Kapitel 1 *Formål, anvendelsesområde og definitioner*

Kapitel 2 *Kategoriseringsbestemmelser*

Kapitel 3 *Styrkelse af virksomheders modstandsdygtighed*

Organisatorisk beredskab

Fysisk sikring

Cybersikkerhed

Overordnede koordinerende og operative opgaver

Sektorberedskabsniveauer og sektorberedskabsforanstaltninger

Kapitel 4 *Underretningspligt*

Kapitel 5 *Sikkerhedsgodkendelser*

Kapitel 6 *Gebyrer*

Kapitel 7 *Tilsyn*

Kapitel 8 *Håndhævelse*

Kapitel 9 *Gensidig bistand*

Kapitel 10 *Fortrolighed, udveksling af oplysninger og digital kommunikation*

Kapitel 11 *Andre bestemmelser*

Kapitel 12 *Straf*

Kapitel 13 *Ikrafttrædelse*

Kapitel 14 Ændringer i anden lovgivning

Kapitel 15 *Territorialbestemmelser*

Forslag

til

Lov om styrket beredskab i energisektoren[1)]

Kapitel 1

Formål, anvendelsesområde og definitioner

§ 1. Lovens formål er at fastsætte en ramme for modstandsdygtighed og beredskab i forhold til naturskabte, menneskeskabte og teknologiske trusler, der kan true eller skade energiforsyningen gennem regler om organisatorisk beredskab, fysisk sikring og cybersikkerhed for virksomheder i energisektoren.

Stk. 2. Loven har endvidere til formål at fastsætte en ramme for myndighedstilsyn med overholdelsen af disse regler og grundlag for samarbejde mellem virksomheder, myndigheder samt øvrige organisationer, der varetager roller i planlægningen af beredskabet og håndteringen af beredskabshændelser i energisektoren.

§ 2. Denne lov finder anvendelse på følgende virksomheder, når disse leverer deres tjenester eller udfører deres aktivitet inden for Danmark:

1) Elektricitetsvirksomheder.
2) Distributionssystemoperatører.
3) Transmissionssystemoperatører.
4) Elproducenter.
5) Udpegede elektricitetsmarkedsoperatører.

[1)] Loven indeholder bestemmelser, der 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 samt dele af 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), EU-Tidende 2022, nr. L 333 side 164.

6) Markedsdeltagere der leverer tjenester, der vedrører aggregering, fleksibelt elforbrug eller energilagring.
7) 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.
8) Operatører af fjernvarme eller fjernkøling.
9) Olierørledningsoperatører.
10) Operatører af olieproduktionsanlæg, -raffinaderier og -behandlingsanlæg, olielagre og olietransmission.
11) Centrale lagerenheder.
12) Gasforsyningsvirksomheder.
13) Lagersystemoperatører.
14) LNG-systemoperatører.
15) Naturgasvirksomheder.
16) Operatører af naturgasraffinaderier og –behandlingsanlæg.
17) Operatører inden for brintproduktion, -lagring og –transmission.
18) Operatører af tankstationer, der er ansvarlige for forvaltningen og driften af en tankstation.

Stk. 2. Loven finder kun anvendelse for de stk. 1 nr. 1-8, 10, 12, og 18 nævnte virksomheder, såfremt virksomheden:

1) Årligt producerer, forbruger eller kontrollerer mere end 25 MW elektricitet.
2) I 2 ud af 3 sidste år har solgt mere end 13,9 GWh fjernvarme
3) Årligt producerer eller injicerer mere end 26 mio. Nm^3 gas i et gasnet.
4) Olieterminaler og lagre med kapacitet på 100.000 m^3 eller derover.
5) Opererer en eller flere tankstationer der sammenlagt har et årligt salg af olieprodukter på 600.000 m3 eller derover, eller som opererer flere end 100 tankstationer på nationalt plan.

Stk. 3. Loven finder anvendelse uanset stk. 2. for virksomheder:

1) Der har positiv lagringsforpligtigelse efter Olieberedskabsloven
2) Nævnt i stk. 1, men som falder under grænserne i stk. 2, såfremt virksomheden beskæftiger minimum 50 ansatte eller har en årlig omsætning på minimum 10 mio. EUR og en årlig samlet balance på minimum 10 mio. EUR.

