2022/2557, overholder nærværende direktiv. Hvor det er relevant, kan de kompetente myndigheder i henhold til direktiv (EU) 2022/2557 anmode de kompetente myndigheder i henhold til nærværende direktiv om at udøve deres tilsyns- og håndhævelsesbeføjelser med hensyn til en enhed, som er identificeret som en kritisk enhed i henhold til direktiv (EU) 2022/2557.

10. Medlemsstaterne sikrer, at deres kompetente myndigheder i henhold til dette direktiv samarbejder med de relevante kompetente myndigheder i den berørte medlemsstat i henhold til forordning (EU) 2022/2554. Medlemsstaterne sikrer navnlig, at deres kompetente myndigheder i henhold til nærværende direktiv underretter tilsynsforummet oprettet i henhold til artikel 32, stk. 1, i forordning (EU) 2022/2554, når de udøver deres tilsyns- og håndhævelsesbeføjelser med det formål at sikre, at en væsentlig enhed, der er udpeget som en kritisk tredjepartsudbyder af IKT-tjenester i henhold til artikel 31, i forordning (EU) 2022/2554, overholder nærværende direktiv.

*Artikel 33*

**Tilsyns- og håndhævelsesforanstaltninger vedrørende vigtige enheder**

1. 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.

2. Medlemsstaterne sikrer, at de kompetente myndigheder, når de udfører deres tilsynsopgaver vedrørende vigtige enheder, som minimum har beføjelse til at pålægge disse enheder:

a) kontrol på stedet og eksternt efterfølgende tilsyn udført af uddannede fagfolk

b) målrettede sikkerhedsaudits udført af et kvalificeret uafhængigt organ eller en kompetent myndighed

c) sikkerhedsscanninger baseret på objektive, ikkediskriminerende, fair og gennemsigtige risikovurderingskriterier, hvor det er nødvendigt i samarbejde med den berørte enhed

d) anmodninger om oplysninger, der er nødvendige for efterfølgende at vurdere de foranstaltninger til styring af cybersikkerhedsrisici, som den berørte enhed har indført, herunder dokumenterede cybersikkerhedspolitikker, samt overholdelse af forpligtelsen til at indgive oplysninger til de kompetente myndigheder i henhold til artikel 27

e) anmodninger om adgang til data, dokumenter og oplysninger, der er nødvendige for udførelsen af deres tilsynsopgaverne

f) anmodninger om dokumentation for gennemførelsen af cybersikkerhedspolitikker såsom resultaterne af sikkerhedsaudits udført af en kvalificeret revisor og den respektive underliggende dokumentation.

De målrettede sikkerhedsaudits, der er omhandlet i første afsnit, litra b), baseres 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.

3. Ved udøvelsen af deres beføjelser i henhold til stk. 2, litra d), e) eller f), angiver de kompetente myndigheder formålet med anmodningen og præciserer, hvilke oplysninger der anmodes om.

4. Medlemsstaterne sikrer, at de 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 dette direktiv

b) udstede bindende instrukser eller pålægge de pågældende enheder at afhjælpe de konstaterede mangler eller overtrædelserne af dette direktiv

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

g) pålægge de pågældende enheder at offentliggøre aspekter af overtrædelser af dette direktiv på en nærmere angivet måde

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 dette stykkes litra a)-g).

5. Artikel 32, stk. 6, 7 og 8, finder tilsvarende anvendelse på tilsyns- og håndhævelsesforanstaltningerne i denne artikel for vigtige enheder.

6. Medlemsstaterne sikrer, at deres kompetente myndigheder i henhold til dette direktiv samarbejder med de relevante kompetente myndigheder i den berørte medlemsstat i henhold til forordning (EU) 2022/2554. Medlemsstaterne sikrer navnlig, at deres kompetente myndigheder i henhold til nærværende direktiv underretter tilsynsforummet oprettet i henhold til artikel 32, stk. 1, i forordning (EU) 2022/2554, når de udøver deres tilsyns- og håndhævelsesbeføjelser med det formål at sikre, at en vigtig enhed, der er udpeget som en kritisk tredjepartsudbyder af IKT-tjenester i henhold til artikel 31, i forordning (EU) 2022/2554, overholder nærværende direktiv.

*Artikel 34*

**Generelle betingelser for pålæggelse af administrative bøder til væsentlige og vigtige enheder**

1. Medlemsstaterne sikrer, at de administrative bøder, der pålægges væsentlige og vigtige enheder i henhold til denne artikel for så vidt angår overtrædelser af dette direktiv, er effektive, står i rimeligt forhold til overtrædelsen og har afskrækkende virkning, under hensyntagen til omstændighederne i hver enkelt sag.

2. 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).

3. Når det besluttes, om der skal pålægges en administrativ bøde, og der træffes afgørelse om dens størrelse i hver enkelt sag, tages der som minimum behørigt hensyn til de i artikel 32, stk. 7, angivne elementer.

4. Medlemsstaterne sikrer, at hvor væsentlige enheder overtræder artikel 21 eller 23, straffes de i overensstemmelse med nærværende artikels stk. 2 og 3 med administrative bøder med et maksimum på mindst 10 000 000 EUR eller et maksimum på mindst 2 % af den samlede globale årsomsætning i det foregående regnskabsår i den virksomhed, som den væsentlige enhed tilhører, alt efter hvad der er højest.

5. Medlemsstaterne sikrer, at hvor vigtige enheder overtræder artikel 21 eller 23, straffes de i overensstemmelse med nærværende artikels stk. 2 og 3 med administrative bøder med et maksimum på mindst 7 000 000 EUR eller et maksimum på mindst 1,4 % af den samlede globale årsomsætning i det foregående regnskabsår i den virksomhed, som den vigtige enhed tilhører, alt efter hvad der er højest.

6. Medlemsstaterne kan fastsætte beføjelser til at pålægge tvangsbøder for at tvinge en væsentlig eller vigtig enhed til at bringe en overtrædelse af dette direktiv til ophør i overensstemmelse med en forudgående afgørelse truffet af den kompetente myndighed.

7. Uden at det berører tilsynsmyndighedernes beføjelser i henhold til artikel 32 og 33, kan hver enkelt medlemsstat fastsætte regler om, hvorvidt og i hvilket omfang administrative bøder kan pålægges offentlige forvaltningsorganer.

8. Hvis en medlemsstats retssystem ikke giver mulighed for at pålægge administrative bøder, sørger den pågældende medlemsstat for, at denne artikel 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. Medlemsstaten giver Kommissionen meddelelse om bestemmelserne i de love, som den vedtager i henhold til dette stykke, senest den 17. oktober 2024 og underretter den straks om eventuelle senere ændringslove eller ændringer, der berører dem.

*Artikel 35*

**Overtrædelser, der medfører brud på persondatasikkerheden**

1. Hvor de kompetente myndigheder i forbindelse med tilsyn eller håndhævelse bliver opmærksomme på, at en væsentlig eller vigtig enheds overtrædelse af forpligtelserne i dette direktivs artikel 21 og 23 kan medføre et

brud på persondatasikkerheden som defineret i artikel 4, nr. 12), i forordning (EU) 2016/679, som skal anmeldes i henhold til nævnte forordnings artikel 33, underretter de uden unødigt ophold tilsynsmyndigheder som omhandlet i nævnte forordnings artikel 55 eller 56.

2. Hvor tilsynsmyndighederne som omhandlet i artikel 55 eller 56 i forordning (EU) 2016/679 pålægger en administrativ bøde i henhold til nævnte forordnings artikel 58, stk. 2, litra i), må de kompetente myndigheder ikke pålægge en administrativ bøde i henhold til dette direktivs artikel 34 for en i nærværende artikels stk. 1 omhandlet overtrædelse, der skyldes den samme adfærd som den, der var genstand for den administrative bøde i henhold til artikel 58, stk. 2, litra i), i forordning (EU) 2016/679. De kompetente myndigheder kan dog anvende de håndhævelsesforanstaltninger eller pålægge de sanktioner, der er omhandlet i dette direktivs artikel 32, stk. 4, litra a)-h), artikel 32, stk. 5, og artikel 33, stk. 4, litra a)-g).

3. Hvor den tilsynsmyndighed, der er kompetent i henhold til forordning (EU) 2016/679, er etableret i en anden medlemsstat end den kompetente myndighed, underretter den kompetente myndighed tilsynsmyndigheden, der er etableret i sin egen medlemsstat, om det i stk. 1 omhandlede potentielle brud på persondatasikkerheden.

*Artikel 36*

**Sanktioner**

Medlemsstaterne fastsætter regler om sanktioner, der skal anvendes i tilfælde af overtrædelser af de nationale foranstaltninger, der er vedtaget i medfør af dette direktiv, og træffer alle nødvendige foranstaltninger for at sikre, at de gennemføres. Sanktionerne skal være effektive, stå i et rimeligt forhold til overtrædelsen og have afskrækkende virkning. Medlemsstaterne giver senest den 17. januar 2025 Kommissionen meddelelse om disse regler og foranstaltninger og underretter den straks om alle senere ændringer, der berører dem.

*Artikel 37*

**Gensidig bistand**

1. 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 bistå hinanden efter behov. Dette samarbejde indebærer mindst, at:

a) 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) en kompetent myndighed kan anmode en anden kompetent myndighed om at træffe tilsyns- eller håndhævelsesforanstaltninger

c) 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.

Den gensidige bistand, der er omhandlet i første afsnit, litra c), kan omfatte anmodninger om oplysninger og tilsynsforanstaltninger, herunder anmodninger om at foretage inspektioner på stedet eller eksternt tilsyn eller målrettede sikkerhedskontroller. En kompetent myndighed, som en anmodning om bistand er rettet til, må ikke afvise anmodningen, medmindre det er fastslået, at den ikke er kompetent til at yde den ønskede bistand, at den bistand, der anmodes om, ikke står i et rimeligt forhold til den kompetente myndigheds tilsynsopgaver, eller anmodningen vedrører oplysninger eller indebærer aktiviteter, som, hvis de blev videregivet eller udført, ville stride mod den medlemsstats væsentlige interesser med hensyn til national sikkerhed, offentlige sikkerhed eller forsvar. Før den kompetente myndighed afslår en sådan anmodning, hører den de øvrige berørte kompetente myndigheder samt, efter anmodning fra en af de berørte medlemsstater, Kommissionen og ENISA.

2. Hvor det er hensigtsmæssigt og efter fælles overenskomst, kan de kompetente myndigheder fra forskellige medlemsstater gennemføre fælles tilsynstiltag.

## KAPITEL VIII

## DELEGEREDE RETSAKTER OG GENNEMFØRELSESRETSAKTER

*Artikel 38*

### Udøvelse af de delegerede beføjelser

1. Beføjelsen til at vedtage delegerede retsakter tillægges Kommissionen på de i denne artikel fastsatte betingelser.

2. Beføjelsen til at vedtage delegerede retsakter, jf. artikel 24, stk. 2, tillægges Kommissionen for en periode på fem år fra den 16. januar 2023.

3. Den i artikel 24, stk. 2, omhandlede delegation af beføjelser kan til enhver tid tilbagekaldes af Europa-Parlamentet eller Rådet. En afgørelse om tilbagekaldelse bringer delegationen af de beføjelser, der er angivet i den pågældende afgørelse, til ophør. Den får virkning dagen efter offentliggørelsen af afgørelsen i *Den Europæiske Unions Tidende* eller på et senere

tidspunkt, der angives i afgørelsen. Den berører ikke gyldigheden af delegerede retsakter, der allerede er i kraft.

4. Inden vedtagelse af en delegeret retsakt hører Kommissionen eksperter, som er udpeget af hver enkelt medlemsstat, i overensstemmelse med principperne i den interinstitutionelle aftale af 13. april 2016 om bedre lovgivning.

5. Så snart Kommissionen vedtager en delegeret retsakt, giver den samtidigt Europa-Parlamentet og Rådet meddelelse herom.

6. En delegeret retsakt vedtaget i henhold til artikel 24, stk. 2, træder kun i kraft, hvis hverken Europa-Parlamentet eller Rådet har gjort indsigelse inden for en frist på to måneder fra meddelelsen af den pågældende retsakt til Europa-Parlamentet og Rådet, eller hvis Europa-Parlamentet og Rådet inden udløbet af denne frist begge har informeret Kommissionen om, at de ikke agter at gøre indsigelse. Fristen forlænges med to måneder på Europa-Parlamentets eller Rådets initiativ.

*Artikel 39*

**Udvalgsprocedure**

1. Kommissionen bistås af et udvalg. Dette udvalg er et udvalg som omhandlet i forordning (EU) nr. 182/2011.

2. Når der henvises til dette stykke, finder artikel 5 i forordning (EU) nr. 182/2011 anvendelse.

3. Når udvalgets udtalelse indhentes efter en skriftlig procedure, afsluttes proceduren uden noget resultat, hvis formanden for udvalget træffer beslutning herom, eller hvis et medlem af udvalget anmoder herom inden for tidsfristen for afgivelse af udtalelsen.

## KAPITEL IX
## AFSLUTTENDE BESTEMMELSER

*Artikel 40*

**Evaluering**

Senest den 17. oktober 2027 og derefter hver 36. måned evaluerer Kommissionen, hvorledes dette direktiv fungerer og forelægger en rapport for Europa-Parlamentet og Rådet. Rapporten skal navnlig vurdere relevansen af størrelsen af de berørte enheder og sektorerne, delsektorerne og typerne af enheder omhandlet i bilag I og II for, hvordan økonomien og samfundet fungerer i relation til cybersikkerhed. I det øjemed og med henblik på yderligere at fremme det strategiske og operationelle samarbejde tager Kommissionen hensyn til samarbejdsgruppens og CSIRT-netværkets rapporter om

de erfaringer, der er gjort på strategisk og operationelt plan. Rapporten ledsages om nødvendigt af et lovgivningsforslag.

*Artikel 41*

**Gennemførelse**

1. Medlemsstaterne vedtager og offentliggør senest den 17. oktober 2024 de love og bestemmelser, der er nødvendige for at efterkomme dette direktiv. De underretter straks Kommissionen herom.

De anvender disse love og bestemmelser fra den 18. oktober 2024.

2. De i stk. 1 omhandlede love og bestemmelser skal ved vedtagelsen indeholde en henvisning til dette direktiv eller skal ved offentliggørelsen ledsages af en sådan henvisning. Medlemsstaterne fastsætter de nærmere regler for henvisningen.

*Artikel 42*

**Ændringer af forordning (EU) nr. 910/2014**

I forordning (EU) nr. 910/2014 udgår artikel 19 med virkning fra den 18. oktober 2024.

*Artikel 43*

**Ændring af direktiv (EU) 2018/1972**

I direktiv (EU) 2018/1972 udgår artikel 40 og 41 med virkning fra den 18. oktober 2024.

*Artikel 44*

**Ophævelse**

Direktiv (EU) 2016/1148 ophæves med virkning fra den 18. oktober 2024.

Henvisninger til det ophævede direktiv gælder som henvisninger til nærværende direktiv og læses efter sammenligningstabellen i bilag III.

*Artikel 45*

**Ikrafttræden**

Dette direktiv træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

*Artikel 46*

**Adressater**

Dette direktiv er rettet til medlemsstaterne.

Udfærdiget i Strasbourg, den 14. december 2022.

*På Europa-Parlamentets vegne*

R. METSOLA

*Formand*

*På Rådets vegne*

M. BEK

*Formand*

---

(1) EUT C 233 af 16.6.2022, s. 22.

(2) EUT C 286 af 16.7.2021, s. 170.

(3) Europa-Parlamentets holdning af 10.11.2022 (endnu ikke offentliggjort i EUT) og Rådets afgørelse af 28.11.2022.

(4) 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 (EUT L 194 af 19.7.2016, s. 1).

(5) Kommissionens henstilling 2003/361/EF af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder (EUT L 124 af 20.5.2003, s. 36).

(6) 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 (EUT L 257 af 28.8.2014, s. 73).

(7) Europa-Parlamentets og Rådets direktiv 97/67/EF af 15. december 1997 om fælles regler for udvikling af Fællesskabets indre marked for posttjenester og forbedring af disse tjenesters kvalitet (EFT L 15 af 21.1.1998, s. 14).

(8) 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) (EUT L 119 af 4.5.2016, s. 1).

(9) Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (Direktiv om databeskyttelse inden for elektronisk kommunikation) (EFT L 201 af 31.7.2002, s. 37).

(10) Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og om ændring af forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011 (se side 1 i denne EUT).

(11) Europa-Parlamentets og Rådets forordning (EF) nr. 300/2008 af 11. marts 2008 om fælles bestemmelser om sikkerhed inden for civil luftfart og om ophævelse af forordning (EF) nr. 2320/2002 (EUT L 97 af 9.4.2008, s. 72).

([12]) Europa-Parlamentets og Rådets forordning (EU) 2018/1139 af 4. juli 2018 om fælles regler for civil luftfart og oprettelse af Den Europæiske Unions Luftfartssikkerhedsagentur og om ændring af forordning (EF) nr. 2111/2005, (EF) nr. 1008/2008, (EU) nr. 996/2010, (EU) nr. 376/2014 og direktiv 2014/30/EU og 2014/53/EU og om ophævelse af (EF) nr. 552/2004 og (EF) nr. 216/2008 og Rådets forordning (EØF) nr. 3922/91 (EUT L 212 af 22.8.2018, s. 1).

([13]) 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 (se side 164 i denne EUT).

([14]) Europa-Parlamentets og Rådets forordning (EU) 2021/696 af 28. april 2021 om oprettelse af Unionens rumprogram og Den Europæiske Unions Agentur for Rumprogrammet og om ophævelse af forordning (EU) nr. 912/2010, (EU) nr. 1285/2013 og (EU) nr. 377/2014 og afgørelse nr. 541/2014/EU (EUT L 170 af 12.5.2021, s. 69).

([15]) Kommissionens henstilling (EU) 2017/1584 af 13. september 2017 om en koordineret reaktion på væsentlige cybersikkerhedshændelser og -kriser (EUT L 239 af 19.9.2017, s. 36).

([16]) Rådets gennemførelsesafgørelse (EU) 2018/1993 af 11. december 2018 om EU's integrerede ordninger for politisk kriserespons (EUT L 320 af 17.12.2018, s. 28).

([17]) Europa-Parlamentets og Rådets afgørelse nr. 1313/2013/EU af 17. december 2013 om en EU-civilbeskyttelsesmekanisme (EUT L 347 af 20.12.2013, s. 924).

([18]) 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) (EUT L 151 af 7.6.2019, s. 15).

([19]) Kommissionens henstilling (EU) 2019/534 af 26. marts 2019 Cybersikkerheden i forbindelse med 5G-net (EUT L 88 af 29.3.2019, s. 42).

([20]) Europa-Parlamentets og Rådets direktiv (EU) 2018/1972 af 11. december 2018 om oprettelse af en europæisk kodeks for elektronisk kommunikation (EUT L 321 af 17.12.2018, s. 36).

([21]) Europa-Parlamentets og Rådets forordning (EU) 2021/694 af 29. april 2021 om programmet for et digitalt Europa og om ophævelse af afgørelse (EU) 2015/2240 (EUT L 166 af 11.5.2021, s. 1).

([22]) EUT L 123 af 12.5.2016, s. 1.

([23]) Europa-Parlamentets og Rådets forordning (EU) nr. 182/2011 af 16. februar 2011 om de generelle regler og principper for, hvordan medlemsstaterne skal kontrollere Kommissionens udøvelse af gennemførelsesbeføjelser (EUT L 55 af 28.2.2011, s. 13).

([24]) Europa-Parlamentets og Rådets forordning (EU) 2022/2065 af 19. oktober 2022 om et indre marked for digitale tjenester og om ændring af direktiv 2000/31/EF (forordning om digitale tjenester) (EUT L 277 af 27.10.2022, s. 1).

([25]) Europa-Parlamentets og Rådets forordning (EU) 2018/1725 af 23. oktober 2018 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i Unionens institutioner, organer, kontorer og agenturer og om fri udveksling af sådanne oplysninger og om ophævelse af forordning (EF) nr. 45/2001 og afgørelse nr. 1247/2002/EF (EUT L 295 af 21.11.2018, s. 39).

([26]) EUT C 183 af 11.5.2021, s. 3.

([27]) Europa-Parlamentets og Rådets direktiv 2011/93/EU af 13. december 2011 om bekæmpelse af seksuelt misbrug og seksuel udnyttelse af børn og børnepornografi og om erstatning af Rådets rammeafgørelse 2004/68/RIA (EUT L 335 af 17.12.2011, s. 1).

([28]) Europa-Parlamentets og Rådets direktiv 2013/40/EU af 12. august 2013 om angreb på informationssystemer og om erstatning af Rådets rammeafgørelse 2005/222/RIA (EUT L 218 af 14.8.2013, s. 8).

([29]) Europa-Parlamentets og Rådets forordning (EU) nr. 1025/2012 af 25. oktober 2012 om europæisk standardisering, om ændring af Rådets direktiv 89/686/EØF og 93/15/EØF og Europa-Parlamentets og Rådets direktiv 94/9/EF, 94/25/EF, 95/16/EF, 97/23/EF, 98/34/EF, 2004/22/EF, 2007/23/EF, 2009/23/EF og 2009/105/EF og om ophævelse af Rådets beslutning 87/95/EØF og Europa-Parlamentets og Rådets afgørelse nr. 1673/2006/EF (EUT L 316 af 14.11.2012, s. 12).

([30]) 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 (EUT L 241 af 17.9.2015, s. 1).

([31]) Europa-Parlamentets og Rådets direktiv 2005/29/EF af 11. maj 2005 om virksomheders urimelige handelspraksis over for forbrugerne på det indre marked og om ændring af Rådets direktiv 84/450/EØF og Europa-Parlamentets og Rådets direktiv 97/7/EF, 98/27/EF og 2002/65/EF og Europa-Parlamentets og Rådets forordning (EF) nr. 2006/2004 (direktivet om urimelig handelspraksis) (EUT L 149 af 11.6.2005, s. 22).