Stk. 4. Kapitel 5 om sikkerhedsgodkendelser og baggrundskontrol i energisektoren og § 18 om gebyrbetaling for anmodning om betaling ved indgivelse af ansøgninger og dispensationer finder anvendelse på alle virk-

somheder, organisationer, fonde, erhvervsdrivende fonde der varetager opgaver som direkte led eller i forbindelse med leveringen af de stk. 1 nævnte tjenester.

Stk. 5. Loven gælder på land- og søterritoriet, den eksklusive økonomiske zone samt kontinentalsokkelen.

§ 3. I denne lov forstås ved følgende:

1) Aggregering: Funktion, der varetages af en fysisk eller juridisk person, der samler flere kunders forbrug eller producerede elektricitet til salg, køb eller auktion på et elektricitetsmarked. Aggregering er ikke levering af elektricitet.
2) Centrale lagerenheder: Organ eller tjeneste, som er tildelt beføjelser til at handle med henblik på at erhverve, holde eller sælge olielagre, herunder beredskabslager og specifikke lagre.
3) Cyberhændelse: 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.
4) Cybersikkerhed: De aktiviteter, der er nødvendige for at beskytte net- og informationssystemer, brugerne af sådanne systemer og andre personer berørt af cybertrusler.
5) 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.
6) Distributionssystemoperatører: En fysisk eller juridisk person, der er ansvarlig for driften, vedligeholdelsen og om nødvendigt udbygningen af distributionssystemet i et givet område samt i givet fald dets sammenkoblinger med andre systemer og for at sikre, at systemet på lang sigt kan tilfredsstille en rimelig efterspørgsel efter distribution af elektricitet eller gas.
7) Elektricitetsvirksomheder: En fysisk eller juridisk person, der driver mindst en af følgende former for virksomhed: produktion, transmission, distribution, aggregering, fleksibelt elforbrug, energilagring, levering eller køb af elektricitet, og som er ansvarlig for de kommercielle, tekniske eller vedligeholdelsesmæssige opgaver i forbindelse med disse aktiviteter, men som ikke er slutkunde der varetager salg, herunder videresalg, af elektricitet til kunder.

8) Elproducenter: En fysisk eller juridisk person, der fremstiller elektricitet.
9) Energilagring: I elektricitetssystemet, udsættelse af den endelige anvendelse af elektricitet til et senere tidspunkt end det, hvor den blev produceret, eller konvertering af elektrisk energi til en energiform, der kan lagres, lagringen af sådan energi og den efterfølgende rekonvertering af sådan energi til elektrisk energi eller anvendelse som anden energibærer.
10) Fleksibelt elforbrug: Ændringer i en slutkundes elforbrug i forhold til det normale eller aktuelle forbrugsmønster som reaktion på markedssignaler, herunder som reaktion på tidspunktafhængige elpriser eller finansielle incitamenter, eller som reaktion på accept af slutkundens bud om at sælge en forbrugsreduktion eller -forøgelse til en bestemt pris på et organiseret marked, hvad enten dette sker alene eller gennem aggregering.
11) Gasforsyningsvirksomheder: Enhver fysisk eller juridisk person, der varetager forsyningsopgaven.
12) Hændelse: En begivenhed, herunder en cyberhændelse, der har potentiale til i betydelig grad at forstyrre, eller som forstyrrer, leveringen af en væsentlig tjeneste, herunder når den påvirker de nationale systemer, der sikrer retsstatsprincippet.
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) Lagersystemoperatører: Enhver fysisk eller juridisk person, der foretager oplagring af gas og er ansvarlig for driften af en gaslagerfacilitet
18) LNG-systemoperatører: Enhver fysisk eller juridisk person, der foretager flydendegørelse af naturgas eller import, losning og forgasning af LNG og er ansvarlig for driften af en LNG-facilitet.
19) Markedsdeltagere der leverer tjenester, der vedrører aggregering, fleksibelt elforbrug eller energilagring: En fysisk eller juridisk per-

son, der køber, sælger eller producerer elektricitet, der udfører aggregering, eller der er en operatør af tjenester vedrørende fleksibelt elforbrug eller energilagringstjenester, herunder ved afgivelse af handelsordrer, på et eller flere elektricitetsmarkeder, herunder på balanceringsenergimarkeder.

20) Modstandsdygtighed: En enhed evne til at forebygge, beskytte mod, reagere på, modstå, afbøde, absorbere, tilpasse sig og sikre genopretning efter en hændelse.

21) Naturgasvirksomheder: Enhver fysisk eller juridisk person, der driver mindst en af følgende former for virksomhed: produktion, transmission, distribution, forsyning, køb eller oplagring af naturgas, herunder LNG, og som er ansvarlig for de kommercielle, tekniske og/eller vedligeholdelsesmæssige opgaver i forbindelse med disse aktiviteter, men som ikke er endelig kunde.