([32]) Europa-Parlamentets og Rådets forordning (EU) 2019/1150 af 20. juni 2019 om fremme af retfærdighed og gennemsigtighed for erhvervsbrugere af onlineformidlingstjenester (EUT L 186 af 11.7.2019, s. 57).

---

## BILAG I

## SEKTORER AF SÆRLIGT 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 ([1]), 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 ([2])<br>- 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<br>- 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 Eu- |

| | | |
|---|---|---|
| | | ropa-Parlamentets og Rådets direktiv (EU) 2018/2001 ([3]) |
| | 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 ([4]) |
| | d) Gas | - Forsyningsvirksomheder som defineret i artikel 2, nr. 8), i Europa-Parlamentets og Rådets direktiv 2009/73/EF ([5]) |
| | | - 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 |

| | | |
|---|---|---|
| | e) 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 ([6]), 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 ([7]); 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 ([8]) |
| | b) Jernbane | - Infrastrukturforvaltere som defineret i artikel 3, nr. 2), i Europa-Parlamentets og Rådets direktiv 2012/34/EU ([9]) |
| | | - 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 højsøfarvand eller kystnært farvand som defineret for søtransport i bilag I til Europa-Parlamentets og Rådets forordning (EF) nr. 725/2004 ([10]), 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 ([11]), 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 ([12]) |
| | d) Vejtransport | - Vejmyndigheder som defineret i artikel 2, nr. 12), i Kommissionens delegerede forordning (EU) 2015/962 ([13]), 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 defi- |

| | | |
|---|---|---|
| | | neret i artikel 4, nr. 1), i Europa-Parlamentets og Rådets direktiv 2010/40/EU ([14]) |
| 3. Bankvirksomhed | | Kreditinstitutter som defineret i artikel 4, nr. 1), i Europa-Parlamentets og Rådets forordning (EU) nr. 575/2013 ([15]) |
| 4. Finansielle markedsinfrastrukturer | | - Operatører af markedspladser som defineret i artikel 4, nr. 24), i Europa-Parlamentets og Rådets direktiv 2014/65/EU ([16]) |
| | | - Centrale modparter (CCP'er) som defineret i artikel 2, nr. 1), i Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012 ([17]) |
| 5. Sundhed | | - Sundhedstjenesteydere som defineret i artikel 3, litra g), i Europa-Parlamentets og Rådets direktiv 2011/24/EU ([18]) |
| | | - EU-referencelaboratorier, der er omhandlet i artikel 15, i Europa-Parlamentets og Rådets forordning (EU) 2022/2371 ([19]) |
| | | - Enheder, der udfører forsknings- og udviklingsaktiviteter vedrørende lægemidler som defineret i artikel 1, nr. 2), i Europa-Parlamentets og Rådets direktiv 2001/83/EF ([20])<br>- Enheder, der fremstiller farmaceutiske råvarer og farmaceutiske præparater som omhandlet i hovedafdeling |

| | | |
|---|---|---|
| | | C, hovedgruppe 21, i NACE rev. 2<br><br>- 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 ([21]) 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) 2020/2184 ([22]) bortset 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 ([23]), 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<br>- Udbydere af administrerede sikkerhedstjenester |
| 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 |

(1) Europa-Parlamentets og Rådets direktiv (EU) 2019/944 af 5. juni 2019 om fælles regler for det indre marked for elektricitet og om ændring af direktiv 2012/27/EU (EUT L 158 af 14.6.2019, s. 125).

(2) Europa-Parlamentets og Rådets forordning (EU) 2019/943 af 5. juni 2019 om det indre marked for elektricitet (EUT L 158 af 14.6.2019, s. 54).

(3) Europa-Parlamentets og Rådets direktiv (EU) 2018/2001 af 11. december 2018 om fremme af anvendelsen af energi fra vedvarende energikilder (EUT L 328 af 21.12.2018, s. 82).

(4) Rådets direktiv 2009/119/EF af 14. september 2009 om forpligtelse for medlemsstaterne til at holde minimumslagre af råolie og/eller olieprodukter (EUT L 265 af 9.10.2009, s. 9).

(5) Europa-Parlamentets og Rådets direktiv 2009/73/EF af 13. juli 2009 om fælles regler for det indre marked for naturgas og om ophævelse af direktiv 2003/55/EF (EUT L 211 af 14.8.2009, s. 94).

(6) Europa-Parlamentets og Rådets direktiv 2009/12/EF af 11. marts 2009 om lufthavnsafgifter (EUT L 70 af 14.3.2009, s. 11).

(7) Europa-Parlamentets og Rådets forordning (EU) nr. 1315/2013 af 11. december 2013 om Unionens retningslinjer for udvikling af det transeuropæiske transportnet og om ophævelse af afgørelse nr. 661/2010/EU (EUT L 348 af 20.12.2013, s. 1).

(8) Europa-Parlamentets og Rådets forordning (EF) nr. 549/2004 af 10. marts 2004 om rammerne for oprettelse af et fælles europæisk luftrum (»rammeforordningen«) (EUT L 96 af 31.3.2004, s. 1).

(9) Europa-Parlamentets og Rådets direktiv 2012/34/EU af 21. november 2012 om oprettelse af et fælles europæisk jernbaneområde (EUT L 343 af 14.12.2012, s. 32).

(10) Europa-Parlamentets og Rådets forordning (EF) nr. 725/2004 af 31. marts 2004 om bedre sikring af skibe og havnefaciliteter (EUT L 129 af 29.4.2004, s. 6).

(11) Europa-Parlamentets og Rådets direktiv 2005/65/EF af 26. oktober 2005 om bedre havnesikring (EUT L 310 af 25.11.2005, s. 28).

(12) Europa-Parlamentets og Rådets direktiv 2002/59/EF af 27. juni 2002 om oprettelse af et trafikovervågnings- og trafikinformationssystem for skibsfarten i Fællesskabet og om ophævelse af Rådets direktiv 93/75/EØF (EFT L 208 af 5.8.2002, s. 10).

([13]) Kommissionens delegerede forordning (EU) 2015/962 af 18. december 2014 om supplerende regler til Europa-Parlamentets og Rådets direktiv 2010/40/EU for så vidt angår tilrådighedsstillelse af EU-dækkende tidstro trafikinformationstjenester (EUT L 157 af 23.6.2015, s. 21).

([14]) Europa-Parlamentets og Rådets direktiv 2010/40/EU af 7. juli 2010 om rammerne for indførelse af intelligente transportsystemer på vejtransportområdet og for grænsefladerne til andre transportformer (EUT L 207 af 6.8.2010, s. 1).

([15]) Europa-Parlamentets og Rådets forordning (EU) nr. 575/2013 af 26. juni 2013 om tilsynsmæssige krav til kreditinstitutter og om ændring af forordning (EU) nr. 648/2012 (EUT L 176 af 27.6.2013, s. 1).

([16]) Europa-Parlamentets og Rådets direktiv 2014/65/EU af 15. maj 2014 om markeder for finansielle instrumenter og om ændring af direktiv 2002/92/EF og direktiv 2011/61/EU (EUT L 173 af 12.6.2014, s. 349).

([17]) Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012 af 4. juli 2012 om OTC-derivater, centrale modparter og transaktionsregistre (EUT L 201 af 27.7.2012, s. 1).

([18]) Europa-Parlamentets og Rådets direktiv 2011/24/EU af 9. marts 2011 om patientrettigheder i forbindelse med grænseoverskridende sundhedsydelser (EUT L 88 af 4.4.2011, s. 45).

([19]) Europa-Parlamentets og Rådets forordning (EU) 2022/2371 af 23. november 2022 om alvorlige grænseoverskridende sundhedstrusler og om ophævelse af afgørelse nr. 1082/2013/EU (EUT L 314 af 6.12.2022, s. 26).

([20]) Europa-Parlamentets og Rådets direktiv 2001/83/EF af 6. november 2001 om oprettelse af en fællesskabskodeks for humanmedicinske lægemidler (EFT L 311 af 28.11.2001, s. 67).

([21]) Europa-Parlamentets og Rådets forordning (EU) 2022/123 af 25. januar 2022 om styrkelse af Det Europæiske Lægemiddelagenturs rolle i forbindelse med kriseberedskab og krisestyring med hensyn til lægemidler og medicinsk udstyr (EUT L 20 af 31.1.2022, s. 1).

([22]) Europa-Parlamentets og Rådets direktiv (EU) 2020/2184 af 16. december 2020 om kvaliteten af drikkevand (EUT L 435 af 23.12.2020, s. 1).

([23]) Rådets direktiv 91/271/EØF af 21. maj 1991 om rensning af byspildevand (EFT L 135 af 30.5.1991, s. 40).

---

## BILAG II

## ANDRE KRITISKE SEKTORER

| 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 ([1]), 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 ([2]) 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 ([3]), 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 ([4]), 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 ([5]), 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 |

(1) Europa-Parlamentets og Rådets direktiv 2008/98/EF af 19. november 2008 om affald og om ophævelse af visse direktiver (EUT L 312 af 22.11.2008, s. 3).

(2) Europa-Parlamentets og Rådets forordning (EF) nr. 1907/2006 af 18. december 2006 om registrering, vurdering og godkendelse af samt begrænsninger for kemikalier (REACH), om oprettelse af et europæisk kemikalieagentur og om ændring af direktiv 1999/45/EF og ophævelse af Rådets forordning (EØF) nr. 793/93 og Kommissionens forordning (EF) nr. 1488/94 samt Rådets direktiv 76/769/EØF og Kommissionens direktiv 91/155/EØF, 93/67/EØF, 93/105/EF og 2000/21/EF (EUT L 396 af 30.12.2006, s. 1).

(3) Europa-Parlamentets og Rådets forordning (EF) nr. 178/2002 af 28. januar 2002 om generelle principper og krav i fødevarelovgivningen, om oprettelse af Den Europæiske Fødevaresikkerhedsautoritet og om procedurer vedrørende fødevaresikkerhed (EFT L 31 af 1.2.2002, s. 1).

(4) Europa-Parlamentets og Rådets forordning (EU) 2017/745 af 5. april 2017 om medicinsk udstyr, om ændring af direktiv 2001/83/EF, forordning (EF) nr. 178/2002 og forordning (EF) nr. 1223/2009 og om ophævelse af Rådets direktiv 90/385/EØF og 93/42/EØF (EUT L 117 af 5.5.2017, s. 1).

(5) Europa-Parlamentets og Rådets forordning (EU) 2017/746 af 5. april 2017 om medicinsk udstyr til in vitro-diagnostik og om ophævelse af direktiv 98/79/EF og Kommissionens afgørelse 2010/227/EU (EUT L 117 af 5.5.2017, s. 176).

## BILAG III

## SAMMENLIGNINGSTABEL

| Direktiv (EU) 2016/1148 | Nærværende direktiv |
|---|---|
| Artikel 1, stk. 1 | Artikel 1, stk. 1 |
| Artikel 1, stk. 2 | Artikel 1, stk. 2 |
| Artikel 1, stk. 3 | — |
| Artikel 1, stk. 4 | Artikel 2, stk. 12 |
| Artikel 1, stk. 5 | Artikel 2, stk. 13 |
| Artikel 1, stk. 6 | Artikel 2, stk. 6 og 11 |
| Artikel 1, stk. 7 | Artikel 4 |
| Artikel 2 | Artikel 2, stk. 14 |
| Artikel 3 | Artikel 5 |
| Artikel 4 | Artikel 6 |
| Artikel 5 | — |
| Artikel 6 | — |

| | |
|---|---|
| Artikel 7, stk. 1 | Artikel 7, stk. 1 og 2 |
| Artikel 7, stk. 2 | Artikel 7, stk. 4 |
| Artikel 7, stk. 3 | Artikel 7, stk. 3 |
| Artikel 8, stk. 1-5 | Artikel 8, stk. 1-5 |
| Artikel 8, stk. 6 | Artikel 13, stk. 4 |
| Artikel 8, stk. 7 | Artikel 8, stk. 6 |
| Artikel 9, stk. 1, 2 og 3 | Artikel 10, stk. 1, 2 og 3 |
| Artikel 9, stk. 4 | Artikel 10, stk. 9 |
| Artikel 9, stk. 5 | Artikel 10, stk. 10 |
| Artikel 10, stk. 1, stk. 2 og stk. 3, første afsnit | Artikel 13, stk. 1, 2 og 3 |
| Artikel 10, stk. 3, andet afsnit | Artikel 23, stk. 9 |
| Artikel 11, stk. 1 | Artikel 14, stk. 1 og 2 |
| Artikel 11, stk. 2 | Artikel 14, stk. 3 |
| Artikel 11, stk. 3 | Artikel 14, stk. 4, første afsnit, litra a)-q) og litra s), og stk. 7 |
| Artikel 11, stk. 4 | Artikel 14, stk. 4, første afsnit, litra r), og andet afsnit |
| Artikel 11, stk. 5 | Artikel 14, stk. 8 |
| Artikel 12, stk. 1-5 | Artikel 15, stk. 1-5 |
| Artikel 13 | Artikel 17 |
| Artikel 14, stk. 1 og 2 | Artikel 21, stk. 1-4 |
| Artikel 14, stk. 3 | Artikel 23, stk. 1 |
| Artikel 14, stk. 4 | Artikel 23, stk. 3 |
| Artikel 14, stk. 5 | Artikel 23, stk. 5, 6 og 8 |
| Artikel 14, stk. 6 | Artikel 23, stk. 7 |
| Artikel 14, stk. 7 | Artikel 23, stk. 11 |
| Artikel 15, stk. 1 | Artikel 31, stk. 1 |
| Artikel 15, stk. 2, første afsnit, litra a) | Artikel 32, stk. 2, litra e) |
| Artikel 15, stk. 2, første afsnit, litra b) | Artikel 32, stk. 2, litra g) |
| Artikel 15, stk. 2, andet afsnit | Artikel 32, stk. 3 |

| | |
|---|---|
| Artikel 15, stk. 3 | Artikel 32, stk. 4, litra b) |
| Artikel 15, stk. 4 | Artikel 31, stk. 3 |
| Artikel 16, stk. 1 og 2 | Artikel 21, stk. 1-4 |
| Artikel 16, stk. 3 | Artikel 23, stk. 1 |
| Artikel 16, stk. 4 | Artikel 23, stk. 3 |
| Artikel 16, stk. 5 | — |
| Artikel 16, stk. 6 | Artikel 23, stk. 6 |
| Artikel 16, stk. 7 | Artikel 23, stk. 7 |
| Artikel 16, stk. 8 og 9 | Artikel 21, stk. 5, og artikel 23, stk. 11 |
| Artikel 16, stk. 10 | — |
| Artikel 16, stk. 11 | Artikel 2, stk. 1, 2 og 3 |
| Artikel 17, stk. 1 | Artikel 33, stk. 1 |
| Artikel 17, stk. 2, litra a) | Artikel 32, stk. 2, litra e) |
| Artikel 17, stk. 2, litra b) | Artikel 32, stk. 4, litra b) |
| Artikel 17, stk. 3 | Artikel 37, stk. 1, litra a) og b) |
| Artikel 18, stk. 1 | Artikel 26, stk. 1, litra b), og stk. 2 |
| Artikel 18, stk. 2 | Artikel 26, stk. 3 |
| Artikel 18, stk. 3 | Artikel 26, stk. 4 |
| Artikel 19 | Artikel 25 |
| Artikel 20 | Artikel 30 |
| Artikel 21 | Artikel 36 |
| Artikel 22 | Artikel 39 |
| Artikel 23 | Artikel 40 |
| Artikel 24 | — |
| Artikel 25 | Artikel 41 |
| Artikel 26 | Artikel 45 |
| Artikel 27 | Artikel 46 |
| Bilag I, punkt 1 | Artikel 11, stk. 1 |
| Bilag I, punkt 2, litra a), nr. i)-iv) | Artikel 11, stk. 2, litra a)-d) |
| Bilag I, punkt 2, litra a), nr. v) | Artikel 11, stk. 2, litra f) |
| Bilag I, punkt 2, litra b) | Artikel 11, stk. 4 |

| | |
|---|---|
| Bilag I, punkt 2, litra c), nr. i) og ii) | Artikel 11, stk. 5, litra a) |
| Bilag II | Bilag I |
| Bilag III, punkt 1 og 2 | Bilag II, punkt 6 |
| Bilag III, punkt 3 | Bilag I, punkt 8 |

**Bilag 2**

## Sektorer af særligt kritisk betydning

| Sektor | Delsektor | Type enhed |
|---|---|---|
| **1.** 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 højsøfarvand 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 ikke-væsentlig 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. |
| **2.** 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 lægemidler 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. |
| **3.** Drikkevand | | - Leverandører og distributører af drikkevand som defineret i artikel 2, nr. 1, litra a, i Europa-Parlamentets og Rådets direktiv (EU) 2020/2184, bortset fra distributører for hvilke distribution af drikkevand er en ikke-væsentlig del af deres generelle aktivitet med distribution af andre råvarer og varer. |
| **4.** Spildevand | | - Virksomheder der indsamler, bortskaffer eller behandler byspildevand, husspildevand eller industrispildevand som defineret i artikel 2, nr. 1-3, i Rådets direktiv 91/271/EØF, bortset fra virksomheder for hvilke indsamling, bortskaffelse eller behandling af byspildevand, husspildevand eller industrispildevand er en ikke-væsentlig del af deres generelle aktivitet. |
| **5.** Digital infrastruktur | | - Udbydere af internetudvekslingspunkter. |
| | | - DNS-tjenesteudbydere, bortset fra operatører af rodnavneservere. |
| | | - Topdomænenavneadministratorer. |
| | | - Udbydere af cloudcomputingtjenester. |
| | | - Udbydere af datacentertjenester med undtagelse af datacentertjenester, der er udpeget i medfør af § 333, stk. 1, i lov om finansiel virksomhed. |
| | | - Udbydere af indholdsleveringsnetværk. |

| | | |
|---|---|---|
| | | - Tillidstjenesteudbydere. |
| | | - Udbydere af offentlige elektroniske kommunikationsnet med undtagelse af udbydere, der er omfattet af lov om cybersikkerhed i telesektoren. |
| | | - Udbydere af offentligt tilgængelige elektroniske kommunikationstjenester med undtagelse af udbydere, der er omfattet af lov om cybersikkerhed i telesektoren. |
| **6.** Forvaltning af IKT-tjenester (business-to-business) | | - Udbydere af administrerede tjenester |
| | | - Udbydere af administrerede sikkerhedstjenester |
| **7.** 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. |
| **8.** 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 3**

## Andre kritiske sektorer

| 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 til 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 intet andetsteds nævnt | - 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 en afgørende rolle i samfundet, og både virksomheder, myndigheder og borgere er i stigende grad afhængige af velfungerende digitale systemer i hverdagen. Men med den høje grad af digitalisering følger også en høj grad af sårbarhed. Det kan være i forhold til nedbrud forårsaget af eksempelvis systemsvigt og menneskelige fejl, men også 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.

Det 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 yderligere. Europa-Parlamentet og Rådet har derfor vedtaget NIS 2-direktivet (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 ophæver og erstatter NIS 1-direktivet (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 2-direktivet har til formål at skabe et højere og mere ensartet cybersikkerhedsniveau på tværs af medlemsstaterne. Direktivet stiller bl.a. cybersikkerhedskrav til virksomheder, myndigheder og organisationer (enheder) inden for en lang række samfundskritiske sektorer, som bl.a. omfatter energi, transport, bankvirksomhed, sundhed, drikke- og spildevand, digital infrastruktur og den offentlige forvaltning. Samtidig fastsættes en række oplysnings- og underretningspligter over for myndighederne, herunder underretning ved væsentlige hændelser samt pligt til at oplyse enhedernes brugere

om bl.a. væsentlige hændelser og eventuelle modforholdsregler, som brugerne kan træffe. Direktivet styrker desuden myndighedernes tilsynsbeføjelser og håndhævelsesmuligheder og indfører bl.a. mulighed for, at myndighederne midlertidigt kan suspendere topledere i enhederne. Derudover indfører direktivet væsentligt skærpede sanktionsmuligheder i form af et højere bødeniveau.

Formålet med dette lovforslag er at gennemføre 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 gennemførelse af NIS 1-direktivet vil samtidig blive ophævet.

Uden for den foreslåede hovedlovs anvendelsesområde står tele-, energi- og finanssektorerne. Det skyldes, at der i disse sektorer allerede findes en omfattende sektorspecifik regulering af cybersikkerheden. For disse sektorer er der derfor helt særlige hensyn, som gør, at den nye regulering bør ske sektorvist, således at gennemførelsen af NIS 2-direktivet kan integreres med den eksisterende regulering.

## 2. Lovforslagets baggrund

### 2.1. Fra NIS 1- til NIS 2-direktivet

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

NIS 1-direktivet fastlægger for det første krav til rammerne for arbejdet med sikkerhed i net- og informationssystemer både nationalt og på EU-niveau, herunder krav til samarbejdsorganer og myndighedsstruktur. For det andet stiller direktivet krav om, at der fastsættes sikkerhedskrav og underretningspligter for operatører af væsentlige tjenester og udbydere af digitale tjenester.

Med NIS 1-direktivet er der således allerede taget skridt hen mod at øge cybersikkerheden på tværs af EU.

Baggrunden for NIS 2-direktivet er, at der fra EU's side er konstateret store forskelle i medlemsstaternes gennemførelse af NIS 1-direktivet, herunder med hensyn til, hvilke enheder der anses for omfattet af direktivet, da afgrænsningen heraf i vid udstrækning blev overladt til medlemsstaternes skøn. NIS 1-direktivet giver også medlemsstaterne meget vide skønsbefø-

jelser med hensyn til gennemførelsen af direktivets sikkerheds- og hændelsesrapporteringsforpligtelser samt bestemmelserne om tilsyn og håndhævelse.

Formålet med NIS 2-direktivet er derfor at skabe et højere og mere ensartet cybersikkerhedsniveau på tværs af medlemsstaterne.

NIS 2-direktivet 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 det var tilfældet med NIS 1-direktivet.

## 2.2. Model for implementering af NIS 2-direktivet

### 2.2.1. Lovgivningsmodel

Kravene i NIS 2-direktivet er rettet mod en bred vifte af sektorer, og direktivet har således et meget bredt anvendelsesområde.

Ved gennemførelsen anser Forsvarsministeriet det på den ene side for væsentligt, at direktivets krav målrettes og tilpasses de enkelte sektorers særlige forhold. Samtidig er det på den anden side 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 videreføre de enkelte ressortministeriers ansvar for cybersikkerhed og tilsyn i deres respektive sektorer, mens Center for Cybersikkerhed tillægges en tværgående rolle og får til opgave at facilitere et tæt samarbejde mellem de ressortansvarlige myndigheder.

Med lovforslaget bemyndiges de relevante ressortministre på visse områder til at fastsætte nærmere regler i bekendtgørelsesform. En nærmere udmøntning af de centrale krav i bekendtgørelsesform vil skabe en klarere ramme for de berørte enheder, samtidig med at de centrale krav vil kunne tage højde for særlige sektorvise forhold. Anvendelsen af bekendtgørelsesformen vil herudover sikre, at der i nødvendigt omfang hurtigere kan gennemføres ændringer på baggrund af eksempelvis den teknologiske udvikling eller ændringer i trusselsbilledet.

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 forsvarsministeren. Det vil i praksis være Center for Cybersikkerhed, der på forsvarsministerens vegne forhandler de nærmere krav med de relevante ressortministerier.

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 sikre, at direktivet udmøntes på den måde, der er mest hensigtsmæssig for sektoren. Samtidig vil Center for Cybersikkerhed bistå med i videst muligt omfang at skabe et fælles cybersikkerhedsniveau på tværs af de omfattede sektorer.

Med dette lovforslag har Forsvarsministeriet 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 Forsvarsministeriet 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 (med undtagelse af tele-, energi- og finanssektorerne), indebærer, at den nuværende regulering, der gennemfører NIS 1-direktivet for de omfattede sektorer, 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, og de nationale myndigheder, som NIS 2-direktivet foreskriver, er derfor i vidt omfang allerede etableret eller udpeget.

Det vil påhvile de relevante ressortministerier at oprette eller udpege kompetente myndigheder med ansvar for cybersikkerhed og ansvar for at føre

tilsyn med de enkelte sektorer. Der er allerede på baggrund af NIS 1-direktivet udpeget kompetente myndigheder for så vidt angår de sektorer, som var omfattet af dette direktiv. Med NIS 2-direktivet omfattes yderligere sektorer, og der skal derfor også etableres kompetente myndigheder for disse sektorer. Der henvises i øvrigt 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. Her vil det eksempelvis kunne være relevant at gennemføre fælles tilsynsbesøg. Der vil også mere generelt 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 centrale kontaktpunkt skal sikre det tværsektorielle samarbejde mellem de nationale kompetente myndigheder, hvorfor det centrale kontaktpunkt bl.a. vil facilitere koordinationen vedrørende tilsynsarbejde mellem de kompetente myndigheder. Derudover vil det centrale kontaktpunkt udøve en forbindelsesfunktion 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). 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 varetages i dag af Center for Cybersikkerhed, og den opgave vil centeret 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 varetager endvidere funktionen som CSIRT, der er den nationale enhed, som håndterer it-sikkerhedshændelser. Også denne funktion vil centeret fortsat skulle varetage. Det gælder også i forhold til de sektorer, hvor NIS 2-direktivet gennemføres ved sektorspecifik regulering, jf. afsnit 1 ovenfor.

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. Som led i funktionen som centralt kontaktpunkt og CSIRT faciliterer Center for Cybersikkerhed derfor samarbejdet mellem de myndigheder, der varetager opgaver i medfør af direktivet.

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.

Opgaven som cyberkrisestyringsmyndighed vil blive varetaget af Center for Cybersikkerhed i forlængelse af opgaverne som CSIRT og centralt kontaktpunkt. Center for Cybersikkerhed har allerede i dag til opgave at koordinere operative opgaver i tilfælde af cyberangreb mod og på tværs af samfundskritiske sektorer. Som cyberkrisestyringsmyndighed får Center for Cybersikkerhed til opgave at styre omfattende cybersikkerhedshændelser inden for de eksisterende rammer for national krisestyring. I situationer, hvor Den Nationale Operative Stab (NOST) aktiveres, koordinerer Center for Cybersikkerhed sin indsats som cyberkrisestyringsmyndighed inden for rammerne af NOST, jf. den udarbejdede delplan til NOST Hovedplan.

Der vil i overensstemmelse med NIS 2-direktivets artikel 9, stk. 4, blive udarbejdet en national beredskabsplan for omfattende cybersikkerhedshændelser og -kriser, der fastsætter målene og ordningerne for håndtering heraf. 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, jf. også afsnit 2.2.3. nedenfor.

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. Der vil i det fremadrettede arbejde med strategien være fokus på NIS 2-direktivets krav.

Det bemærkes, at det ikke med den myndighedsstruktur, som er beskrevet i lovforslaget, har været hensigten at udelukke, at opgaver fremadrettet vil kunne ressortoverføres mellem ministre, samt overføres mellem myndigheder under den enkelte minister.

### 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, så de bedre er i 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 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 forhold, 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-direktivet, jf. NIS 2-direktivets artikel 2, stk. 3.

Forsvarsministeriet fremsætter samtidig med nærværende lovforslag et lovforslag om gennemførelse af CER-direktivet. Der anvendes i vidt omfang samme overordnede tilgang til gennemførelsen af de to direktiver. Der vil desuden i mange sektorer være sammenfald mellem de kompetente myndigheder efter henholdsvis NIS 2-direktivet og CER-direktivet, og det forudsættes i øvrigt, at myndigheder med opgaver i medfør af de to direktiver også i praksis koordinerer på tværs i relevant omfang.

### 2.4. Nuværende implementering af NIS 1-direktivet

I Danmark er NIS 1-direktivet gennemført sektorvist i regulering under de respektive ressortministerier.

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 m.v., 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 fastsætter forpligtelser for operatører af væsentlige tjenester og udbydere af digitale tjenester inden for direktivets anvendelsesområde.

Det påhviler 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 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 nedenfor.

### 3.1.2. Forsvarsministeriets overvejelser

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

NIS 2-direktivet fastsætter detaljerede regler for, hvilke virksomheder, myndigheder og organisationer (i direktivet kaldet 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 er en enhed defineret 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 Forsvarsministeriets 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 er Forsvarsministeriets opfattelse, at hele enheden vil være at anse for omfattet af direktivets anvendelsesområde, også selv om enheden har flere forretningsområder eller er opdelt i flere administrative enheder, og det eksempelvis alene er ét af disse forretningsområder, som er omfattet af de sektorer, der er omhandlet i direktivets bilag.

Det forhold, at en enhed i sin helhed bliver omfattet af NIS 2-direktivet, medfører imidlertid ikke, at der vil blive stillet krav om sikkerhedsforanstaltninger eller hændelsesrapportering i forhold til alle enhedens net- og informationssystemer.

Det er således Forsvarsministeriets 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 i lyset af de aktiviteter, som er omfattet af direktivets anvendelsesområde. Det afgørende element for, hvilke af enhedens net- og informationssystemer, der er underlagt direktivets krav, bliver på den baggrund, hvorvidt der ud fra en konkret risikovurdering er tale om net- og informationssystemer, som – hvis de blev kompromitteret – vurderes at ville kunne påvirke enhedens levering af de tjenester eller opretholdelse af de aktiviteter, som er baggrunden for, at enheden er omfattet af direktivet.

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 sektorerne: 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.

Af direktivets bilag II fremgår følgende 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.

Som udgangspunkt omfattes kun enheder af en vis størrelse, således at enheder af en størrelse svarende til mikrovirksomheder og små virksomheder som udgangspunkt ikke omfattes af direktivets anvendelsesområde. 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 af direktivet oplistede sektorer – enheder, der er identificeret som kritiske i medfør af gennemførelsen af CER-direktivet, og enheder, der leverer domænenavnsregistreringstjenester.

Det er op til medlemsstaterne, om direktivet også skal finde anvendelse på offentlige forvaltningsenheder på lokalt plan samt uddannelsesinstitutioner, navnlig hvis uddannelsesinstitutionerne udfører kritiske forskningsaktiviteter. Tilvalgsordningen vil alene gælde i det omfang, enhederne ikke allerede omfattes af direktivets anvendelsesområde. Offentlige forvaltningsenheder på lokalt plan vil i nogle tilfælde levere tjenester i de øvrige sektorer, og allerede af den grund være omfattet af direktivets anvendelsesområde.

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.

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. Overordnet følger det af artiklen, at enheder, der ikke opfylder kriterierne for at være væsentlige enheder, anses for at være vigtige enheder.

Som væsentlige enheder anses: 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.

Der vil også være enheder (f.eks. kommuner eller større virksomheder og organisationer), som udøver aktiviteter i flere af de sektorer, der er omhandlet i direktivets 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. På baggrund af tilkendegivelser fra EU-Kommissionen i regi af Samarbejdsgruppen er det Forsvarsministeriets 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. Dette vil også gælde for de dele af enhedens aktiviteter, som isoleret set alene ville have medført, at enheden ville være at betragte som vigtig. Det skal dog understreges, at de kompetente myndigheder vil føre deres tilsyn ud fra en risikovurdering, således at frekvensen for tilsynene og tilsynets omfang tilpasses enhedens aktiviteter.

### 3.1.3. Den foreslåede ordning

Det foreslås, at NIS 2-direktivets bestemmelser om, hvilke enheder der omfattes af direktivet, herunder kategoriseringen af væsentlige og vigtige enheder, minimumsimplementeres 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.

Det foreslås på den baggrund, 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 sektorvise regulering, der gennemfører NIS 2-direktivet i henholdsvis tele-, energi- eller finanssektorerne. Enheder vil dog fortsat kunne være omfattet af denne lov, hvis de udover aktiviteterne i eksempelvis energisektoren også udfører aktiviteter inden for en af de sektorer, som er nævnt i lovens bilag 2 og 3.

Det foreslås desuden, at vedkommende minister bemyndiges til ved bekendtgørelse at bestemme, at loven helt eller delvist også finder anvendelse

på henholdsvis offentlige forvaltningsenheder på lokalt plan – eksempelvis kommunerne – og uddannelsesinstitutioner.

Det foreslås endvidere, at kategoriseringen af enheder som henholdsvis væsentlige og vigtige følger tilgangen i direktivet.

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, bemærkes det, at direktivet både nævner disse som væsentlige og vigtige enheder. Det er Forsvarsministeriets 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 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. Forsvarsministeriets overvejelser

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

Den grundlæggende tilgang svarer i vidt omfang til NIS 1-direktivets sikkerhedskrav, idet bestemmelsen i NIS 2-direktivet dog bygger videre herpå og i større detaljeringsgrad foreskriver, hvad foranstaltningerne som minimum bør omfatte eller tage højde for.

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.

Europa-Kommissionen kan – og forudsættes på nogle områder at – vedtage gennemførelsesretsakter om foranstaltningerne.

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

Det er Forsvarsministeriets opfattelse, at NIS 2-direktivets krav om foranstaltninger til styring af cybersikkerhedsrisici bør konkretiseres nærmere, således at der ved gennemførelsen i størst muligt omfang fastsættes klare og tydelige krav til de omfattede enheder. Dermed skabes dels forudsætningerne for etablering af et højt fælles sikkerhedsniveau, dels forudsigelighed for de omfattede enheder.

Det er Forsvarsministeriets opfattelse, at 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 forsvarsministeren, jf. afsnit 2.2 ovenfor.

Forsvarsministeriet har lagt vægt på, at gennemførelsen af NIS 2-direktivet sker i overensstemmelse med regeringens principper for minimumsimplementering af erhvervsrettet EU-regulering, hvorefter den nationale regulering som udgangspunkt ikke bør gå videre end minimumskravene i EU-reguleringen.

Det vil på den baggrund skulle sikres, at de bekendtgørelser, der udmønter direktivets krav om foranstaltninger, udarbejdes inden for rammerne af en minimumsimplementering af direktivet. I det omfang Europa-Kommissionen vedtager gennemførelsesretsakter om foranstaltningerne, vil det endvidere skulle sikres, at bekendtgørelserne er i overensstemmelse med de rammer, der måtte følge af disse. Såfremt gennemførelsesretsakterne måtte regulere området fuldt ud, vil allerede udstedte bekendtgørelser i givet fald skulle ophæves.

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.

Det er Forsvarsministeriet opfattelse, at de relevante ministre efter forhandling med forsvarsministeren 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. Det er Forsvarsministeriets opfattelse, at bekendtgørelserne bør udarbejdes inden for rammerne af regeringens principper om minimumsimplementering.

### 3.2.3. Den foreslåede ordning

Det foreslås, at NIS 2-direktivets regler i artikel 21 og 24 vedrørende foranstaltninger til styring af cybersikkerhedsrisici og brug af europæiske cybersikkerhedscertificeringsordninger minimumsimplementeres 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.

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 som minimum 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 forsvarsministeren – kan fastsætte nærmere regler om de krav til foranstaltninger, som væsentlige og vigtige enheder skal træffe til styring af cybersikkerhedsrisici. Kravene vil dermed 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. Det forudsættes, at der i forbindelse med fastsættelsen af de nærmere regler om krav til foranstaltninger til styring af cybersikkerhedsrisici vil ske en koordination mellem de enkelte ressortministerier med henblik på at sikre, at der ikke fastsættes indbyrdes modsatrettede regler. Der henvises herom til afsnit 2.3 ovenfor.

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.

Endelig foreslås det på baggrund af direktivets artikel 24, at vedkommende ressortminister efter forhandling med forsvarsministeren 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 cybersikkerehdscertificeringsordning 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, 7, 8 og 30.

## 3.3. Hændelsesrapportering

### 3.3.1. Gældende ret

NIS 1-direktivet forpligter 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 og til Center for Cybersikkerhed i centerets funktion som national CSIRT og centralt 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 Center for Cybersikkerhed 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. Center for Cybersikkerhed foretager dog i dag i centerets funktion som national CSIRT og centralt kontaktpunkt orientering af offentligheden i tilfælde, hvor en hændelse berører flere sektorer.

### 3.3.2. Forsvarsministeriets overvejelser

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

NIS 2-direktivets artikel 23 indeholder forpligtelser for væsentlige og vigtige enheder til at foretage hændelsesunderretning, som i det væsentlige svarer til forpligtelserne i NIS 1-direktivet.

Enhederne skal således uden unødigt ophold underrette deres CSIRT eller kompetente myndighed om enhver hændelse, der har væsentlig indvirkning på leveringen af enhedens tjenester. Direktivet fastsætter 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.

Henset til kriteriernes kvalitative og skønsprægede karakter, opfatterForsvarsministeriet det som hensigtsmæssigt, at der sektorvist efter behov kan fastsættes nærmere regler om, hvornår en hændelse anses for at være væsentlig, herunder ved fastsættelse af kvantitative eller i øvrigt objektivt konstaterbare kriterier vedrørende eksempelvis hændelsens varighed eller skadens omfang.

Direktivet fastsætter endvidere bestemte frister for, hvornår der skal afgives henholdsvis en tidlig varsling, en ajourføring heraf, en foreløbig rapport, eventuelt en statusrapport og en endelig rapport.

Det påhviler CSIRT'en at give enheden en tilbagemelding, herunder – såfremt det ønskes – operativ rådgivning og vejledning om mulige foranstaltninger, som enheden kan træffe for at håndtere hændelsen, og supplerende teknisk bistand.

Som noget nyt i forhold til NIS 1-direktivet pålægger NIS 2-direktivet desuden væsentlige og vigtige enheder at informere modtagerne af deres tjenester (brugerne) om væsentlige hændelser, der sandsynligvis vil påvirke leveringen af disse tjenester negativt, samt – i tilfælde af en væsentlig cybertrussel – om eventuelle modforanstaltninger, som brugerne kan træffe.

Herudover foreskriver direktivet, ligesom NIS 1-direktivet, at myndighederne 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.

Det er Forsvarsministeriets opfattelse, at det er mest hensigtsmæssigt, at den nuværende rollefordeling i forhold til at informere offentligheden videreføres, således at det som udgangspunkt er de kompetente myndigheder, der foretager dette, mens det dog ved hændelser, der kan påvirke flere sektorer eller som har grænseoverskridende karakter, er Center for Cybersikkerhed (som CSIRT), der informerer offentligheden.

Det forudsættes, at offentligheden vil blive informeret på en måde, som ikke kompromitterer fortrolige oplysninger.

### 3.3.3. Den foreslåede ordning

Det foreslås, at NIS 2-direktivets regler i artikel 23 vedrørende hændelsesrapporteringer minimumsimplementeres 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.

Det foreslås således, at der fastsættes rapporteringsforpligtelser, som i deres indhold svarer til NIS 2-direktivets artikel 23.

Det foreslås på den baggrund, 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 foreslås endvidere, at vedkommende ressortminister bemyndiges til – efter forhandling med forsvarsministeren – inden for sit område at fastsætte nærmere regler om, hvornår en hændelse anses for at være væsentlig. Reglerne vil nærmere kunne præcisere, hvornår der i de enkelte sektorer skal foretages underretning. Formålet med reglerne vil dermed være i videst muligt omfang at kunne fjerne fortolkningstvivl. Ved at fastsætte reglerne i sek-

torvise bekendtgørelser, kan der tages de fornødne hensyn til særlige forhold, som måtte gøre sig gældende i de enkelte sektorer. Det foreslås, at reglerne udstedes efter forhandling med forsvarsministeren, navnlig for i videst muligt omfang at sikre ensartethed under hensyn til de sektorspecifikke forhold.

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 Center for Cybersikkerhed i centerets funktion som CSIRT og centralt kontaktpunkt, der vil kunne informere offentligheden om den væsentlige hændelse.

Forud for orientering af offentligheden foreslås det, at den relevante kompetente myndighed eller CSIRT'en hører den væsentlige eller vigtige enhed, der har underrettet om hændelsen, herunder med henblik på vurdering af, hvilke oplysninger der må betragtes som fortrolige. En kompetent myndighed eller CSIRT'en skal desuden ved overvejelse om orientering af offentligheden om en hændelse sikre, at de hensyn til fortrolighed, der fremgår af 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.

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 myndighederne anser for fortrolige – og som dermed ikke skal offentliggøres.

Der henvises i øvrigt til bemærkningerne til de foreslåede §§ 12, 13 15 og 16.

## 3.4. Tilsyn og håndhævelse

### 3.4.1. Gældende ret

Der er i NIS 1-direktivets artikel 15 og 17 fastsat 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 regulering gældende for de specifikke sektorer, hvor direktivet finder anvendelse, jf. afsnit 2.4 ovenfor.

### 3.4.2. Forsvarsministeriets overvejelser

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

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. Medlemsstaterne kan dog tillade, at de kompetente myndigheder prioriterer deres tilsynsopgaver baseret på en risikobaseret tilgang.

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. Det er således i direktivet 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 således, 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 hvis der fremkommer oplysninger 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.

Direktivet oplister herudover de tilsynsforanstaltninger, 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 tilsynsforanstaltninger for henholdsvis væsentlige og vigtige enheder er i vidt omfang identiske, idet direktivets forudsætning om en differentieret tilgang til tilsynet med væsentlige og vigtige enheder dog afspejler sig i visse forskelle i de foranstaltninger, der som minimum skal kunne anvendes. Mens direktivet eksempelvis foreskriver, at myndighederne skal kunne foretage stikprøvekontrol med væsentlige enheder, gør dette sig ikke 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.

Direktivet oplister endvidere 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 overfor henholdsvis væsentlige og vigtige enheder er i vidt omfang identiske, idet væsentlige enheder dog som noget særligt kan pålægges at udpege en monitoreringsansvarlig med veldefinerede opgaver til i en nærmere fastsat periode at føre tilsyn med de pågældende enheders overholdelse af kravene til foranstaltninger til styring af cybersikkerhedsrisici og underretningsforpligtelser.

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.

#### 3.4.2.1. Særligt om midlertidige suspensioner

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

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 Forsvarsministeriets 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 forsvarsministeren – 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 Forsvarsministeriets 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. 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.

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 Forsvarsministeriets opfattelse, at det er mest hensigtsmæssigt, at 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 i første omgang træffes af den relevante kompetente myndighed, der vil kunne belyse og begrunde, hvorfor indgrebet vurderes påkrævet.

Der er i dag i f.eks. fødevarelovens § 52 b mulighed for, at fødevarevirksomheder, der overtræder fødevarelovgivningen eller forordningen, der regulerer fødevareforhold, gentagne gange på en sådan måde, at der er nærliggende risiko for, at virksomheden fortsat ikke vil blive drevet i overensstemmelse med reglerne, kan blive forbudt fortsat drift af den pågældende virksomhed i indtil seks måneder. Efter bestemmelsen i § 52 b, stk. 3, kan den, som afgørelsen vedrører, forlange sagen indbragt for domstolene.

På tilsvarende måde som efter reglerne i fødevarelovens § 52 b, er det Forsvarsministeriets 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.

Ud fra et hensyn til de berørte personer og enheder finder Forsvarsministeriet, at der ikke bør stilles krav om, at muligheden for administrativ rekurs skal være udnyttet, før sagen kan forlanges indbragt for retten. De berørte personer eller enheder bør således kunne vælge, om de vil anmode om, at sagen indbringes for retten med det samme, eller om de først ønsker at påklage afgørelsen.

Det vil være op til vedkommende ressortminister at beslutte, hvilken myndighed der skal indbringe sagen for retten og varetage de sædvanlige partsbeføjelser i sagen. Den enkelte minister vil eksempelvis kunne bemyndige den kompetente myndighed eller en eventuel rekursmyndighed på området til at indbringe sagen for retten.

### 3.4.3. Den foreslåede ordning

Det foreslås, at NIS 2-direktivets regler i artikel 31-33 vedrørende tilsyn og håndhævelse minimumsimplementeres 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.

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 forudsatte 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 rent 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 forsvarsministeren 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, jf. den foreslåede bestemmelse i § 23, stk. 1.