22) 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.

23) Nærvedhændelse: En begivenhed, der kunne have bragt tilgængeligheden, autenticiteten, integriteten eller fortroligheden af lagrede, overførte eller behandlede data eller af de tjenester, der tilbydes af eller er tilgængelige via net- og informationssystemer, i fare, men som det lykkedes at forhindre, eller som ikke materialiserede sig.

24) Operatører af fjernvarme eller fjernkøling: Operatører af distribution af termisk energi i form af damp, varmt vand eller afkølede væsker

fra centrale eller decentrale produktionssteder gennem et net til flere bygninger eller anlæg til anvendelse ved rum- eller procesopvarmning eller –køling.

25) Organiseret marked:

a) Et multilateralt system, der samler eller faciliterer samlingen af flere tredjeparters købs- og salgsinteresser i engrosenergiprodukter på en måde, der fører til indgåelse af en kontrakt

b) Ethvert andet system eller enhver anden facilitet, hvor flere købs- og salgsinteresser i engrosenergiprodukter tilhørende tredjeparter kan interagere på en måde, der fører til indgåelse af en kontrakt.

Dette omfatter elektricitets- og gasbørser, mæglere og andre personer, der erhvervsmæssigt arrangerer transaktioner, og markedspladser, herunder ethvert reguleret marked, en MHF eller en OHF.

26) 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.

27) Risikovurdering: Den samlede proces med henblik på at bestemme arten og omfanget af en risiko ved at identificere og analysere potentielle relevante trusler, sårbarheder og farer, der kunne føre til en hændelse, og ved at evaluere det potentielle tab eller den potentielle forstyrrelse af leveringen af en væsentlig tjeneste forårsaget af denne hændelse.

28) Transmissionssystemoperatører: En fysisk eller juridisk person, der er ansvarlig for driften, vedligeholdelsen og om nødvendigt udbygningen af transmissionssystemet i et givet område samt i givet fald dets sammenkoblinger med andre systemer og for at sikre, at systemet på lang sigt kan tilfredsstille en rimelig efterspørgsel efter transmission af elektricitet eller gas.

29) Udpegede elektricitetsmarkedsoperatører: En markedsoperatør, der af den kompetente myndighed er blevet udpeget til at udføre opgaver i forbindelse med den fælles day-ahead- eller intraday-kobling.

30) 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.

31) Væsentlig tjeneste: En tjeneste, der er afgørende for opretholdelsen af vitale samfundsmæssige funktioner, økonomiske aktiviteter, folkesundhed og offentlig sikkerhed eller miljøet.

Kapitel 2
Identificering og kategorisering af virksomheder

§ 4. Klima-, energi- og forsyningsministeren identificerer kritiske virksomheder samt kritiske systemer og anlæg i energisektoren, der anvendes til at levere virksomhedens tjenester.

Stk. 2. Klima- energi, og forsyningsministeren fastsætter nærmere regler om identifikation og kategorisering af virksomheder og virksomheders systemer og anlæg, som anvendes til levering af virksomhedens tjenester.

§ 5. Virksomheder betragtes som kritiske enheder af særlig europæisk betydning, når virksomheden opfylder alle af følgende betingelser:

1) Er blevet identificeret som kritisk virksomhed efter § 4, stk. 1.
2) Leverer de samme eller lignende væsentlige tjenester til eller i seks eller flere medlemsstater.
3) Er blevet underrettet om, at virksomheden betragtes som en kritisk enhed af særlig europæisk betydning i overensstemmelse med EU-regler.

Stk. 2. Klima-, energi- og forsyningsministeren underretter virksomheder, at de betragtes som kritiske enheder af særlig europæisk betydning i energisektoren i overensstemmelse med EU-regler.

Stk. 3. Klima-, energi- og forsyningsministeren fastsætter nærmere regler til brug for udpegelsen af kritiske enheder af særlig europæisk betydning.

Stk. 4. Klima-, energi- og forsyningsministeren kan fastsætte regler om særlige forpligtelser for virksomheder af særlig europæisk betydning.

Kapitel 3
Virksomheders modstandsdygtighed og beredskab

Organisatorisk beredskab

§ 6. Virksomheder skal foretage nødvendig beredskabsplanlægning og gennemføre passende organisatoriske foranstaltninger for at beskytte leveringen af deres tjenester og sikre effektiv genoprettelse af deres tjenester.

Stk. 2. Klima-, energi- og forsyningsministeren fastsætter efter forhandling med forsvarsministeren nærmere regler om det organisatoriske beredskab, jf. stk. 1, herunder regler om:

1) Ledelsesansvar, herunder krav om godkendelse af virksomhedens risiko- og sårbarhedsvurdering samt beredskabsplaner, tilsynsrapporter og leverandørkontrakter.
2) At ledelsesorganer tilegner sig viden og kundskaber inden for risiko- og sårbarhedsstyring.
3) Identifikations- og adgangskontrolpolitikker for beskyttelse mod uautoriseret adgang.
4) Udpegelse af personer til at varetage specifikke beredskabsroller.
5) Politikker for informationssystemsikkerhed.
6) Politikker for og udarbejdelse af risiko- og sårbarhedsvurderinger, som omfatter nyindkøb, projekter og etablering af net- og informationssystemer og anlæg.
7) Forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem virksomheden og dens direkte leverandører eller tjenesteudbydere.
8) Beredskabsplaner og beredskabsplanlægning for håndtering af hændelser.
9) Øvelsesplanlægning, herunder afholdelse af øvelser og træning af beredskabsforanstaltninger.
10) Beredskabstræning, cybersikkerhedsadfærd- og sikkerhedsuddannelse af ansatte i virksomheden.
11) Kapacitet til at modtage og videreformidle advarsler om trusler.
12) Tilmelding til en it-sikkerhedstjeneste.

Fysisk sikring

§ 7. Virksomheder skal træffe passende foranstaltninger for at opretholde nødvendig fysisk sikring af lokationer og anlæg, der bruges til at levere virksomhedens tjenester, eller hvorfra drift af net- og informationssystemer finder sted.

Stk. 2. Klima-, energi- og forsyningsministeren fastsætter nærmere regler om fysisk sikring, jf. stk. 1, herunder regler om:

1) Forhindring af at hændelser indtræffer under behørig hensyntagen til katastroferisikoreduktions- og klimatilpasningsforanstaltninger.
2) Etablering af foranstaltninger til overvågning, detektion og reaktion i forbindelse med uautoriseret adgang til og på anlæg og lokationer.
3) Tilstrækkelig fysisk sikring af virksomhedens anlæg og lokationer, herunder kontrolrum og kontrolrummets arbejdsstationer.
4) Håndtering af hændelser og genopretning efter hændelser.
5) Medarbejdersikkerhedsstyring.

Cybersikkerhed

§ 8. Virksomheder skal foretage nødvendig planlægning og træffe passende cybersikkerhedsforanstaltninger for at sikre beskyttelsen af net- og informationssystemer, der bruges til at levere virksomhedens tjenester.

Stk. 2. Klima-, energi- og forsyningsministeren fastsætter efter forhandling med forsvarsministeren nærmere regler for cybersikkerhedsforanstaltninger jf. stk. 1, herunder regler om følgende:

1) Forvaltning af net- og informationssystemer og passende teknisk sikkerhed til beskyttelse af enheder med adgang til virksomhedens netværk.
2) Etablering af netværks- og infrastruktursikkerhed, herunder principper for netværksarkitektur og -topologi med henblik på at minimere risici for virksomhedens net- og informationssystemer.
3) Sikkerhedskrav til geografisk placering af drift af net- og informationssystemer.
4) Sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer.

5) Backup-styring og genopretning af net- og informationssystemer til sikring af driftskontinuitet for leveringen af tjenesten.
6) Etablering af logning til at understøtte alarmer, efterforskningsarbejde, hændelseshåndtering og monitorering af uregelmæssigheder i net- og informationssystemer.
7) Etablering af procedurer for løbende kontrol af cybersikkerheden i og omkring net- og informationssystemer.
8) Brug af sikret tale-, video- og tekstkommunikation og sikrede nødkommunikationssystemer.
9) Brug af kryptering samt politikker og procedurer, der skal understøtte sikkerheden og fortroligheden af net- og informationssystemer, der er kritiske for leveringen af virksomhedens tjenester.
10) Brug af multifaktorautentificering eller kontinuerlig autentificering og adgangsbeskyttelse til sikring mod uautoriseret adgang til virksomhedernes net- og informationssystemer.
11) Foranstaltninger til forebyggelse og håndtering af hændelser.