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.

Der vil inden for rammerne af de almindelige forvaltningsretlige principper om administrativ rekurs være adgang til at påklage en afgørelse om midlertidig suspension eller et midlertidigt forbud mod, at fysiske personer må udøve ledelsesfunktioner.

Det foreslås endvidere, 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. Det er ikke et krav, at muligheden for administrativ rekurs forinden er udnyttet.

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 §§ 21-26.

## 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. Forsvarsministeriets 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.

Sanktionerne skal være effektive, stå i et rimeligt forhold til overtrædelsen og have afskrækkende virkning.

NIS 2-direktivets artikel 34 indeholder herudover regler om de generelle betingelser for pålæggelse af administrative bøder til væsentlige og vigtige enheder.

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

Indførelsen 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 Forsvarsministeriets 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 Forsvarsministeriets 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, 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 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.

Efter NIS 2-direktivets artikel 34, stk. 5, skal vigtige enheders overtrædelse af direktivets artikel 21 (foranstaltninger til styring af cybersikkerhedsrisici) eller artikel 23 (rapporteringsforpligtelser) straffes med et maksimum på mindst 7.000.000 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.

I dansk strafferet gælder der typisk ikke noget lovbestemt maksimum for bødestrørrelser. Ud fra et hensyn til at minimumsimplementere NIS 2-direktivet er det Forsvarsministeriets opfattelse, at der bør fastsættes maksimale bødeniveauer svarende til de niveauer, der er fastsat i direktivet. Dermed vil virksomheder og myndigheder ikke kunne straffes med højere bøder, end det der er forudsat i direktivet.

#### 3.5.2.1. Særligt om den offentlige forvaltning

Det følger af NIS 2-direktivets artikel 34, stk. 7, at hver enkelt medlemsstat kan fastsætte regler om, hvorvidt og i hvilket omfang (administrative) bøder kan 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.

Efter Forsvarsministeriets opfattelse bør der i lovforslaget indsættes en bemyndigelse til, at digitaliserings- og ligestillingsministeren kan fastsætte regler om, at offentlige myndigheder og institutioner m.v., som er omfattet af forvaltningslovens § 1, stk. 1 eller 2, uanset straffelovens § 27, stk. 2, kan straffes i anledning af overtrædelser, der begås ved udøvelse af virksomhed, der ikke svarer til eller kan sidestilles med virksomhed udøvet af private.

Dette vil medføre, at der i en bekendtgørelse kan fastsættes regler om, at offentlige myndigheder – uanset det generelle princip i straffelovens § 27, stk. 2 – kan straffes efter de foreslåede straffebestemmelser i lovforslaget på samme måde som private aktører.

Det er Forsvarsministeriets vurdering, at der i givet fald bør kunne fastsættes regler om særskilte bødelofter for offentlige myndigheders overtrædelse af denne lov.

#### 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.

Efter retsplejelovens § 997, stk. 3, kan der i domme, hvorved nogen tilpligtes at opfylde en forpligtelse mod det offentlige, som tvangsmiddel fastsættes en fortløbende bøde, der tilfalder statskassen (tvangsbøder).

Det følger således allerede af de almindelige regler i retsplejeloven, at domstolene kan pålægge tvangsbøder for at få nogen til at opfylde en forpligtelse mod det offentlige.

Administrative tvangsbøder er derimod tvangsbøder, som ikke pålægges af domstolene, men af forvaltningen. En administrativ tvangsbøde er således en afgørelse om, at en økonomisk sanktion vil blive pålagt, hvis en handlepligt ikke opfyldes – f.eks. et påbud eller en pligt til at udlevere bestemte oplysninger.

Sådanne bøder kan ofte opfattes som en straf, og der er ikke samme retssikkerhedsgarantier som tvangsbøder pålagt af domstolene. Det antages derfor normalt i dansk ret, at der kun bør gives hjemmel til administrative tvangsbøder, hvis der foreligger et helt særligt behov for effektiv kontrol og håndhævelse på det pågældende område. Endvidere bør de forhold, der udløser tvangsbøderne, være let konstaterbare.

Forsvarsministeriet er på den baggrund tilbageholdende med at foreslå, at der 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.

Forsvarsministeriet vurderer som udgangspunkt, at de retsmidler, der foreslås med denne lov, herunder tilsyns- og håndhævelsesforanstaltningerne samt muligheden for at offentliggøre afgørelser m.v., 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, herunder valg af 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 sikrer, at enhver fysisk person, der er ansvarlig for eller optræder som juridisk repræsentant for en væsentlig enhed på grundlag af beføjelsen til at repræsentere den, beføjelsen til at træffe afgørelser på dennes vegne eller beføjelsen til at udøve kontrol over den, har beføjelse til at sikre, at den overholder NIS 2-direktivet. Medlemsstaterne sikrer, at det er muligt at drage sådanne fysiske personer til ansvar for tilsidesættelse af deres forpligtelser til at sikre 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 insitutioner, samt ansvaret for embedsmænd og personer valgt eller udnævnt til offentlige hverv, jf. bestemmelsens 2. led.

Efter Rigsadvokatmeddelelse CIR1H nr. 11550 af 17. april 2015 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).

Forsvarsministeriet 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 Forsvarsministeriets 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 for-

anstaltninger til styring af cybersikkerhedsrisici) og artikel 23 (om rapporteringsforpligtelser), 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 persondatasikkerheden, er bestemmelsen i NIS 2-direktivets artikel 35, stk. 2, udtryk for det almindelige forbud mod dobbelt strafforfølgning. Det anføres således i præambelbetragtning nr. 131, at pålæggelse af sanktioner for overtrædelse af de nationale regler, der gennemfører NIS 2-direktivet, ikke bør føre til et brud på princippet om *ne bis in idem* som fortolket af Den Europæiske Unions Domstol.

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

For at sikre, at myndighederne har mulighed for at undgå, at den samme adfærd straffes dobbelt, forpligter NIS 2-direktivets artikel 35, stk. 1, de kompetente myndigheder efter NIS 2-direktivet til uden unødigt ophold at underrette tilsynsmyndighederne efter databeskyttelsesforordningen – 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.

Forsvarsministeriet bemærker i forlængelse heraf, at det af databeskyttelsesforordningens artikel 4, nr. 12, følger, at »brud på persondatasikkerheden« er defineret som et brud på sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til

personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet. Bestemmelsen i forordningens artikel 33, stk. 1, indebærer, at den dataansvarlige skal anmelde et brud på persondatasikkerheden til Datatilsynet, »medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder«.

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

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 NIS 2-direktivets regler i artikel 34-36 vedrørende sanktioner minimumsimplementeres 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, idet der dog lægges op til, at offentlige myndigheder skal kunne pålægges bøder for manglende efterlevelse af NIS 2-reguleringen.

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, §§ 7, 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 eller 25, 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 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 m.v. (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 afsnit 3.5.2 ovenfor.

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

For så vidt angår offentlige myndigheder foreslås det, at råderummet i direktivet, hvorefter medlemsstaterne kan bestemme, »i hvilket omfang« offentlige forvaltningsorganer kan pålægges (administrative) bøder, vil kunne anvendes ved, at digitaliserings- og ligestillingsministeren bemyndiges til at fastsætte regler om, at offentlige myndigheder og institutioner m.v., som er omfattet af forvaltningslovens § 1, stk. 1 eller 2, uanset straffelovens § 27, stk. 2, kan straffes i anledning af overtrædelser, der begås ved udøvelse af

virksomhed, der ikke svarer til eller kan sidestilles med virksomhed udøvet af private. Såfremt bemyndigelsen anvendes, vil dette medføre, at offentlige myndigheder – uanset det generelle princip i straffelovens § 27, stk. 2, – kan straffes efter de foreslåede straffebestemmelser i lovforslaget på samme måde som private aktører.

Det bemærkes, at offentlige myndigheder, uanset om den foreslåede bemyndigelse udnyttes, i overensstemmelse med det almindelige udgangspunkt vil kunne straffes for overtrædelser, der begås ved udøvelse af virksomhed, der svarer til eller kan sidestilles med virksomhed udøvet af private.

Det foreslås endvidere, at digitaliserings- og ligestillingsministeren bemyndiges til at fastsætte regler om særskilte bødelofter for offentlige myndigheders overtrædelse af denne lov.

Det vil i de nærmere regler – i overensstemmelse med retsstillingen efter databeskyttelsesloven – eksempelvis kunne fastsættes, at bødelofterne for offentlige myndigheder skal være lavere end dem, der i øvrigt er fastsat for private virksomheder. I databeskyttelsesloven er der eksempelvis for visse overtrædelser forudsat et bødeloft på 2 pct. af myndighedens driftsbevilling, dog maksimalt 8 mio. kr. For andre overtrædelser er der forudsat et bødeloft på 4 pct. af driftsbevillingen, dog maksimalt 16 mio. kr.

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

## 4. Økonomiske konsekvenser og implementeringskonsekvenser for det offentlige

### 4.1. Økonomiske konsekvenser og implementeringskonsekvenser for det offentlige

Efter lovforslaget vil statslige myndigheder og efter omstændighederne regionerne 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.

De nærmere krav til foranstaltninger til styring af cybersikkerhed vil i medfør af den foreslåede bestemmelse i § 6, stk. 3, blive fastsat i sektorspecifikke bekendtgørelser. Da de nærmere økonomiske konsekvenser ved foranstaltningerne til styring af cybersikkerhedsrisici vil afhænge af det nærmere indhold af bekendtgørelserne, 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 2 og 3.

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.

### 4.2. De syv principper for digitaliseringsklar lovgivning

Det er Forsvarsministeriets opfattelse, at lovforslaget er i overensstemmelse med principperne for digitaliseringsklar lovgivning.

Det Forsvarsministeriets 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 Forsvarsministeriets 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 Forsvarsministeriets 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 Forsvarsministeriets opfattelse, at de øvrige principper ikke er relevante for lovforslaget.

**5. Økonomiske og administrative konsekvenser for erhvervslivet m.v.**

Lovforslaget indebærer, at loven vil finde anvendelse på virksomheder, der opererer i Danmark og er omfattet af lovens bilag 2 eller 3, såfremt virksomhederne er af en vis størrelse. Som udgangspunkt omfattes således kun mellemstore og store virksomheder. Lovforslaget indebærer desuden, at loven også vil finde anvendelse på bestemte typer virksomheder uanset deres størrelse. Lovens anvendelsesområde er nærmere beskrevet i lovforslagets §§ 1 og 2 og de specielle bemærkninger hertil.

Lovforslaget forventes at medføre negative erhvervsøkonomiske konsekvenser. 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.

Det er vanskeligt at estimere de erhvervsøkonomiske konsekvenser på nuværende tidspunkt, da der er betydelig usikkerhed om både population og

effekter af de kommende krav. Gennemførelsen af NIS 2-direktivet i dansk ret vurderes dog – samlet set – at få væsentlige erhvervsøkonomiske konsekvenser.

Lovforslagets mest centrale krav – herunder navnlig kravene til foranstaltninger til styring af cybersikkerhedsrisici i medfør af lovforslagets § 6, stk. 3 – konkretiseres yderligere i bekendtgørelser. En sådan konkretisering vil muliggøre en kvantificering af virksomhedernes omkostninger. Det følger af Erhvervsministeriets Vejledning om Erhvervsøkonomiske Konsekvensvurderinger, at såfremt et lovforslag kun udstikker rammerne for reguleringen og giver hjemmel til fastsættelse af nærmere regler i bekendtgørelser, kan kvantificeringen finde sted på bekendtgørelsesniveau. Det vil også være på dette tidspunkt, at der i givet fald skal udarbejdes egentlige AMVAB-målinger af de administrative omkostninger ved bekendtgørelserne. I forhold til lovforslaget bør konsekvensvurderingen dog i videst muligt omfang inkludere de forventede endelige konsekvenser for erhvervslivet – dvs. inklusive konsekvenserne efter eventuel sekundær regulering. Derfor følger nedenfor et foreløbigt estimat for virksomheders forventede omkostninger baseret på en analyse af ENISA.

De erhvervsøkonomiske omkostninger følger navnlig af NIS 2-direktivets udvidelse af dækningsområdet i forhold til NIS 1-direktivet, hvorved flere virksomheder omfattes. Dermed vil flere virksomheder skulle leve op til direktivets krav.

Der er ikke på nuværende tidspunkt et fuldt overblik over, hvor mange danske virksomheder som vil blive omfattet af lovforslaget. Et indledende estimat viser, at omkring 2.000 virksomheder kan blive omfattet. En nærmere vurdering heraf vil blive foretaget i forbindelse med det videre implementeringsarbejde, bl.a. ved udarbejdelsen af de sektorspecifikke bekendtgørelser i medfør af nærværende lovforslag. Det vurderes, at ca. 150 danske virksomheder allerede er omfattet af NIS 1-direktivet og derved efterlever en del af de krav, der følger af NIS 2-direktivet. Dette tal vil ligeledes skulle efterprøves i den endelige kvantificering.

Europa-Kommissionens konsekvensvurdering fra december 2020 angiver, at en gennemsnitlig virksomhed skal bruge 22-25% af sine nuværende omkostninger til it-sikkerhed på at omstille sig til kravene i NIS 2-direktivet. Tallet er 12-15% for virksomheder, der allerede er omfattet af NIS 1-direktivet. Europa-Kommissionens konsekvensvurdering indeholder ikke en kvantificering af de løbende omkostninger.

Den Europæiske Unions Agentur for Cybersikkerhed, ENISA, har i sin rapport "NIS Investment" fra november 2022 angivet, at danske virksomheder

(som median) har omkostninger til it-sikkerhed på 825.000 euro pr. virksomhed. Med udgangspunkt i ovenstående estimater fra ENISA og Europa-Kommissionen, kan de erhvervsøkonomiske konsekvenser ved gennemførelsen af NIS 2-direktivet i dansk ret foreløbigt estimeres i et spænd på ca. 2,6 mia. kr. til ca. 3 mia. kr. i omstillingsomkostninger. Der foreligger endnu ikke tilstrækkelige oplysninger til at lave et foreløbigt skøn over de samlede løbende erhvervsøkonomiske omkostninger.

| It-omkostninger til It-sikkerhed pr. virksomhed | Procentsats | Omkostning til efterlevelse af NIS 2 krav, pr. virksomhed | Population | Foreløbigt estimat for samlede erhvervsøkonomiske omstillingsomkostninger |
|---|---|---|---|---|
| Scenarie 1 | | | | |
| 6.154.500 kr.* | 12% | 738.540 kr. | 150 | 110.781.000 kr. |
| 6.154.500 kr. | 22% | 1.353.990 kr. | 1850 | 2.504.881.500 kr. |
| | | | | **2.615.662.500 kr.** |
| Scenarie 2 | | | | |
| 6.154.500 kr. | 15% | 923.175 kr. | 150 | 138.476.250 kr. |
| 6.154.500 kr. | 25% | 1.538.625 kr. | 1850 | 2.846.456.250 kr. |
| | | | | **2.984.932.500 kr.** |

*825.000 euro ved kurs 7,46 kr.

Der vil blive arbejdet på en yderligere kvantificering af lovforslagets erhvervsøkonomiske konsekvenser frem mod fremsættelsen af lovforslaget.

Innovations- og Iværksættertjekket vurderes ikke at være relevant for lovforslaget, fordi forslaget ikke påvirker virksomheders eller iværksætteres muligheder for at teste, udvikle og anvende nye teknologier og innovation.

## 6. Administrative konsekvenser for borgerne

Lovforslaget vurderes ikke at have administrative konsekvenser for borgerne.

## 7. Miljømæssige konsekvenser

Lovforslaget vurderes ikke at have konsekvenser for klima, miljø eller natur.

## 8. Forholdet til databeskyttelsesretten

Behandling af personoplysninger er i almindelighed reguleret i databeskyttelsesforordningen og databeskyttelsesloven.

Spørgsmålet om, hvorvidt der må behandles personoplysninger, er i dag som udgangspunkt reguleret i databeskyttelsesforordningens artikel 6, stk. 1 (om behandling af almindelige personoplysninger), artikel 9, stk. 2 (om behandling af følsomme personoplysninger), og artikel 10 (om behandling af personoplysninger vedrørende straffedomme og lovovertrædelser).

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.

Der kan således indgå almindelige personoplysninger i de oplysninger, som enhederne som led i overholdelsen af registreringsforpligtelserne i de foreslåede bestemmelser i §§ 9 og 10 skal indgive til de kompetente myndigheder, eksempelvis i form af visse kontaktoplysninger på medarbejdere hos enheden.

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.

Derudover kan der indgå almindelige personoplysninger i en enheds hændelsesunderretning til myndighederne i medfør af den foreslåede underretningspligt i §§ 12 og 13. 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 blive behandlet almindelige personoplysninger. Det er Forsvarsministeriets 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 følger af NIS 2-direktivets artikel 2, stk. 14, 1. led, at enheder, de kompetente myndigheder, de centrale kontaktpunkter og CSIRT'erne behandler personoplysninger i det omfang, det er nødvendigt med henblik på dette direktiv og i overensstemmelse med databeskyttelsesforordningen, navnlig på grundlag af artikel 6 deri.

Det er Forsvarsministeriets opfattelse, at behandling af almindelige personoplysninger i forbindelse med overholdelsen af registreringsforpligtelserne i §§ 9 og 10 og underretningsforpligtelserne i §§ 12 og 13, samt i forbindelse med 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. Det følger af artikel 6, stk. 1, litra c, at behandling er lovlig, hvis den er nødvendig for at overholde en retlig forpligtelse, som påhviler den dataansvarlige, ligesom det følger af litra e, at behandling er lovlig, hvis den er nødvendig af hensyn til udførelse af en opgave i samfundets interesse. Det er endvidere Forsvarsministeriets opfattelse, at behandlingen af almindelige personoplysninger kan ske i medfør af databeskyttelsesforordningens artikel 6, stk. 1, litra f. Det følger af denne bestemmelse, at behandling er lovlig, hvis den er nødvendig for, at den dataansvarlige eller en tredjemand kan forfølge en legitim interesse, medmindre den registreredes interesser eller grundlæggende rettigheder og frihedsrettigheder, der kræver beskyttelse af personoplysninger, går forud herfor, navnlig hvis den registrerede er et barn.

For så vidt angår offentlige myndigheder henvises der til forordningens artikel 6, stk. 1, litra e, hvorefter behandling bl.a. er lovlig, hvis behandlingen er nødvendig af hensyn til udførelse af en opgave i samfundets interesse.

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

Center for Cybersikkerhed varetager opgaverne som centralt kontaktpunkt og national CSIRT.

Navnlig vil opgaven som national CSIRT indebære, at Center for Cybersikkerhed 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 centeret 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 centeret vil få adgang til disse oplysninger. Det bemærkes i den forbindelse, at centerets 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, og § 3, stk. 2, i databeskyttelsesloven, at centerets virksomhed er undtaget databeskyttelsesloven og databeskyttelsesforordningen. Uanset at Center for Cybersikkerheds virksomhed er undtaget fra databeskyttelseslovgivningen, finder størstedelen af de centrale principper i databeskyttelseslovgivningen anvendelse på Center for Cybersikkerhed 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 centerets bistand i medfør af den foreslåede § 17.

Center for Cybersikkerhed er som nævnt ikke omfattet af de databeskyttelsesretlige regler, hvorfor centeret heller ikke er omfattet af begrebet "dataansvarlig" i databeskyttelsesforordningen og databeskyttelsesloven. Centeret vil dog i relation til de væsentlige og vigtige enheder være at betragte som en selvstændig dataansvarlig for den behandling af personoplysninger, som centeret udfører. I tilfælde af, at Center for Cybersikkerhed som CSIRT 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.

I relation til almindelige personoplysninger henvises der for så vidt angår private virksomheder til databeskyttelsesforordningens artikel 6, stk. 1, litra f. Det følger af denne bestemmelse, at behandling er lovlig, hvis den er nødvendig for, at den dataansvarlige eller en tredjemand kan forfølge en legitim interesse, medmindre den registreredes interesser eller grundlæggende rettigheder og frihedsrettigheder, der kræver beskyttelse af personoplysninger,

går forud herfor, navnlig hvis den registrerede er et barn. Det fremgår i den forbindelse af databeskyttelsesforordningens præambelbetragtning 49, at behandling af personoplysninger – i det omfang, det er strengt nødvendigt og forholdsmæssigt for at sikre net- og informationssikkerheden – der foretages af eksempelvis Computer Emergency Response Teams (CERT'er), udgør en legitim interesse for den berørte dataansvarlige.

For så vidt angår en situation, hvor de offentlige myndigheder, der er omfattet af direktivet, herunder de kompetente myndigheder, videregiver oplysninger til Center for Cybersikkerhed som CSIRT, henvises der til forordningens artikel 6, stk. 1, litra e, hvorefter behandling bl.a. er lovlig, hvis behandlingen er nødvendig af hensyn til udførelse af en opgave i samfundets interesse. Henset til at videregivelsen er nødvendig af hensyn til udførelsen af Center for Cybersikkerheds opgave som CSIRT og centralt kontaktpunkt, vurderer Forsvarsministeriet, at videregivelse af almindelige personoplysninger til Center for Cybersikkerhed er omfattet af forordningens artikel 6, stk. 1, litra e.

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 Center for Cybersikkerhed.

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. Forsvarsministeriet har ved vurderingen lagt vægt på, at Center for Cybersikkerhed som CSIRT bl.a. har til opgave at overvåge og analysere cybertrusler, sårbarheder og hændelser på nationalt plan, samt at reagere på hændelser. Forsvarsministeriet har endvidere lagt vægt på, at centerets 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. Forsvarsministeriet 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 Center for Cybersikkerheds udførelse 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 Center for Cybersikkerhed.

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. Forsvarsministeriet 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.

## 9. 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 skal 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 lidt over fire måneder efter direktivets implementeringsfrist.

## 10. Hørte myndigheder og organisationer m.v.

Et udkast til lovforslag har i perioden fra den [xx] til den [xx] været sendt i høring hos følgende myndigheder og organisationer m.v.:

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, De Samvirkende Købmænd, Danish e-infrastructure consortium, 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, Rigsrevisionen, Rådet for Digital Sikkerhed, Samtlige byretspræsidenter, SMVdanmark, Statsadvokaten i København og Statsadvokaten i Viborg.

## 11. 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 esti- |

| | | |
|---|---|---|
| | | meres med betydelig usikkerhed at udgøre ca. 105-147 mio. kr. årligt.<br><br>Derudover estimeres der med betydelig usikkerhed at være udgifter i regionerne på 63-100 mio. kr. årligt.<br><br>I det omfang kommunerne omfattes af lovforslaget estimeres der 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 (i det omfang de er omfattet af lovforslaget) skal overholde lovens forpligtelser. Disse forpligtelser vil bl.a. omfatte registrerings- og underretningsforpligtelserne i lovens §§ 9, 10 og 12.<br><br>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. |
| Økonomiske konsekvenser for erhvervslivet | Ingen. | Det er vanskeligt at stimere de erhvervsøkonomiske konsekvenser på nuværende tidspunkt. |

| | | |
|---|---|---|
| | | På baggrund af Europa-Kommissionens konsekvensvurdering fra december 2020 og rapporten "NIS Investment" udgivet af Den Europæiske Unions Agentur for Cybersikkerhed, kan de erhvervsøkonomiske konsekvenser ved gennemførelsen af NIS 2-direktivet i dansk ret foreløbigt estimeres i et spænd på ca. 2,6 mia. kr. til 3 mia. kr. i omstillingsomkostninger. Der foreligger ikke oplysninger ift. de løbende omkostninger. |
| Administrative konsekvenser for erhvervslivet | Ingen. | Lovforslaget forventes at medføre negative implementeringskonsekvenser for erhvervslivet, da virksomheder, organisationer mv., da de (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 og 12.<br><br>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. |
| Administrative konsekvenser for borgerne | Ingen. | Ingen. |

| | | |
|---|---|---|
| Miljømæssige konsekvenser | Ingen. | Ingen. |
| Forholdet til EU-retten | Loven og de bekendtgørelser, der vil blive udstedt i medfør af loven, gennemfører dele af Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022 om foranstaltninger til sikring af et højt cybersikkerhedsniveau i hele Unionen, om ændring af forordning (EU) nr. 910/2014 og direktiv (EU) 2018/1972 og om ophævelse af direktiv (EU) 2016/1148 (NIS 2-direktivet). Der henvises til EU-tidende 2022, L nr. 333, side 80. Direktivet er medtaget som bilag 1 til loven. | |
| Er i strid med de principper for implementering af erhvervsrettet EU-regulering/Går videre end minimumskrav i EU-regulering (sæt X) | Ja | Nej<br><br>X |

*Bemærkninger til lovforslagets enkelte bestemmelser*

*Til § 1*

I dag er net- og informationssikkerhed reguleret 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). NIS 1-direktivet omfatter 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.

INIS 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 den foreslåede *§ 1, stk. 1,* at loven finder anvendelse på offentlige og private enheder, der er omfattet af anvendelsesområdet i artikel 2 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), jf. dog stk. 2-7 og § 2.

Forsvarsministeriet har lagt 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.

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 § 1, stk. 2-7, og set i lyset af jurisdiktionsbestemmelsen i § 2. 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. 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. Direktivets bilag I og II fremgår af lovens bilag 1.

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.

NIS 2-direktivets artikel 2, stk. 1, indebærer, at enhederne som udgangspunkt mindst skal udgøre mellemstore virksomheder, som defineret i Eu-

ropa-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.

Af artikel 2 i 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.

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 leve op til størrelseskravet i NIS 2-direktivets artikel 2, stk. 1, skal enhederne således beskæftige mindst 50 personer og have en årlig omsætning eller en samlet årlig balance på over 10 mio. euro.

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

I overensstemmelse med principperne i den nævnte præambelbetragtning vil visse enheder efter omstændigehederne, kunne anses for ikke at leve op til 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 artikels stk. 1. Dette vil 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 enhe-

dernes 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.

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 ved en forvaltningsakt kunne konstatere, hvorvidt enheden er omfattet af lovens anvendelsesområde. Det bemærkes i denne forbindelse, at de kompetente myndigheder 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 finder anvendelse på enheder i energisektoren. Loven finder endvidere ikke anvendelse på enheder i det omfang, de er omfattet af lov om cybersikkerhed i telesektoren eller er udpeget i medfør af § 333, stk. 1, i lov om finansiel virksomhed. Dog gælder lovens § 17 for disse enheder.

Baggrunden for denne bestemmelse er, at NIS 2-direktivet gennemføres ved særskilt regulering for henholdsvis tele-, energi- og finanssektorerne.

Den foreslåede § 17 fastsætter CSIRT'ens opgaver over for væsentlige og vigtige enheder. Center for Cybersikkerhed varetager funktionen som CSIRT for enheder i alle sektorer, herunder også energi-, tele- og finanssektorerne.

Bestemmelsen indebærer således, at enheder i energisektoren samt enheder, der omfattes af lov om cybersikkerhed i telesektoren, eller som udpeges i medfør af § 333, stk. 1, i lov om finansiel virksomhed, generelt ikke vil være omfattet af nærværende lov, idet Center for Cybersikkerhed dog i medfør af lovens § 17 vil varetage funktionen som CSIRT også for disse enheder.

Ved enheder i energisektoren forstås enheder, der er omfattet af sektor 1, i bilag I til NIS 2-direktivet, dvs. sektoren »Energi« med delsektorerne: a) Elektricitet, b) fjernvarme og fjernkøling, c) olie, d) gas og e) brint.

I telesektoren vil enheder i enhedskategorierne »udbydere af offentlige elektroniske kommunikationsnet« og »udbydere af offentligt tilgængelige elektroniske kommunikationstjenester«, i sektoren »Digital infrastruktur« i bilag I til NIS 2-direktivet, som udgangspunkt blive omfattet af lov om cybersikkerhed i telesektoren. I det omfang kommuner og regioner måtte udbyde offentlige elektroniske kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester, vil de imidlertid være omfattet af nærværende lov.

I finanssektoren vil udbydere af datacentertjenester blive omfattet af lov om finansiel virksomhed i det omfang, de udpeges i medfør af lovens § 333, stk. 1. Indtil en sådan udpegning i givet fald måtte ske, vil de pågældende udbydere af datacentertjenester være omfattet af nærværende lov.

I tilfælde, hvor en enhed indgår i flere sektorer i direktivets bilag, og det alene er den ene sektor, der er omfattet af den foreslåede bestemmelse i stk. 2, 1. pkt., vil enheden fortsat være omfattet af denne lovs bestemmelser for så vidt angår enhedens aktiviteter i de øvrige sektorer.

Det følger af det foreslåede *stk. 3*, at vedkommende minister inden for sit område kan bestemme, at loven helt eller delvist 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.

Forsvarsministeriet har lagt vægt på, at der foretages en direktivnær minimumsimplementering. Den foreslåede bestemmelse svarer indholdsmæssigt til NIS 2-direktivets artikel 4, stk. 1, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Den foreslåede bestemmelse indebærer, at det vil være op til vedkommende minister inden for sit område at bestemme, om – og i givet fald i hvilket omfang – der skal gøres undtagelse fra hele eller dele af nærværende lov med henvisning til EU-retsakter og eventuel national gennemførelse heraf. I overensstemmelse med direktivets artikel 4, stk. 2, vil der 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 direktivets 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).

Forsvarsministeriet har lagt vægt på, at der foretages en direktivnær minimumsimplementering. Den foreslåede bestemmelse svarer indholdsmæssigt til NIS 2-direktivets artikel 2, stk. 8, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

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 og 8 (foranstaltninger til styring af cybersikkerheden) og §§, 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 m.v., 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 handlin-

ger, der derfor vil kunne undtages fra forpligtelserne i §§ 6 og 8 (foranstaltninger til styring af cybersikkerheden) og §§ 12, 13, 15 og 16 (oplysnings- og underretningspligter).

Det er Forsvarsministeriets opfattelse, at det forhold, at en enhed »udelukkende leverer tjenester« til forvaltningsenheder, der udfører ovenfor nævnte aktiviteter, indebærer, at de 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 stk. 4 ikke finder anvendelse, hvor en enhed fungerer som tillidstjenesteudbyder.

Den foreslåede bestemmelse vil gennemføre NIS 2-direktivets artikel 2, stk. 9.

Forsvarsministeriet har lagt vægt på, at der foretages en direktivnær minimumsimplementering. Den foreslåede bestemmelse svarer indholdsmæssigt til NIS 2-direktivets artikel 2, stk. 9, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Det følger af det foreslåede *stk. 6,* at offentlige og private enheder, uanset om de er omfattet af lovens anvendelsesområde, kan give frivillig underretning til CSIRT'en efter § 14 og deltage i den frivillige udveksling af oplysninger mellem enheder i cybersikkerhedsfællesskaber efter § 19.

Efter den foreslåede bestemmelse i § 14 kan offentlige og private enheder underrette CSIRT'en om hændelser, der negativt påvirker eller vurderes at kunne påvirke tilgængeligheden, integriteten eller fortroligheden af data, informationssystemer, digitale netværk eller digitale servicer.

Efter den foreslåede bestemmelse i § 19 faciliterer CSIRT'en, at der på frivillig basis kan ske udveksling af oplysninger mellem enheder i cybersikkerhedsfællesskaber.

Den foreslåede bestemmelse i stk. 6 indebærer, at enheder, der ellers ikke ville være omfattet af lovens anvendelsesområde, har mulighed for at give frivillig underretning til CSIRT'en om hændelser og for på frivillig basis at deltage i de cybersikkerhedsfællesskaber, som CSIRT'en faciliterer, herunder udveksle oplysninger med andre deltagende enheder.

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

Det følger af det foreslåede *stk. 7*, at vedkommende minister inden for sit område 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 Forsvarsministeriets opfattelse, at forvaltningsenheder på lokalt plan i Danmark hovedsageligt skal forstås som kommuner og lokale folkekirkelige myndigheder, dvs. menighedsråd og provstiudvalg. Det er på nuværende tidspunkt ikke intentionen at fastsætte regler om, at kommunerne og lokale folkekirkelige myndigheder omfattes af loven.

For så vidt angår uddannelsesinstitutioner forventes det primært at være aktuelt at sætte reglerne i kraft for universiteter omfattet af universitetsloven, jf. lovbekendtgørelse nr. 778 af 7. august 2019. Det kan dog ikke udelukkes, at loven også vil blive sat i kraft for andre videregående uddannelsesinstitutioner i det omfang, 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. 7 ikke er udnyttet. Dette vil eksempelvis kunne være tilfældet i en situation, hvor en

kommune agerer som sundhedstjenesteyder i overensstemmelse med lovforslagets bilag 2. I denne situation vil kommunen kunne være omfattet af lovens anvendelsesområde på baggrund af disse aktiviteter, også selvom bemyndigelsen i det foreslåede stk. 7 ikke er udnyttet. Den foreslåede bestemmelse i stk. 7 vil således alene være relevant, hvis man måtte ønske at omfatte offentlige forvaltningsenheder på lokalt plan eller uddannelsesinstitutioner, som følge af andre aktiviteter eller tjenester end dem, der er oplistet i direktivets bilag.

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

*Til § 2*

Det følger af artikel 18, 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 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 III 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 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 den foreslåede *§ 2, 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 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 fremgår heraf, at enheder, der er omfattet af direktivets anvendelsesområde, anses for at henhøre under jurisdiktionen i den medlemsstat, hvor de er etableret.

Forsvarsministeriet har lagt vægt på, at der foretages en direktivnær minimumsimplementering. 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 er omfattet af lovens anvendelsesområde, og 2) enheden er etableret i Danmark. Dette udgangspunkt er dog modificeret, 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.

Forsvarsministeriet har lagt vægt på, at der foretages en direktivnær minimumsimplementering. 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.

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.

Forsvarsministeriet har lagt vægt på, at der foretages en direktivnær minimumsimplementering. 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.

I overensstemmelse med NIS 2-direktivets præambelbetragtning nr. 114 indebærer forretningsstedskriteriet, at der sker en faktisk udøvelse af virksomhed gennem faste ordninger. De pågældende ordningers juridiske form – hvorvidt der er tale om en filial eller et datterselskab med status som juridisk person – er ikke den afgørende faktor i denne forbindelse. Opfyldelsen af det nævnte kriterium bør ikke 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 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. Det følger videre af samme præambelbetragtning, at hvis tjenesterne udføres af en gruppe af virksomheder, bør den kontrollerende virksomheds hovedforretningssted anses for at være hele gruppens hovedforretningssted.

Hovedforretningsstedet vil således efter den foreslåede bestemmelse skulle anses for at være placeret i den medlemsstat, hvor enheden hovedsageligt træffer beslutning om cybersikkerhedsforanstaltninger og risikohåndtering i relation til cybersikkerheden.

Det følger af det foreslåede *stk. 4*, at er en enhed omfattet af 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. Hvis 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. Artikel 26, stk. 3, fastsætter, 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.

Forsvarsministeriet har lagt vægt på, at der foretages en direktivnær minimumsimplementering. 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.

Det følger af det foreslåede *stk. 5*, 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.

Forsvarsministeriet har lagt vægt på, at der foretages en direktivnær minimumsimplementering. 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 § 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 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).

Forsvarsministeriet har lagt vægt på, at der foretages en direktivnær minimumsimplementering. 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 *stk. 1, 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 stk. 1, *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 stk. 1, *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 stk. 1, *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 stk. 1, *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 stk. 1, *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 stk. 1, *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 stk. 1, *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 stk. 1, *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 stk. 1, *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 stk. 1, *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 stk. 1, *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 stk. 1, *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 stk. 1, *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 stk. 1, *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 stk. 1, *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 stk. 1, *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 stk. 1, *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 stk. 1, *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 stk. 1, *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 stk. 1, *nr. 21*, 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 stk. 1, *nr. 22,* 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 stk. 1, *nr. 23,* 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 stk. 1, *nr. 24,* 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 stk. 1, *nr. 25*, 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 stk. 1, *nr. 26*, 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 stk. 1, *nr. 27*, 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, eller 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 stk. 1, *nr. 28*, 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 stk. 1, *nr. 29,* 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 stk. 1, *nr. 30,* 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 bestemmelsen fortolkes i overensstemmelse med NIS 2-direktivets definition.

Det foreslås i stk. 1, *nr. 31,* 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 stk. 1, *nr. 32,* 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 materiel eller immateriel skade.

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

*Til § 4*

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 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 den foreslåede *§ 4, stk. 1,* at enheder af en type, som er omfattet af bilag 2, og som overskrider tærsklerne for mellemstore virksomheder, anses for at være væsentlige enheder.

Den foreslåede bestemmelse vil gennemføre artikel 3, stk. 1, litra a, 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 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.

Forsvarsministeriet har lagt vægt på at der foretages en direktivnær minimumsimplementering. 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 lovforslagets bilag 2, og 2) enheden skal overskride tærsklerne for at være en mellemstor virksomhed.

Af lovforslagets bilag 2 fremgår følgende sektorer: 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. Der henvises til lovforslagets bilag 2 for en nærmere oversigt over, hvilke enhedstyper der er omfattet af den foreslåede bestemmelse.

Hvorvidt en enhed overskrider tærsklerne for mellemstore virksomheder efter den foreslåede bestemmelse, vil skulle vurderes ud fra de kriterier, der er fastsat i artikel 2, stk. 1, i bilaget til Europa-Kommissionens henstilling 2003/361/EF af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder. Det fremgår heraf, 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. EUR.

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

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

forbindelse med leveringen af sine tjenester og med hensyn til de tjenester, som enheden leverer.

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

Det følger af det foreslåede *stk. 2,* at i det omfang kommuner eller regioner måtte udføre opgaver som udbydere af offentlige elektroniske kommunikationsnet eller udbydere af offentligt tilgængelige elektroniske kommunikationstjenester, og er af en størrelse, der svarer til tæsklerne for mellemstore virksomheder, anses de for at være væsentlige enheder.

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 Forsvarsministeriets opfattelse være uhensigtsmæssigt, såfremt kommuner og regioner omfattes af det særskilte lovforslag, der gennemfører NIS 2-direktivet i telesektoren ved at integrere NIS 2-kravene med den eksisterende omfangsrige regulering af informationssikkerheden i telesektoren.

Den foreslåede bestemmelse vil delvist gennemføre artikel 3, stk. 1, litra c, 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 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.

Forsvarsministeriet har lagt vægt på at der foretages en minimumsimplementering. Den foreslåede bestemmelse skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Den foreslåede bestemmelse vil alene gælde for kommuner og regioner, i det omfang de udføre opgaver som udbydere af offentlige elektroniske kommunikationsnet eller udbydere af offentligt tilgængelige elektroniske kommunikationstjenester.

Hvorvidt en kommune eller region er af en størrelse, der svarer til tærsklerne for en mellemstor virksomhed efter den foreslåede bestemmelse, vil skulle vurderes ud fra de kriterier, der er fastsat i artikel 2 i bilaget til Europa-Kommissionens henstilling 2003/361/EF af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder. Det fremgår af heraf, 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 fremgår videre, at kategorien små virksomheder omfatter virksomheder, som beskæftiger under 50 personer, og som har en årlig omsætning eller en samlet årlig balance på ikke over 10 mio. euro.

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.

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) statslige myndigheder, 3) enheder, der er identificeret som kritiske enheder i henhold til lov om kritiske enheders modstandsdygtighed, 4) enheder, der inden den 16. januar 2023 er blevet identificeret som operatører af væsentlige tjenester i overensstemmelse med den tidligere gældende regulering, der gennemførte 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, og 5) øvrige enheder af en type, som er omfattet af bilag 2 og 3, 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.

Den foreslåede bestemmelse vil gennemføre artikel 3, stk. 1, litra b og d-g, 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 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.

Det følger af NIS 2-direktivets artikel 2, stk. 2, litra b-e, at uanset deres størrelse finder direktivet også anvendelse på enheder af den type, der er omhandlet i direktivets bilag I eller II, hvor: 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 eller 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.

Forsvarsministeriet har lagt vægt på at der foretages en direktivnær minimumsimplementering. 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.

Det følger af det foreslåede *nr. 2,* at statslige myndigheder anses for at være væsentlige enheder.

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.

Det følger af det foreslåede *nr. 4*, at enheder, der inden den 16. januar 2023 er blevet identificeret som operatører af væsentlige tjenester i overensstemmelse med den tidligere gældende regulering, der gennemførte 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.

Efter NIS 1-direktivets artikel 5, stk. 2, litra a, er det et kriterium for identificering af en enhed som en operatør af væsentlige tjenester, at enheden leverer en tjeneste, der er væsentlig for opretholdelsen af kritiske samfundsmæssige og/eller økonomiske aktiviteter. Det er som følge heraf Forsvarsministeriets opfattelse, at enheder, der er identificeret som operatører af væsentlige tjenester efter den danske gennemførelse af NIS 1-direktivet, som udgangspunkt bør anses for at være væsentlige enheder. Der foreslås dog en modifikation til dette udgangspunkt i lovforslagets § 5, stk. 2.

Det foreslås med *nr. 5*, at øvrige enheder af en type, som er omfattet af lovforslagets bilag 2 og 3, 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 lovforslagets bilag 2 fremgår følgende sektorer: 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 lovforslagets bilag 3 fremgår følgende 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 enhders 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.

Den foreslåede bestemmelse skal ses i sammenhæng med den foreslåede § 4, stk. 4, hvorefter de relevante ministre kan fastsætte nærmere kriterier for, hvornår enheder er omfattet af § 4, stk. 3, nr. 5. Desuden forudsættes det, 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 inden for sit område kan fastsætte nærmere regler om kriterier for, hvornår enheder er omfattet af stk. 3, nr. 5.

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 foreslås på den baggrund, at der i sektorspecifikke bekendtgørelser kan fastsættes nærmere kriterier for, hvornår enheder er omfattet af stk. 3, nr. 5.

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 den foreslåede *§ 5, stk. 1,* at enheder, der ikke opfylder kriterierne for at være væsentlige enheder i medfør af § 4, stk. 1-3, anses for at være vigtige enheder.

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.

Forsvarsministeriet har lagt vægt på at der foretages en minimumsimplementering. 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, at enheder, der er omfattet af lovens anvendelsesområde, og som ikke vil være at anse for væsentlige enheder i medfør af de foreslåede bestemmelser i § 4, stk. 1-3, vil være at anse for vigtige enheder. Dog vil enheder, der leverer domænenavnsregistreringstjenester, hverken være væsentlige eller vigtige enheder, jf. den foreslåede bestemmelse i stk. 3.

Den foreslåede bestemmelse vil navnlig være relevant for enheder, som er af en type omfattet af lovens bilag 2, og som udgør mellemstore virksomheder. Af lovens bilag 2 fremgår følgende sektorer: 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 IKT-tjenester (buisness-to-buisness), 7) offentlig forvaltning og 8) rummet.

Hvorvidt en enhed udgør en mellemstor virksomhed vil skulle vurderes ud fra de kriterier, der er fastsat i artikel 2 i bilaget til Europa-Kommissionens henstilling 2003/361/EF af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder. Det fremgår af heraf, 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. EUR. Det fremgår videre, at kategorien små virksomheder omfatter 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 en enhed udgør en mellemstor virksomhed, vil enheden 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.

Den foreslåede bestemmelse vil desuden navnlig være relevant for enheder, som er af en type omfattet af lovens bilag 3, og som udgør mellemstore virksomheder eller overskrider tærsklerne for at være mellemstore virksomheder.

Af lovens bilag 3 fremgår følgende sektorer: 1) Post- og kurertjenester, 2) affaldshåndtering, 3) fremstilling, produktion og distribution af kemikalier, 4) produktion, tilvirkning og distribution af fødevarer, 5) fremstilling, 6) digitale udbydere og 7) forskning.

For at en enhed udgør en mellemstor virksomhed eller overskrider tærskerlen for at være mellemstore virksomheder, vil enheden skulle beskæftige mindst 50 personer og have en årlig omsætning eller en samlet årlig balance på over 10 mio. euro.

Den foreslåede bestemmelse vil derudover være relevant for visse enheder uanset deres størrelse, som dog ikke er at betragte som væsentlige enheder. Det er eksempelvis relevant for udbydere af digitale tjenester. Der henvises til de specielle bemærkninger til den foreslåede stk. 1, som nærmere beskriver, hvilke enheder, der omfattes af lovens anvendelsesområde og den foreslåede § 4, som fastsætter hvilke enheder, der anses for væsentlige enheder.

Det følger af det foreslåede *stk. 2*, at den relevante kompetente myndighed efter en konkret vurdering kan træffe afgørelse om, at en enhed, 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 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.

Forsvarsministeriet har lagt vægt på at der foretages en minimumsimplementering. 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 Forsvarsministeriets 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, 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 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 afsnit 2.4 i lovforslagets almindelige bemærkninger.

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 Forsvarsministeriets 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 lovforlagets § 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 følger af det foreslåede *stk. 3,* at enheder der leverer domænenavnsregistreringstjenester hverken anses for at være væsentlige eller vigtige enheder.

NIS 2-direktivets artikel 3, stk. 1 og 2, indeholder nærmere regler for, hvornår enheder skal anses for at være henholdsvis væsentlige eller vigtige.

Det følger således af NIS 2-direktivets artikel 3, stk. 1, at følgende enheder anses for at være væsentlig enheder: a) 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, 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 i henhold til artikel 2, i bilaget til henstilling 2003/361/EF, 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.

Det følger af NIS 2-direktivets artikel 3, stk. 2, 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. Dette indbefatter enheder, som medlemsstaterne har identificeret som vigtige enheder i medfør af artikel 2, stk. 2, litra b)-e).

Forsvarsministeriet bemærker, at enheder der leverer domænenavnsregistreringstjenester er omfattet af visse af NIS 2-direktivets bestemmelser, men at denne type af enhed ikke er omfattet af definitionen af hverken en væsentlig eller vigtig enhed.

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

*Til § 6*

Det følger af artikel 14, 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 skal 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 skal disse foranstaltninger sikre et sikkerhedsniveau for net- og informationssystemer, der står i forhold til risikoen. Efter artikel 14, stk. 2, skal medlemsstaterne sikre, at operatører af væsentlige tjenester træffer 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 den foreslåede *§ 6, 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 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 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, 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.

Forsvarsministeriet har lagt vægt på, at der foretages en direktivnær minimumsimplementering. Den foreslåede bestemmelse svarer indholdsmæssigt til NIS 2-direktivets artikel 21, stk. 1-3, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

I overensstemmelse med NIS 2-direktivets artikel 6, stk. 1, nr. 2, skal »sikkerhed i net- og informationssystemer« forstås som net- og informationssystemers evne til, på et givet sikkerhedsniveau, at modstå enhver begivenhed, der kan være til skade for tilgængeligheden, autenticiteten, integriteten eller fortroligheden af lagrede, overførte eller behandlede data eller af de tjenester, der tilbydes af eller er tilgængelige via disse net- og informationssystemer.

Det er Forsvarsministeriets 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 i lyset af de aktiviteter, som er omfattet af direktivets anvendelsesområde. Det afgørende bliver på den baggrund, hvorvidt der er tale om net- og informationssystemer, som – hvis de blev kompromitteret – ville kunne påvirke enhedens levering af de tjenester eller opretholdelse af de aktiviteter, som er baggrunden for, at enheden er omfattet af direktivet.

Bestemmelsen vil derfor også efter omstændighederne kunne finde anvendelse for hele eller kun dele af enhedernes forretningsområder. Afhængig af en enheds konkrete it-infrastruktur kan det være nødvendigt, at foranstaltningerne gennemføres for alle dele af enhedens forretningsområder, herunder eventuelt også forretningsområder, som ikke måtte være omfattet af lovens anvendelsesområde. En enhed med flere forskellige forretningsområder, hvor nogle forretningsområder omfattes af lovens anvendelsesområde, mens andre ikke gør, vil således – såfremt der anvendes samme it-infrastruktur på tværs af hele forretningen – kunne være nødt til at gennemføre foranstaltningerne for hele forretningen.

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

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

Det følger af det foreslåede *stk. 2,* at en enhed, der finder, at den ikke overholder 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.

Forsvarsministeriet har lagt vægt på, at der foretages en direktivnær minimumsimplementering. Den foreslåede bestemmelse svarer indholdsmæssigt til NIS 2-direktivets artikel 21, stk. 4, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Den foreslåede bestemmelse i stk. 2 understreger, at enheder skal handle på eventuelle konstateringer af mangler i overholdelsen af de krav til foranstaltninger, der følger af det foreslåede stk. 1 og regler om krav til foranstaltninger udstedt i medfør af det foreslåede stk. 3. Dette skal ses i sammenhæng med den foreslåede § 7 om ledelsens ansvar.

Det følger af det foreslåede *stk. 3,* at vedkommende minister inden for sit område efter forhandling med forsvarsministeren kan fastsætte nærmere regler om krav til foranstaltninger efter stk. 1.

Den foreslåede bestemmelse indebærer, at der i sektorspecifikke bekendtgørelser kan fastsættes nærmere regler om krav til de foranstaltninger til styring af cybersikkerhedsrisici, som væsentlige og vigtige enheder inden for de pågældende sektorer skal træffe. Reglerne vil kunne stille mere konkretiserede krav til de foranstaltninger, som enhederne skal træffe i medfør af den foreslåede bestemmelse i stk. 1.

De nærmere regler vil skulle udarbejdes inden for den ramme, som det foreslåede stk. 1 udgør, herunder udarbejdes under hensyntagen til de forudsætninger, som er indlagt i det foreslåede stk. 1. Det indebærer bl.a., at reglerne vil skulle være i overensstemmelse med regeringens principper om minimumsimplementering.

Ved at bekendtgørelserne udstedes af de relevante ressortministre inden for deres områder, vil reglerne kunne målrettes de enkelte sektorer. Reglerne vil dermed i relevant omfang 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 forsvarsministeren. I praksis vil de nærmere krav skulle forhandles mellem ressortmyndighederne og Center for Cybersikkerhed. Center for Cybersikkerhed vil i den forbindelse have til opgave i videst muligt omfang 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. Center for Cybersikkerhed vil endvidere have til opgave at påse, at der ikke fastsættes regler, som er indbyrdes modstridende på tværs af sektorerne.

Det bemærkes, at det følger af NIS 2-direktivets artikel 21, stk. 5, 1. led, at Europa-Kommissionen senest den 17. oktober 2024 vedtager gennemførelsesretsakter, der fastsætter de tekniske og metodologiske krav til de foranstaltninger, der er omhandlet i artikel 21, stk. 2, 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. Der henvises til den foreslåede bestemmelse i § 30, der indebærer, at vedkommende minister inden for sit område kan fastsætte regler, som er nødvendige for at gennemføre retsakter udstedt af Europa-Kommissionen i medfør af NIS 2-direktivet.

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 Forsvarsministeriets 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.

Det foreslås i *§ 7, 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 og sikrer, at foranstaltningerne har den fornødne effekt.

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.

Forsvarsministeriet har lagt vægt på, at der foretages en direktivnær minimumsimplementering. Den foreslåede bestemmelse svarer med sproglige tilpasninger uden indholdsmæssig betydning til NIS 2-direktivets artikel 20, stk. 1, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Den foreslåede bestemmelse i stk. 1 fastslår, 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 § 33.

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 overveje at tilbyde tilsvarende kurser til sine 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.

Forsvarsministeriet har lagt vægt på, at der foretages en direktivnær minimumsimplementering. Den foreslåede bestemmelse svarer med sprolige tilpasninger uden indholdsmæssig betydning til NIS 2-direktivets artikel 20, stk. 2, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

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.

Det følger af den foreslåede *§ 8*, at vedkommende minister inden for sit område efter forhandling med forsvarsministeren 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. Produktet kan udvikles af den væsentlige eller vigtige enhed eller indkøbes fra tredjeparter.

Bestemmelsen vil gennemføre artikel 24, 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). 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.

Forsvarsministeriet har lagt vægt på, at der foretages en direktivnær minimumsimplementering. 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 Forsvarsministeriets 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 forsvarsministeren.

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 *§ 9, 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. lovforslagets bilag 2 eller 3, 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 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). 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.

Forsvarsministeriet har lagt vægt på, at der foretages en direktivnær minimumsimplementering. 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 bestemmelsen 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.

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 den 17. januar 2025. En enhed, der omfattes af lovens anvendelsesområde efter denne dato, skal indgive oplysningerne 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.

Forsvarsministeriet har lagt vægt på, at der foretages en direktivnær minimumsimplementering. 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 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.

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.

Forsvarsministeriet har lagt vægt på, at der foretages en direktivnær minimumsimplementering. 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 den foreslåede *§ 10, stk. 1*, at væsentlige og vigtige 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. lovforslagets bilag

2 eller 3 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 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 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.

Forsvarsministeriet har lagt vægt på, at der foretages en direktivnær minimumsimplementering. 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 § 9.

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.

De kompetente myndigheder vil – via det centrale kontaktpunkt – i overensstemmelse med NIS 2-direktivets artikel 3, stk. 5, bl.a. 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 den 17. april 2025. En enhed, der omfattes af lovens anvendelsesområde efter denne dato, skal indgive oplysningerne 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.

Forsvarsministeriet har lagt vægt på, at der foretages en direktivnær minimumsimplementering. 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 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.

Forsvarsministeriet 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 den foreslåede *§ 11, 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 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 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.

Forsvarsministeriet har lagt vægt på at der foretages en direktivnær minimumsimplementering. Den foreslåede bestemmelse svarer med sprolige 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.

Forsvarsministeriet har lagt vægt på, at der foretages en direktivnær minimumsimplementering. 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 domænenavnsregistre-

ringstjenester, har indført politikker og procedurer, herunder verifikationsprocedurer, for at sikre, at de i artikel 28, stk. 1, omhandlede databaser indeholder nøjagtige og fuldstændige oplysninger. Medlemsstaterne kræver, at sådanne politikker og procedurer gøres offentligt tilgængelige

Forsvarsministeriet har lagt vægt på, at der foretages en direktivnær minimumsimplementering. 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 skal topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester, efter bestemmelsen 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.

Forsvarsministeriet har lagt vægt på, at der foretages en direktivnær minimumsimplementering. 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 under alle omstændigheder 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.

Forsvarsministeriet har lagt vægt på, at der foretages en direktivnær minimumsimplementering. 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.

Forsvarsministeriet har lagt vægt på, at der foretages en direktivnær minimumsimplementering. 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 digitaliserings- og ligestillingsministeren kan fastsætte nærmere regler om krav til politikker og procedurer efter stk. 3.

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

De nærmere regler vil skulle udarbejdes inden for den ramme, som det foreslåede stk. 3 udgør, herunder udarbejdes under hensyntagen til de forudsætninger, som er indlagt i det foreslåede stk. 3. Det indebærer bl.a., at reglerne vil skulle være i overensstemmelse med regeringens principper om minimumsimplementering.

*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 den foreslåede *§ 12, stk. 1*, at væsentlige og vigtige enheder uden unødigt ophold skal underrette den relevante kompetente myndighed og CSIRT'en 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 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 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.

Forsvarsministeriet har lagt vægt på, at der foretages en direktivnær minimumsimplementering. 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.

Såfremt en væsentlig hændelse, der underrettes om i medfør af bestemmelsen, måtte have grænseoverskridende virkning, vil CSIRT'en i ovenstemmelse 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 materiel eller immateriel skade.

Den foreslåede bestemmelse vil gennemføre NIS 2-direktivets artikel 23, stk. 3, som fastslår, at en hændelse anses for at være væsentlig, hvis: a) 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.

Forsvarsministeriet har lagt vægt på, at der foretages en direktivnær minimumsimplementering. Den foreslåede bestemmelse svarer med en enkelt sproglig konsekvensrettelse uden indholdsmæssig betydning til NIS 2-direktivets artikel 23, stk. 3, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Det følger af det foreslåede *stk. 3*, at vedkommende minister inden for sit område efter forhandling med forsvarsministeren kan fastsætte nærmere regler om, hvornår en hændelse anses for at være væsentlig.

Henset til at kriterierne for, hvornår en hændelse anses for at være væsentlig efter det foreslåede stk. 2, har en kvalitativ og skønspræget karakter, vurderes det hensigtsmæssigt, at der kan fastsættes nærmere sektorvise regler, som præciserer, hvornår en hændelse i den pågældende sektor anses for at være væsentlig.

Den foreslåede bestemmelse har således til formål at give den relevante ressortminister mulighed for efter behov at præcisere, under hvilke omstændigheder der skal foretages underretning, således at eventuel fortolkningstvivl i videst mulig omfang kan fjernes. Der kan eksempelvis fastsættes kvantitative eller i øvrigt mere objektivt konstaterbare kriterier. De regler, der kan fastsættes i medfør af det foreslåede stk. 3, vil således i givet fald præcisere den foreslåede bestemmelse i stk. 2.

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 forsvarsministeren, således, at der – med respekt for de sektorvise forhold – i videst muligt omfang sikres ensartethed.

Det bemærkes, at Europa-Kommissionen senest den 17. oktober 2024 vedtager gennemførelsesretsakter, der yderligere præciserer de tilfælde, hvor en hændelse anses for at være væsentlig, jf. artikel 23, stk. 3, for så vidt angår 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. 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. Det forudsættes, at bemyndigelsen ikke udnyttes, før retsakterne fra Europa-Kommissionen foreligger, for så vidt angår 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.

Der henvises i øvrigt til afsnit 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 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).

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.

Forsvarsministeriet har lagt vægt på, at der foretages en direktivnær minimumsimplementering. 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.

Væsentlige og vigtige enheder vil indledningsvist 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.

Den tidlige varsling vil 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.

CSIRT'en kan på baggrund af hændelsesunderretningen anmode 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. 4. 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.

Efter NIS 2-direktivets præambelbetragtning nr. 101 er formålet med denne flertrinstilgang at finde den rette balance mellem på den ene side hurtig underretning, der vil bidrage til at afbøde den potentielle spredning af væsentlige hændelser og give væsentlige og vigtige enheder mulighed for at søge

assistance, og på den anden side en dybdegående underretning, der gør det muligt at høste erfaringer af individuelle hændelser.

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, jf. den foreslåede bestemmelse i § 31.

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 under alle omstændigheder 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.

Forsvarsministeriet har lagt vægt på, at der foretages en direktivnær minimumsimplementering. 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.

Forsvarsministeriet har lagt vægt på, at der foretages en direktivnær minimumsimplementering. 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 eller eventuelt andre relevante aktører, eksempelvis en sektorvis DCIS (decentral cyber- og informationssikkerhedsenhed). 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 afsnit 3.3 i lovforslagets almindelige bemærkninger.

*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 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 den foreslåede bestemmelse i *§ 14, stk. 1*, at offentlige og private enheder 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 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), 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.

Forsvarsministeriet har lagt vægt på, at der foretages en direktivnær minimumsimplementering. 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 indebærer, at alle offentlige og private enheder kan underrette CSIRT'en – dvs. Center for Cybersikkerhed – om hændelser, nærvedhændelser og cybertrusler. Det bemærkes, at den foreslåede bestemmelse i § 1, stk. 6, medfører, at § 14 vil finde anvendelse på enheder, der ikke ellers ville være omfattet af lovens anvendelsesområde.

I NIS 2-direktivets artikel 6, nr. 5, er en »nærvedhændelse« defineret 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 materialiserede sig.

Det bemærkes, at der for statslige myndigheder er pr. 1. september 2014 som følge af en regeringsbeslutning etableret en egentlig forpligtelse til at underrette Center for Cybersikkerhed ved større it-sikkerhedsmæssige hændelser, f.eks. hacker- og overbelastningsangreb. For øvrige myndigheder og virksomheder er der etableret en frivillig ordning, hvor de pågældende organisationer opfordres til at underrette Center for Cybersikkerhed ved større sikkerhedshændelser. Ordningen er etableret efter dialog med en række branche- og interesseorganisationer samt virksomheder. Denne ordning ændres ikke af den foreslåede bestemmelse.

Det følger af den foreslåede *stk. 2,* at CSIRT'en behandler underretninger efter stk. 1 på samme måde som underretninger modtaget i medfør af § 12. CSIRT'en kan prioritere håndteringen af underretninger, der er modtaget i medfør af § 12.

Bestemmelsen vil gennemføre artikel 30, stk. 2, 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 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 obliga-

toriske 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.

Forsvarsministeriet har lagt vægt på, at der foretages en direktivnær minimumsimplementering. 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.

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

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 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 bestemmelser, der regulerer, i hvilket omfang operatører af væsentlige tjenester skal underrette modtagerne af deres tjenester om væsentlige hændelser, der påvirker de tjenester, som operatørerne leverer.

Det følger af den foreslåede *§ 15, stk. 1,* at væsentlige og vigtige enheder i relevant omfang 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 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), 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.

Forsvarsministeriet har lagt vægt på, at der foretages en direktivnær minimumsimplementering. 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 indebærer 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 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.

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.

Forsvarsministeriet har lagt vægt på, at der foretages en direktivnær minimumsimplementering. 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 indebærer i overensstemmelse med NIS 2-direktivets præambelbetragtning nr. 103, 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 materialisere sig, 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 indebærer bestemmelsen endvidere, at oplysninger om væsentlige cybertrusler skal stilles gratis til rådighed for modtagerne i et let forståeligt sprog.

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

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

*Til § 16*

Det følger af artikel 14, 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 efter høring af den underrettende operatør af væsentlige tjenester kan den kompetente myndighed eller CSIRT'en oplyse offentligheden om konkrete hændelser, hvis offentlighedens kendskab hertil er nødvendig for at forebygge en hændelse eller håndtere en igangværende hændelse.

Det følger endvidere af artikel 16, stk. 7, i NIS 1-direktivet, at efter høring af udbyderen af de digitale tjenester kan 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 afsnit 2.4 i lovforslagets almindelige bemærkninger.

Det følger af den foreslåede *§ 16, 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 eller håndtere hændelsen, eller hvis offentliggørelse af hændelsen på anden vis er i offentlighedens interesse.

Bestemmelsen vil delvist gennemføre artikel 23, stk. 7, 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 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.

Forsvarsministeriet har lagt vægt på, at der foretages en direktivnær minimumsimplementering. 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 indebærer, 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 vurdere behovet for 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 m.v.

Det vil i den forbindelse skulle sikres, at offentligheden informeres på en 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 den væsentlige 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.

Forsvarsministeriet har lagt vægt på, at der foretages en direktivnær minimumsimplementering. 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 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 væ-

sentlige 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.

Forsvarsministeriet har lagt vægt på, at der foretages en direktivnær minimumsimplementering. Den foreslåede bestemmelse svarer med sproglige tilpasninger uden indholdsmæssig betydning til NIS 2-direktivets artikel 23, stk. 7, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

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

CSIRT'en vil i overensstemmelse med proceduren beskrevet i bemærkningerne til det foreslåede stk. 1, skulle foretage høring af den berørte enhed, før det vurderes, om enheden skal offentliggøre hændelsen. I forbindelse med en offentliggørelse vil CSIRT'en endvidere skulle varetage de fortrolighedshensyn, 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.

Forsvarsministeriet har lagt vægt på, at der foretages en direktivnær minimumsimplementering. 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 indebærer, at CSIRT'en efter høring af en enhed i en anden medlemsstat, hvor enheden er ramt af en væsentlig hændelse, kan informere offentligheden i Danmark om den væsentlige hændelse.

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

Før der foretages en vurdering af om, en enhed 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 offentliggørelse vil CSIRT'en endvidere skulle varetage de fortrolighedshensyn, der er beskrevet i bemærkningerne til det foreslåede stk. 1.

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

*Til § 17*

Det følger af bilag 1, nr. 2, 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 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 afsnit 2.4 i lovforslagets almindelige bemærkninger.

Det følger af lov om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter, jf. lov nr. 437 af 8. maj 2018, at

Center for Cybersikkerhed i dag varetager de tværgående opgaver som CSIRT og centralt kontaktpunkt efter NIS 1-direktivet.

Center for Cybersikkerheds virksomhed er primært reguleret i lov om Center for Cybersikkerhed, jf. lovbekendtgørelse nr. 836 af 7. august 2019 (CFCS-loven). Det følger af lovens § 1, at Center for Cybersikkerhed har til opgave at understøtte et højt informationssikkerhedsniveau i den informations- og kommunikationsteknologiske infrastruktur, som samfundsvigtige funktioner er afhængige af. Med henblik herpå indeholder loven en række særlige hjemler, der skal understøtte Center for Cybersikkerheds opgaveløsning. Eksempelvis har Center for Cybersikkerheds netsikkerhedstjeneste til opgave at opdage, analysere og bidrage til at imødegå sikkerhedshændelser hos tilsluttede myndigheder og virksomheder, jf. lovens § 3, og kan på den baggrund bl.a. monitorere net og systemer hos tilsluttede myndigheder og virksomheder i medfør af lovens § 4. Derudover kan centeret eksempelvis gennemføre forebyggende sikkerhedstekniske undersøgelser i medfør af CFCS-lovens § 6 a, når en myndighed eller virksomhed har anmodet centeret herom. Forebyggende sikkerhedstekniske undersøgelser indebærer bl.a., at Center for Cybersikkerhed efter aftale med en myndighed eller virksomhed forsøger at skaffe sig adgang til den pågældende myndighed eller virksomheds systemer og netværk.

Det følger af den foreslåede *§ 17, 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, med-

delelser 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.

Center for Cybersikkerhed vil varetage funktionen som CSIRT i forhold til alle de af direktivet omfattede sektorer, dvs. også de sektorer, hvor NIS 2-direktivet gennemføres ved sektorspecifik regulering, jf. afsnit 1 i lovforslagets almindelige bemærkninger. Den foreslåede bestemmelse i § 17 vil på den baggrund finde anvendelse i forhold til alle væsentlige og vigtige enheder, uanset om disse måtte være omfattet af nærværende lov eller anden regulering, der gennemfører NIS 2-direktivet, jf. også den foreslåede § 1, stk. 7.

Forsvarsministeriet har lagt vægt på, at der foretages en minimumsimplementering. 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. CSIRT'en vil også i medfør af CFCS-lovens § 4 kunne tilbyde at forestå monitorering af enhedens net- og informationssystemer, i det omfang betingelserne i CFCS-lovens § 3 for tilslutning til netsikkerhedstjenesten er opfyldt.

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 med hjemmel i CFCS-loven. Konkret teknisk bistand vil eksempelvis kunne ydes ved, at CSIRT'en med hjemmel i CFCS-lovens §§ 4 eller 5 efter aftale med enheden undersøger data, der stilles til rådighed fra enheden.

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 Forsvarsministeriets 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 et kriterium for anvendelse af proaktive scanninger efter bestemmelsen, at enheden har anmodet herom. I det omfang Center for Cybersikkerhed vil skulle foretage indgribende proaktive scanninger, vil dette skulle ske inden for rammerne af CFCS-lovens § 6 a om forebyggende sikkerhedstekniske undersøgelser.

Center for Cybersikkerhed 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.

I det omfang der foretages indgribende scanninger, herunder scanninger der indebærer indgreb omfattet af grundlovens § 72, vil dette således være omfattet af den foreslåede bestemmelse i nr. 3 og, som nævnt ovenfor, skulle ske inden for rammerne af CFCS-lovens § 6 a om forebyggende sikkerhedsundersøgelser. I overensstemmelse med NIS 2-direktivet vil sådanne scanninger skulle foretages for at opdage sårbarheder med en potentielt væsentlig indvirkning.

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.

Forsvarsministeriet har lagt vægt på, at der foretages en direktivnær minimumsimplementering. 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 indebærer, at CSIRT'en ud fra en risikobaseret tilgang kan 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 afsnit 2.2.2 i lovforslagets almindelige bemærkninger.

*Til § 18*

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 det foreslåede *§ 18, 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.

Forsvarsministeriet har lagt vægt på, at der foretages en direktivnær minimumsimplementering. 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 indebærer 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 har ikke 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 forsvarsministeren 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*

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 enhedernes frivillige indbyrdes udveksling af cybersikkerhedsoplysninger m.v.

Det følger af den foreslåede *§ 19, 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 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 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.

Forsvarsministeriet har lagt vægt på, at der foretages en direktivnær minimumsimplementering. Den foreslåede bestemmelse svarer med sproglige tilpasninger uden indholdsmæssig betydningtil NIS 2-direktivets artikel 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.

På den baggrund er det Forsvarsministeriets 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.

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 CSIRT'en 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.

Forsvarsministeriet har lagt vægt på, at der foretages en direktivnær minimumsimplementering. 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. Der lægges dog op til, at underretningen sendes til CSIRT'en og ikke den kompetente myndighed. Baggrunden herfor er, at det efter det foreslåede stk. 1 vil være CSIRT'en, der faciliterer udvekslingen af oplysninger mellem enheder i cybersikkerhedsfællesskaber.

Den foreslåede bestemmelse indebærer en forpligtelse for væsentlige og vigtige enheder til at underrette CSIRT'en, når de indgår i eller udtræder af de cybersikkerhedsfællesskaber, som CSIRT'en faciliterer efter stk. 1.

Forpligtelsen til at underrette CSIRT'en, 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 følger af artikel 8, 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 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 II, og de tjenester, der er omhandlet i direktivets bilag III. 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 afsnit 2.4 i lovforslagets almindelige bemærkninger.

Det følger af den foreslåede *§ 20, stk. 1,* at vedkommende minister inden for sit område fastsætter regler om, hvilken myndighed der skal varetage funktionen som kompetent myndighed inden for en given sektor eller delsektor, jf. lovens bilag 2 og 3.

Som led i implementeringen af NIS 2-direktivet vil det påhvile de relevante ressortministerier at oprette eller udpege kompetente myndigheder for de enkelte sektorer 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 indebærer, at vedkommende minister inden for sit område ved bekendtgørelse kan fastsætte regler om, hvilken myndighed

der skal varetage funktionen som kompetent myndighed. 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 myndigheden inden for en sektor eller delsektor. For at give enhederne et samlet overblik vil en samlet liste over kompetente myndigheder blive gjort offentlig tilgængelig.

Der henvises i øvrigt til afsnit 2.2.2 om nationale myndigheder og samarbejde i lovforslagets almindelige bemærkninger

Det følger af den foreslåede *stk. 2*, at for at sikre operationel uafhængighed ved tilsyn med den offentlige forvaltning kan digitaliserings- og ligestillingsministeren efter forhandling med en anden minister fastsætte regler om, at tilsyn med Digitaliserings- og Ligestillingsministeriet og underliggende myndigheder helt eller delvist overlades til den pågældende minister.

Den foreslåede bestemmelse vil gennemføre artikel 31, stk. 4, 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 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 Forsvarsministeriets opfattelse, at artikel 31, stk. 4, bl.a. indebærer, at det skal sikres, at tilsynet med den offentlige sektor er operationelt uafhængig. 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 hører tilsynet med den statslige del af den offentlige forvaltning under digitaliserings- og ligestillingsministerens 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 Digitaliserings- og Ligestillingsministeriet og 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 indebærer, at digitaliserings- og ligestillingsministeren efter forhandling med en anden minister kan fastsætte regler om, at tilsyn med Digitaliserings- og Ligestillingsministeriet og underliggende myndigheder helt eller delvist overlades til den pågældende minister.

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. Afgørelser truffet af disse underordnede myndigheder vil i givet fald skulle påklages til den pågældende minister – og ikke digitaliserings- og ligestillingsministeren – som led i almindelig administrativ rekurs.

*Til § 21*

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 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 følger af den foreslåede *§ 21, stk. 1*, at de kompetente myndigheder på deres respektive områder fører tilsyn med væsentlige enheders overholdelse af denne lov og regler udstedt i medfør af loven. En kompetent myndighed kan som led i sit tilsyn ud fra en konkret vurdering af omstændighederne i hver enkelt sag anvende følgende tilsynsforanstaltninger over for en væsentlig enhed: 1) Foretage kontrol på stedet og foretage 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 ad hoc, 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 og 7) kræve at få udleveret dokumentation for gennemførelsen af cybersikkerhedspolitikker.

Den foreslåede bestemmelse vil gennemføre artikel 32, stk. 1 og 2, 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 32, stk. 1, at medlemsstaterne skal sikre, at de tilsyns- eller håndhævelsesforanstaltninger, der pålægges væsentlige enheder, for så vidt angår forpligtelserne fastsat i direktivet, er effektive, står i rimeligt forhold til overtrædelsen og har afskrækkende virkning under hensyntagen til omstændighederne i hver enkelt sag.

Efter bestemmelsen i artikel 32, stk. 2, skal medlemsstaterne sikre, at de kompetente myndigheder, når de udfører deres tilsynsopgaver vedrørende væsentlige enheder, som minimum har beføjelse til at pålægge disse enheder a) kontrol på stedet og eksternt tilsyn, herunder stikprøvekontrol, som skal udføres af uddannede fagfolk, b) regelmæssige og målrettede sikkerhedsaudits udført af et kvalificeret uafhængigt organ eller en kompetent myndighed, c) ad hoc-audits, herunder hvor det er berettiget på grund af en væsentlig hændelse eller en overtrædelse af dette direktiv fra den væsentlige enheds side, d) sikkerhedsscanninger baseret på objektive, ikke-diskriminerende, fair og gennemsigtige risikovurderingskriterier, hvor det er nødvendigt i samarbejde med den berørte enhed, e) anmodninger om oplysninger, der er nødvendige for at vurdere de foranstaltninger til styring af cybersikkerhedsrisici, som den berørte enhed har indført, herunder dokumenterede cybersikkerhedspolitikker, samt overholdelse af forpligtelsen til at indgive oplysninger til de kompetente myndigheder i henhold til artikel 27 (om registreringspligt for bestemte typer af digitale tjenester), f) anmodninger om adgang til data, dokumenter og oplysninger, der er nødvendige for udførelsen af deres tilsynsopgaver og g) anmodninger om dokumentation for gennemførelsen af cybersikkerhedspolitikker såsom resultaterne af sikkerhedsaudits udført af en kvalificeret revisor og den respektive underliggende dokumentation.

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.

Forsvarsministeriet har lagt vægt på at der foretages en direktivnær minimumsimplementering. 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.

Den foreslåede bestemmelse fastslår, at de kompetente myndigheder fører tilsyn med væsentlige enheders overholdelse af denne lov og regler udstedt i medfør af loven.

Det bemærkes, at det følger af den foreslåede bestemmelse i § 20, at vedkommende minister udpeger en eller flere kompetente myndigheder. En kompetent myndighed er således en myndighed, der inden for en given sektor eller delsektor er blevet udpeget til at føre tilsyn med efterlevelsen af

denne lov og regler udstedt i medfør af loven. For at give enhederne et samlet overblik vil en samlet liste over kompetente myndigheder blive gjort offentlig tilgængelig.

Det bemærkes endvidere, at de dele af direktivets bestemmelser, der angår rent myndighedsinterne forhold eller som allerede følger af almindelige forvaltningsretlige principper ikke er afspejlet direkte i lovteksten. Det skyldes, at den foreslåede bestemmelse er udformet med fokus på, hvilke konkrete tilsynsforanstaltninger de kompetente myndigheder kan anvende over for enhederne. Således er eksempelvis den del af direktivets artikel 32, stk. 2, litra a, hvorefter kontrollerne skal udføres af uddannede fagfolk, ikke afspejlet direkte i lovteksten. Det samme gælder eksempelvis den del af direktivets artikel 32, stk. 2, litra d, hvorefter sikkerhedsscanninger skal være baseret på objektive, ikke-diskriminerende, fair og gennemsigtige risikovurderingskriterier.

Det fremgår desuden af NIS 2-direktivets artikel 32, stk. 2, litra a, at der kan foretages »eksternt tilsyn«, hvilket er en formulering, der efter Forsvarsministeriets opfattelse kan give anledning til fortolkningstvivl. I den engelske sprogversion af NIS 2-direktivet anvendes formuleringen »off-site supervision«. Efter Forsvarsministeriets opfattelse udgør eksternt tilsyn, forstået som off-site supervision, et tilsyn fra en kompetent myndighed uden fysisk tilstedeværelse *på stedet*, altså eksempelvis udført på skriftligt grundlag. Det bemærkes, at en kompetent myndighed i medfør af den foreslåede bestemmelse kan kræve relevante oplysninger fra en enhed. Det indebærer også, at en kompetent myndighed kan kræve at få udleveret nødvendige oplysninger til afgørelse af, om et forhold er omfattet af loven eller regler udstedt i medfør af loven.

Den kompetente myndigheds tilsyn vil efter den foreslåede bestemmelse kunne gennemføres ved fysiske tilsynsbesøg eller på administrativt grundlag.

Et administrativt tilsyn på skriftligt grundlag vil kunne baseres på de dele af den foreslåede bestemmelse, hvorefter de kompetente myndigheder kan kræve at få relevante oplysninger fra enhederne.

Det er Forsvarsministeriets 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. Et sådant tilsyn vil kunne bestå af stikprøvekontroller.

Såfremt en væsentlig enhed ikke giver adgang til sine lokaler, vil det kunne straffes med bøde i medfør af den foreslåede § 32. Den foreslåede bestemmelse indebærer således ikke, at der gives adgang til lokaler uden retskendelse.

I overensstemmelse med direktivets forudsætninger som udtrykt i præambelbetragtning nr. 122 vil væsentlige enheder – i modsætning til vigtige enheder – blive underlagt løbende tilsyn. Det betyder, at der vil kunne føres tilsyn med en enhed både før og efter, at der eventuelt måtte foreligge oplysninger, der tyder på, at den pågældende enhed ikke efterlever sine forpligtelser efter loven og regler udstedt i medfør af loven, samt både før og efter en eventuel væsentlig hændelse.

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. Det fremgår videre af bestemmelsen, at 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 kunne anlægge en risikobaseret tilgang ved tilrettelæggelsen af deres tilsyn med væsentlige enheder, eksempelvis ved at lægge vægt på enhedernes risikoeksponering, deres størrelse og deres samfundsmæssige betydning.

Anvendelsen af de forskellige tilsynsforanstaltninger, som opregnes i den foreslåede § 21, stk. 1, vil ske efter en konkret vurdering af omstændighederne i hver enkelt sag. Valget af tilsynsforanstaltninger skal ske i overensstemmelse med det almindelige proportionalitetsprincip.

I overensstemmelse med forudsætningerne i direktivets præambelbetragtning nr. 123 bør en kompetent myndigheds udførelse af tilsynsopgaven ikke unødigt hæmme den berørte enheds forretningsaktiviteter. Samme sted fremgår det, at hvor en kompetent myndighed udfører sin tilsynsopgave vedrørende en væsentlig enhed, herunder i form af kontrol på stedet og administrativt tilsyn på skriftligt grundlag, efterforskning af overtrædelser af direktivet og udførelse af sikkerhedsaudits eller -scanninger, bør den kompetente myndighed minimere indvirkningen på den berørte enheds forretningsaktiviteter.

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.

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.

Forsvarsministeriet har lagt vægt på, at der foretages en direktivnær minimumsimplementering. Den foreslåede bestemmelse svarer indholdsmæssigt til NIS 2-direktivets artikel 32, stk. 3, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Det følger af det foreslåede *stk. 3,* at de kompetente myndigheder kan stille nærmere krav om, hvordan og i hvilken form oplysningerne eller materialet nævnt i stk. 1, nr. 5-7, 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. 5-7, samtidig kan kræve, at oplysningerne eller materialet udleveres på en bestemt måde, på et bestemt sprog og i en bestemt form.

Der vil eksempelvis kunne stilles krav om anvendelse af bestemte skemaer, eller at der skal foretages indtastninger på en hjemmeside.

Der henvises i øvrigt til afsnit 3.4 i lovforslagets almindelige bemærkninger.

*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 ud fra en konkret vurdering af omstændighederne i hver enkelt sag kan anvende følgende håndhævelsesforanstaltninger over for en væsentlig enhed 1) påbyde enheden at træffe foranstaltninger, der er nødvendige for at forhindre eller afhjælpe en hændelse, 2) meddele enheden påbud og forbud for at sikre overholdelsen af de krav, der er fastsat i loven eller regler udstedt i medfør af loven, 3) 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 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, 4) påbyde enheden at gennemføre de anbefalinger, der er fremsat i forbindelse med en gennemført sikkerhedsaudit, 5) påbyde enheden at udpege en person med ansvar for i en nærmere fastsat periode at føre tilsyn med enhedens overholdelse af §§ 6, 12, 13, 15 og 16, samt regler udstedt i medfør heraf og 6) 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 artikel 32, stk. 4, litra a-h, 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 der følger en forpligtelse for medlemsstaterne til at sikre, at deres kompetente myndigheder, når de udøver deres håndhævelsesbeføjelser over for væsentlige enheder, som minimum har beføjelse til at a) udstede advarsler om de pågældende enheders overtrædelser af direktivet, b) 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 direktivet, c) pålægge de pågældende enheder at ophøre med at udvise adfærd, der overtræder direktivet, 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, g) udpege en overvågningsansvarlig med veldefinerede opgaver til i en nærmere fastsat periode at føre tilsyn med de pågældende enheders overholdelse af artikel 21 (foranstaltninger til styring af cybersikkerhedsrisici) og 23 (rapporteringsforpligtelser) og h) pålægge de pågældende enheder at offentliggøre aspekter af overtrædelser af direktivet på en nærmere angivet måde.

Forsvarsministeriet har lagt vægt på at der foretages en direktivnær minimumsimplementering. 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.

Forsvarsministeriet har samtidig lagt vægt på, at håndhævelsesbestemmelserne tilpasses de tilsynsmæssige virkemidler, der normalt benyttes i dansk ret. Efter bestemmelsen får de kompetente myndigheder således mulighed

for at udstede påbud og forbud, som vil skulle favne de forskellige håndhævelsesmuligheder oplistet i artikel 32, stk. 4, litra a-h. På den baggrund medtages direktivets bestemmelser om advarsler, der kan sanktioneres med bøde, og såkaldt bindende instrukser ikke som sådan, idet det er Forsvarsministeriets opfattelse, at disse virkemidler i en dansk kontekst dækkes af begreberne påbud og forbud. Det bemærkes i den forbindelse, at de kompetente myndigheder, ud over den foreslåede bestemmelse, som led i sin almindelige virksomhed vil kunne give advarsler i form af henstillinger, der ikke kan sanktioneres med bøde.

I overensstemmelse med NIS 2-direktivets artikel 32, stk. 1, skal de foranstaltninger, der anvendes overfor væsentlige enheder i medfør af den foreslåede bestemmelse, 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 en kompetent myndighed skal foretage en konkret vurdering af omstændighederne i hver enkelt sag, når den anvender håndhævelsesforanstaltningerne over for væsentlige enheder.

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 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.

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 regler, herunder bestemmelserne i kapitel 3 (om vejledning og repræsentation m.v.), kapitel 5 (om partshøring), kapitel 6 (om begrundelse m.v.) og kapitel 7 (om klagevejledning). Derudover vil der være mulighed for at påklage afgørelsen i medfør af det almindelige ulovbestemte princip om administrativ rekurs, ligesom afgørelsen vil kunne indbringes for domstolene.

Der vil i forbindelse med en afgørelse om påbud eller forbud efter den foreslåede § 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 påbyde enheden at træffe foranstaltninger, der er nødvendige for at forhindre eller afhjælpe en hændelse.

Det følger af det foreslåede *nr. 2,* 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 følger af det foreslåede *nr. 3,* at den kompetente myndighed kan 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 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 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 følger af det foreslåede *nr. 4*, 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 § 21, 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 § 21, stk. 1, nr. 3, hvorefter den kompetente myndighed kan foretage sikkerhedsaudits ad hoc.

Det følger af det foreslåede *nr. 5*, at den kompetente myndighed kan påbyde enheden at udpege en person med ansvar for i en nærmere fastsat periode at føre tilsyn med enhedens overholdelse af §§ 6, 12, 13, 15 og 16, samt regler udstedt i medfør heraf.

Enheden vil enten kunne udpege en ansat eller en ekstern person. Det forudsættes, at den pågældende person har de nødvendige kvalifikationer til at udføre opgaven. Den pågældende person vil skulle monitorere 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, 13, 15 og 16, samt regler udstedt i medfør af de nævnte bestemmelser.

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. 1-5 samt resumeer af domme eller bødevedtagelser, hvor der idømmes eller vedtages en bøde.

I overenstemmelse 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 afsnit 3.4 i lovforslagets almindelige bemærkninger.

*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 *§ 23, 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 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 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 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 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.

Forsvarsministeriet har lagt vægt på, at der foretages en direktivnær minimumsimplementering. 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 Forsvarsministeriets opfattelse imidlertid ikke forenelig med den engelske udgave af direktivet, hvori »ineffective« er anvendt. Det er således Forsvarsministeriets opfattelse, at formuleringen »virkningsløse« ville udgøre en indholdsmæssig forskydning i forhold til den engelske sprogversion. Det er desuden Forsvarsministeriets 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 Forsvarsministeriets 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.

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 har vist sig utilstrækkelige.

Det følger af NIS 2-direktivets artikel 32, stk. 7, at den kompetente myndighed ved anvendelsen af håndhævelsesforanstaltninger såsom suspension eller forbud efter den foreslåede bestemmelse skal tage hensyn til en række nærmere angivne forhold.

I direktivets artikel 32, stk. 7, er følgende hensyn oplistet: 1) Overtrædelsens grovhed og vigtigheden af de overtrådte bestemmelser, idet bl.a. følgende under alle omstændigheder skal betragtes som alvorlige overtrædelser: a) Gentagne overtrædelser, b) manglende underretning om eller afhjælpning af væsentlige hændelser, c) manglende afhjælpning af mangler efter bindende instrukser fra kompetente myndigheder, d) hindringer for audits eller overvågningsaktiviteter beordret af den kompetente myndighed efter konstatering af en overtrædelse og e) afgivelse af urigtige eller klart unøjagtige oplysninger vedrørende cybersikkerhedsrisikostyringsforanstaltninger eller rapporteringsforpligtelser, 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.

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 forsvarsministeren vil kunne fastsætte nærmere regler for, hvilke certificeringer og godkendelser, som bestemmelsen i stk. 1, nr. 1, finder anvendelse på. Det forudsættes, at den foreslåede bestemmelse i stk. 1, nr. 1, ikke anvendes, før bemyndigelsen i den foreslåede stk. 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 Forsvarsministeriets 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 følger af det foreslåede *stk. 2*, at midlertidige 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.

Forsvarsministeriet har lagt vægt på, at der foretages en direktivnær minimumsimplementering. 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 ledelsesfunktioner 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 kan forlanges indbragt for domstolene af enheden eller den fysiske person, afgørelsen vedrører. Den myndighed, som vedkommende minister bemyndiger hertil, anlægger i givet fald 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.

Den foreslåede bestemmelse vil ikke afskære enheden eller den fysiske person, som afgørelsen vedrører, fra at påklage afgørelsen som led i almindelig administrativ rekurs i det omfang, dette er muligt.

Det vil efter bestemmelsen være muligt for enheden at forlange afgørelsen indbragt for retten, uanset om der er truffet en administrativ afgørelse i 2. instans.

Efter bestemmelsen vil det være op til vedkommende minister at bestemme, hvilken myndighed der skal anlægge sag ved domstolene. Det vil således ikke nødvendigvis være den myndighed, der har truffet den seneste afgørelse i sagen, der anlægger sagen ved domstolene.

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.

Forsvarsministeriet har lagt vægt på at der foretages en direktivnær minimumsimplementering. 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.

Det følger af det foreslåede *stk. 5*, at vedkommende minister efter forhandling med forsvarsministeren 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 stk. 1, nr. 1, ikke anvendes, før bemyndigelsen i den foreslåede stk. 5, er anvendt.

Der henvises i øvrigt til afsnit 3.4 i lovforslagets almindelige bemærkninger.

*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 følger af det foreslåede *§ 24, stk. 1*, at de kompetente myndigheder på deres respektive områder fører reaktivt tilsyn med vigtige enheders overholdelse af denne lov og regler udstedt i medfør af loven. En kompetent myndighed kan som led i sit tilsyn, hvis der er efter indikationer på, at en vigtig enhed ikke overholder eller har overholdt denne lov eller regler udstedt i medfør af loven, ud fra en konkret vurdering af omstændighederne i hver enkelt sag anvende følgende tilsynsforanstaltninger: 1) Foretage kontrol på

stedet, 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 og 6) kræve at få udleveret dokumentation for gennemførelsen af cybersikkerhedspolitikker.

Den foreslåede bestemmelse vil gennemføre artikel 33, stk. 1 og 2, 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 artikel 33, stk. 1, at når medlemsstaterne kommer i besiddelse af dokumentation for, tegn på eller oplysninger om, at en vigtig enhed angiveligt ikke overholder direktivet, navnlig artikel 21 og 23, 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.

Efter bestemmelsen i artikel 33, stk. 2, skal medlemsstaterne sikre, at de kompetente myndigheder, når de udfører deres tilsynsopgaver vedrørende vigtige enheder, som minimum har beføjelse til at pålægge vigtige enheder: a) Kontrol på stedet og eksternt efterfølgende tilsyn udført af uddannede fagfolk, b) målrettede sikkerhedsaudits udført af et kvalificeret uafhængigt organ eller en kompetent myndighed, c) sikkerhedsscanninger baseret på objektive, ikke-diskriminerende, fair og gennemsigtige risikovurderingskriterier, hvor det er nødvendigt i samarbejde med den berørte enhed, d) anmodninger om oplysninger, der er nødvendige for efterfølgende at vurdere de foranstaltninger til styring af cybersikkerhedsrisici, som den berørte enhed har indført, herunder dokumenterede cybersikkerhedspolitikker, samt overholdelse af forpligtelsen til at indgive oplysninger til de kompetente myndigheder i henhold til artikel 27 (om registreringspligt for bestemte typer af digitale tjenester), e) anmodninger om adgang til data, dokumenter og oplysninger, der er nødvendige for udførelsen af deres tilsynsopgaver og f) anmodninger om dokumentation for gennemførelsen af cybersikkerhedspolitikker såsom resultaterne af sikkerhedsaudits udført af en kvalificeret revisor og den respektive underliggende dokumentation.

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.

Forsvarsministeriet har lagt vægt på at der foretages en direktivnær minimumsimplementering. 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.

Den foreslåede bestemmelse fastslår, at de kompetente myndigheder fører reaktivt tilsyn med vigtige enheders overholdelse af denne lov og regler udstedt i medfør af loven.

Det bemærkes, at det følger af den foreslåede bestemmelse i § 20, at vedkommende minister udpeger en eller flere kompetente myndigheder. En kompetent myndighed er således en myndighed, der inden for en given sektor eller delsektor er blevet udpeget til at føre tilsyn med efterlevelsen af denne lov og regler udstedt i medfør af loven. For at give enhederne et samlet overblik vil en samlet liste over kompetente myndigheder blive gjort offentlig tilgængelig.

Det bemærkes endvidere, at de dele af direktivets bestemmelser, der angår rent myndighedsinterne forhold eller som allerede følger af almindelige forvaltningsretlige principper ikke er afspejlet direkte i lovteksten. Det skyldes, at den foreslåede bestemmelse er udformet med fokus på, hvilke konkrete tilsynsforanstaltninger de kompetente myndigheder kan anvende over for enhederne. Således er eksempelvis den del af direktivets artikel 33, stk. 2, litra a, hvorefter kontrollerne skal udføres af uddannede fagfolk, ikke afspejlet direkte i lovteksten. Det samme gælder eksempelvis den del af direktivets artikel 33, stk. 2, litra c, hvorefter sikkerhedsscanninger skal være baseret på objektive, ikke-diskriminerende, fair og gennemsigtige risikovurderingskriterier.

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 Forsvarsministeriets 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 Forsvarsministeriets 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.

Den kompetente myndigheds tilsyn vil efter de foreslåede bestemmelser kunne gennemføres ved fysiske tilsynsbesøg eller på administrativt grundlag.

Et administrativt tilsyn på skriftligt grundlag vil kunne baseres på de dele af den foreslåede bestemmelse, hvorefter de kompetente myndigheder kan kræve at få relevante oplysninger fra enhederne.

Det er Forsvarsministeriets 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.

Såfremt en vigtig enhed ikke giver adgang til sine lokaler, vil det kunne straffes med bøde i medfør af den foreslåede § 32. Den foreslåede bestemmelse indebærer således ikke, at der gives adgang til lokaler uden retskendelse.

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, rent 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 almindelige proportionalitetsprincip.

I overensstemmelse med forudsætningerne i direktivets præambelbetragtning nr. 123 bør de kompetente myndigheders udførelse af tilsynsopgaver ikke unødigt hæmme den berørte enheds forretningsaktiviteter.

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.

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.

Forsvarsministeriet har lagt vægt på, at der foretages en direktivnær minimumsimplementering. 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) Meddele enheden påbud og forbud for at sikre overholdelsen af de krav, der er fastsat i loven eller regler udstedt i medfør af loven, 2) 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 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, 3) påbyde enheden at gennemføre de anbefalinger, der er fremsat i forbindelse med en gennemført sikkerhedsaudit, og 4) 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.

Den foreslåede bestemmelse vil gennemføre artikel 33, stk. 4, litra a-g, 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). 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.

Forsvarsministeriet har lagt vægt på at der foretages en direktivnær minimumsimplementering. 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.

Forsvarsministeriet har samtidig lagt vægt på, at håndhævelsesbestemmelserne tilpasses de tilsynsmæssige virkemidler, der normalt benyttes i dansk ret. Efter bestemmelsen får de kompetente myndigheder således mulighed for at udstede påbud og forbud, som vil skulle favne de forskellige håndhævelsesmuligheder oplistet i artikel 33, stk. 4, litra a-g. På den baggrund medtages direktivets bestemmelser om advarsler, der kan sanktioneres med bøde, og såkaldt bindende instrukser ikke som sådan, idet det er Forsvarsministeriets opfattelse, at disse virkemidler i en dansk kontekst dækkes af begreberne påbud og forbud. Det bemærkes i den forbindelse, at de kompetente myndigheder, ud over den foreslåede bestemmelse, som led i sin almindelige virksomhed vil kunne give advarsler i form af henstillinger, der ikke kan sanktioneres med bøde.

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, 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.

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 regler, herunder bl.a. bestemmelserne i kapitel 3 (om vejledning og repræsentation m.v.), kapitel 5 (om partshøring), kapitel 6 (om begrundelse m.v.) og kapitel 7 (om klagevejledning). Derudover vil der være mulighed for at påklage afgørelsen i medfør af det ulovbestemte princip om administrativ rekurs, ligesom afgørelsen vil kunne indbringes for domstolene.

Der vil i forbindelse med en afgørelse om påbud eller forbud efter den foreslåede § 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 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 følger af det foreslåede *nr. 2,* at den kompetente myndighed kan 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 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. 2 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 følger af det foreslåede *nr. 3,* 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 § 24, 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 følger af det foreslåede *nr. 4,* 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 overenstemmelse 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 afsnit 3.4 i lovforslagets almindelige bemærkninger.

*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 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). 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.

Forsvarsministeriet 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, og at den kompetente myndighed lader høringsskrivelsen få virkning som en afgørelse, hvis enheden ikke kommer med bemærkninger til høringen inden dennes udløb.

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.

Der henvises i øvrigt til afsnit 3.4 i lovforslagets almindelige bemærkninger.

*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 *§ 27, 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. Samarbejdet indebærer, at: 1) De kompetente myndigheder via det centrale kontaktpunkt underretter 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, og 3) de kompetente myndigheder yder i rimeligt omfang bistand til en anden medlemsstats kompetente myndighed efter modtagelse af en begrundet anmodning herom.

Bestemmelsen vil gennemføre artikel 37, 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), 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.

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.

Forsvarsministeriet har lagt vægt på, at der foretages en direktivnær minimumsimplementering. Den foreslåede bestemmelse svarer indholdsmæssigt til NIS 2-direktivets artikel 37, stk. 1, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Den foreslåede bestemmelse indebærer, at de danske kompetente myndigheder i relevant omfang skal samarbejde med de kompetente myndigheder i andre medlemsstater om deres opgaveudførelse vedrørende en enhed, der 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.

Samarbejdet indebærer, at der skal ske underretning af de kompetente myndigheder i relevante medlemsstater om anvendte tilsyns- og håndhævelsesforanstaltninger. At der skal ske underretning til kompetente myndigheder i

»relevante medlemsstater« betyder, at der skal ske underretning til de kompetente myndigheder i medlemsstater, hvor enheden leverer tjenester, eller hvor dens net- og informationssystemer er beliggende.

Samarbejdet indebærer desuden, at de danske kompetente myndigheder kan anmode en anden medlemsstats kompetente myndigheder om at iværksætte tilsyns- og håndhævelsesforanstaltninger.

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 foretage 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.

Efter NIS 2-direktivets præambelbetragtning nr. 134 er formålet med bestemmelsen i direktivets artikel 37 at sikre, at enhederne overholder de forpligtelser, der er fastat i direktivet. En anmodning om gensidig bistand efter den foreslåede stk. 1 vil derfor ikke blive imødekommet, såfremt anmodningen entydigt vedrører en anden medlemsstats nationale overimplementering af NIS 2-direktivet.

Det følger af det foreslåede *stk. 2*, at 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.

Forsvarsministeriet har lagt vægt på, at der foretages en direktivnær minimumsimplementering. 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 fastat 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.

*Til § 28*

Forvaltningslovens §§ 28-32 fastsætter rammerne for forvaltningsmyndigheders videregivelse af oplysninger til en anden forvaltningsmyndighed. Det følger bl.a. af forvaltningslovens § 28, stk. 1, at for videregivelse af oplysninger om enkeltpersoner (personoplysninger) til en anden forvaltningsmyndighed gælder reglerne i databeskyttelseslovens §§ 6, 7, 8, 10, § 11, stk. 1, og §§ 38 og 40. Det følger af forvaltningslovens § 28, stk. 2, at oplysninger af fortrolig karakter, som ikke er omfattet af stk. 1, kun må videregives til en anden forvaltningsmyndighed, når: 1) Den, oplysningen angår, udtrykkeligt har givet sit samtykke, 2) det følger af lov eller bestemmelser fastsat i henhold til lov, at oplysningen skal videregives, eller 3) det må antages, at oplysningen vil være af væsentlig betydning for myndighedens virksomhed eller for en afgørelse, myndigheden skal træffe.

Det følger af den foreslåede bestemmelse i *§ 28,* at de relevante 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 NIS 2-direktivet.

Det er Forsvarsministeriets opfattelse, at der er behov for at indføre særskilt hjemmel til at kunne videregive oplysninger af fortrolig karakter til andre medlemsstaters myndigheder og institutioner i Den Europæiske Union. Dette vil sikre, at de danske myndigheder i alle tilfælde vil kunne leve op til forpligtelserne i NIS 2-direktivet.

Bestemmelsen indebærer, at de kompetente myndigheder, CSIRT'en og det centrale kontaktpunkt 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 den foreslåede *§ 29, 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 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), 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.

Forsvarsministeriet har lagt vægt på, at der foretages en direktivnær minimumsimplementering. Den foreslåede bestemmelse svarer indholdsmæssigt til NIS 2-direktivets artikel 2, stk. 11, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Der er en vis usikkerhed om fortolkningen af bestemmelsens udstrækning.

Det er Forsvarsministeriets opfattelse, at bestemmelsen primært vil være relevant for oplysninger, der udveksles mellem medlemsstaterne og institutioner i Den Europæiske Union. Bestemmelsen vil på denne baggrund hovedsageligt være relevant i forhold til den foreslåede § 28, der udgør de danske myndigheders videregivelseshjemmel hertil.

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 m.v.), er det Forsvarsministeriets opfattelse, at den foreslåede bestemmelse i § 29, stk. 1, for enheders vedkommende 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 enhed mere generelt kan undlade at efterkomme oplysningsforpligtelserne over for de kompetente myndigheder, herunder som led i myndighedernes tilsyn. Det er Forsvarsministeriets opfattelse, at det kun vil være i yderst sjældne tilfælde, at videregivelse af en enheds oplysninger til den relevante kompetente myndighed vil stride mod væsentlige interesser af hensyn til den nationale sikkerhed, offentlige sikkerhed eller forsvar.

I tilfælde af tvivl om, hvorvidt der i en konkret situation måtte være tale om oplysninger, hvis videregivelse vil stride mod væsentlige interesser med hensyn til den nationale sikkerhed, offentlige sikkerhed eller forsvar, vil den pågældende enhed eller kompetente myndighed kunne rette henvendelse til Politiets Efterretningstjeneste, som er national sikkerhedsmyndighed, eller til Forsvarets Efterretningstjeneste, som er national sikkerhedsmyndighed på Forsvarsministeriets område.

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 inden for sit område 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 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) tillagt kompetence til at vedtage retsakter, der nærmere udmønter bestemte dele af direktivet.

Det følger af NIS 2-direktivets artikel 21, stk. 5, 1. led, at Europa-Kommissionen senest den 17. oktober 2024 vedtager gennemførelsesretsakter, der fastsætter de tekniske og metodologiske krav til de foranstaltninger, der er omhandlet i direktivets artikel 21, stk. 2 (foranstaltninger til styring af cybersikkerhedsrisici), 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.

For så vidt angår andre væsentlige og vigtige enheder end dem, der er nævnt ovenfor, 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).

Senest den 17. oktober 2024 vedtager Europa-Kommissionen gennemførelsesretsakter, der yderligere præciserer de tilfælde, hvor en hændelse anses for at være væsentlig, jf. artikel 23, stk. 3, for så vidt angår 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. Europa-Kommissionen kan også vedtage sådanne gennemførelsesretsakter for så vidt angår andre væsentlige og vigtige enheder.

Europa-Kommissionen samarbejder med Samarbejdsgruppen om udkastene til gennemførelsesretsakter.

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 at fastsætte regler inden for sit område, som er nødvendige for at gennemføre retsakter udstedt af Europa-Kommissionen.

*Til § 31*

Det følger af den foreslåede *§ 31*, at vedkommende minister inden for sit område efter forhandling med forsvarsministeren 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.

Der kan endvidere med hjemmel i bestemmelsen fastsættes regler om, hvem der omfattes af pligten til at kommunikere digitalt, om hvilke forhold, og på hvilken måde.

Bestemmelsen forventes navnlig anvendt til at fastsætte regler om, hvordan 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 m.v., 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, stk. 1, 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 m.v. 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 efter forhandling med forsvarsministeren for at sikre, at der i videst muligt omfang fastsættes ensartede regler på tværs af sektorer.

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, §§ 7, 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 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). 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.

Forsvarsministeriet har lagt vægt på, at der foretages en direktivnær minimumsimplementering. Den foreslåede bestemmelse svarer med sproglige tilpasninger indholdsmæssigt til NIS 2-direktivets artikel 36, stk. 1, og skal således forstås og anvendes i overensstemmelse med direktivets forudsætninger.

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 § 21, stk. 1, nr. 2, og § 24, 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.

Om valg af ansvarssubjekt henvises til afsnit 3.5.2.3 i lovforslagets almindelige bemærkninger.

Det følger af det foreslåede *stk. 2,* at der kan pålægges selskaber m.v. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.

Den foreslåede bestemmelse indebærer, at selskaber m.v. (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 hvor der er pålagt en bøde for overtrædelse af databeskyttelsesforordningen eller databeskyttelsesloven, kan der ikke pålægges en bøde for overtrædelse af denne lov eller regler udstedt i medfør af loven, hvis overtrædelsen skyldes den samme adfærd som den, der var genstand for bøden i medfør af nævnte forordning eller databeskyttelsesloven.

Den foreslåede bestemmelse vil gennemføre NIS 2-direktivets artikel 35, stk. 2, hvoraf det følger, at tilsynsmyndighederne efter Europa-Parlamentets og Rådets forordning af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesforordningen) har pålagt en bøde i henhold til forordningens artikel 58, stk. 2, litra i, må de kompetente myndigheder efter NIS 2-direktivet ikke pålægge en bøde i henhold til NIS 2-direktivets artikel 34, der skyldes den samme adfærd som den, der var genstand for bøden efter databeskyttelsesforordningen.

Forsvarsministeriet har lagt vægt på, at der foretages en direktivnær minimumsimplementering. Den foreslåede bestemmelse svarer indholdsmæssigt til NIS 2-direktivets artikel 35, stk. 2, og skal således forstås og anvendes i overensstemmelse med direktivets forudsætninger.

De kompetente myndigheder vil fortsat kunne anvende øvrige håndhævelsesforanstaltninger i medfør af denne lov, uagtet at der måtte være pålagt en bøde for overtrædelse af databeskyttelseslovgivningen.

Det følger af den foreslåede *stk. 4*, at digitaliserings- og ligestillingsministeren kan fastsætte regler om, at offentlige myndigheder og institutioner m.v., som er omfattet af forvaltningslovens § 1, stk. 1 eller 2, uanset straffelovens § 27, stk. 2, kan straffes i anledning af overtrædelser, der begås ved udøvelse af virksomhed, der ikke svarer til eller kan sidestilles med virksomhed udøvet af private.

Den foreslåede bestemmelse vil delvist gennemføre NIS 2-direktivets artikel 34, stk. 7, hvoraf det følger, at uden at det berører tilsynsmyndighedernes beføjelser i henhold til artikel 32 og 33, kan hver enkelt medlemsstat fastsætte regler om, hvorvidt og i hvilket omfang administrative bøder kan pålægges offentlige forvaltningsorganer.

Den foreslåede bestemmelse indebærer, at digitaliserings- og ligestillingsministeren bemyndiges til at kunne fastsætte regler om, hvorvidt offentlige myndigheder skal kunne straffes efter de foreslåede straffebestemmelser i samme omfang som private aktører, uanset om der er tale om myndighedsudøvelse, eller om myndigheden udøver virksomhed, der svarer til eller kan sidestilles med virksomhed udøvet at private.

Om valg af ansvarssubjekt henvises til afsnit 3.5.2.3 i lovforslagets almindelige bemærkninger.

Det følger af det foreslåede *stk. 5*, at digitaliserings- og ligestillingsministeren kan fastsætte regler om bødeniveauer for offentlige myndigheders overtrædelse af loven.

Den foreslåede bestemmelse vil delvist gennemføre artikel 34, stk. 7, i NIS 2-direktivet, hvoraf det følger, at uden at det berører tilsynsmyndighedernes beføjelser i henhold til artikel 32 og 33, kan hver enkelt medlemsstat fastsætte regler om, hvorvidt og i hvilket omfang administrative bøder kan pålægges offentlige forvaltningsorganer.

Den foreslåede bestemmelse indebærer, at digitaliserings- og ligestillingsministeren kan fastsætte regler om bødelofter for offentlige myndigheders overtrædelse af loven. Det vil i de nærmere regler – i overensstemmelse med retsstillingen efter databeskyttelsesloven – eksempelvis kunne fastsættes, at bødelofterne for offentlige myndigheder skal være lavere end dem, der i øvrigt er fastsat for private virksomheder. I databeskyttelsesloven er der eksempelvis for visse overtrædelser forudsat et bødeloft på 2 pct. af myndighedens driftsbevilling, dog maksimalt 8 mio. kr. For andre overtrædelser er forudsat et bødeloft på 4 pct. af driftsbevillingen, dog maksimalt 16 mio. kr.

Det følger af det foreslåede *stk. 6,* at der i regler udstedt i medfør af loven kan fastsættes straf i form af bøde for overtrædelse af regler udstedt i medfør af loven.

Med bestemmelsen bemyndiges vedkommende minister til at fastsætte straf i form af bøde for overtrædelse af bestemmelser i regler, som udstedes i medfør af § 6, stk. 3, § 8, § 11, stk. 7 og § 30.

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, 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.

Der henvises i øvrigt til afsnit 3.5 i lovforslagets almindelige bemærkninger.

*Til § 33*

Bestemmelsen fastsætter tidspunktet for lovens ikrafttræden.

Det foreslås, at loven træder i kraft den 1. marts 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 4 måneder efter direktivets implementeringsfrist.

*Til § 34*

Lov nr. 436 af 8. maj 2018 om net- og informationssikkerhed for domænenavnssystemer og visse digitale tjenester gennemfører dele af 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).

Med artikel 44 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) ophæves NIS 1-direktivet.

Det følger af den foreslåede *§ 34*, 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. marts 2025.

*Til § 35*

Lov nr. 437 af 8. maj 2018 om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter m.v. gennemfører dele af 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).

Med artikel 44 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) ophæves NIS 1-direktivet.

Det følger af den foreslåede *§ 35*, at lov nr. 437 af 8. maj 2018 om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter m.v. ophæves.

Bestemmelsen vil indebære, at loven ophæves den 1. marts 2025. Med lovens ophævelse bortfalder bekendtgørelse nr. 454 af 8. maj 2018 om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter.

*Til § 36*

Lov nr. 440 af 8. maj 2018 om krav til sikkerhed for net- og informationssystemer inden for sundhedssektoren gennemfører dele af Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (NIS 1-direktivet).

NIS 1-direktivet blev 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.

Med artikel 44 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) ophæves NIS 1-direktivet.

Det følger af den foreslåede *§ 36*, 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. marts 2025. Med lovens ophævelse bortfalder de ovenfor nævnte bekendtgørelser.

*Til § 37*

Lov nr. 441 af 8. maj 2018 om sikkerhed i net- og informationssystemer i transportsektoren gennemfører dele af 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).

Med artikel 44 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) ophæves NIS 1-direktivet.

Det følger af den foreslåede *§ 37*, 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. marts 2025.

*Til § 38*

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.