§ 9. Klima-, energi- forsyningsministeren kan efter forhandling med forsvarsministeren fastsætte regler om, at virksomheder skal anvende særlige IKT-produkter, -tjenester og -processer, der er udviklet af virksomheden eller indkøbt fra tredjeparter, og som er certificeret i henhold til en europæisk cybersikkerhedscertificeringsordning for at påvise overensstemmelse med bestemte krav i § 8, stk. 1, eller i regler om krav til foranstaltninger fastsat i medfør af § 8, stk. 2.

Koordinerende og operative opgaver

§ 10. Klima-, energi- og forsyningsministeren fastsætter nærmere regler om ministerens og Energinets varetagelse af, koordinerende planlægningsmæssige og operative opgaver vedrørende beredskab, jf. § 6, stk. 1 og stk. 2, § 7, stk. 1 og stk. 2 og § 8, stk. 1 og stk. 2.

Sektorberedskabsniveauer og sektorberedskabsforanstaltninger

§ 11. Klima-, energi- forsyningsministeren kan, i en beredskabssituation omfattende sikkerhedsrelaterede hændelser, fastsætte og udmelde sektorberedskabsniveauer for hele energisektoren eller en eller flere delsektorer.

Stk. 2. I en beredskabssituation omfattende sikkerhedsrelaterede hændelser kan klima-, energi- forsyningsministeren fastsætte og pålægge sektorberedskabsforanstaltninger for hele energisektoren, for en eller flere delsektorer, eller for en eller flere virksomheder eller anlæg.

Stk. 3. I en beredskabssituation kan klima-, energi- forsyningsministeren bestemme, at de i stk. 2 nævnte foranstaltninger samt andre foranstaltninger, der skal foretages efter loven eller regler udstedt i medfør af loven, midlertidigt skal intensiveres og suppleres med yderligere foranstaltninger for at sikre en hurtig, koordineret og prioriteret krisehåndtering, herunder gennemførelse af myndighedernes beslutninger i den nationale krisehåndtering.

Stk. 4. I en beredskabssituation omfattende sikkerhedsrelaterede hændelser kan Energinet, i særlige tilfælde, hvor klima-, energi- forsyningsministeren ikke kan fastsætte og udmelde sektorberedskabsniveauer og foranstaltninger, jf. stk. 1, 2 og 3 varetage opgaven på ministerens vegne.

Kapitel 4
Underretningspligt

§ 12. Klima-, energi og forsyningsministeren kan fastsætte regler for underretning og indrapportering af hændelser, væsentlige cybertrusler og nærvedhændelser.

§ 13. Klima-, energi- og forsyningsministeren kan fastsætte regler for virksomheders pligt til at underrette modtagere af deres tjenester, myndigheder eller juridiske personer som udfører myndighedsopgaver om trusler eller hændelser der kan påvirke eller har potentiale til at påvirke virksomhedens levering af tjenester.

§ 14. Klima-, energi- og forsyningsministeren kan efter høring af en virksomhed, der er ramt af en hændelse, informere offentligheden om hændelsen, hvis offentliggørelsen er nødvendig for at forebygge eller håndtere

hændelsen, eller hvor offentliggørelse af hændelsen på anden vis er i offentlighedens interesse.

Stk. 2. Klima-, energi- og forsyningsministeren kan i situationer efter stk. 1, kræve at virksomheden foretager offentliggørelse af hændelsen.

§ 15. Enhver kan underrette Klima-, Energi- og Forsyningsministeriet om væsentlige hændelser, cybertrusler og nærvedhændelser, der negativt påvirker eller vurderes at kunne påvirke tilgængelighed, integritet eller fortrolighed af data, informationssystemer, digitale netværk eller digitale servicer i energisektoren.

Kapitel 5
Sikkerhedsgodkendelser og baggrundskontrol

§ 16. Klima-, energi- og forsyningsministeren kan efter forhandling med justitsministeren fastsætte regler om, at personer, der har direkte adgang til at påvirke forsyningen i energisektoren, skal sikkerhedsgodkendes af Klima-, Energi- og Forsyningsministeriet. Klima-, energi- og forsyningsministeren kan endvidere efter forhandling med justitsministeren fastsætte regler om ansøgning om, betingelser for og meddelelse og tilbagekaldelse af sikkerhedsgodkendelser.

Stk. 2. Klima-, energi- og forsyningsministeren kan efter forhandling med justitsministeren fastsætte nærmere regler om, på hvilke betingelser virksomheder kan få foretaget baggrundskontrol af personer i energisektoren med henblik på at vurdere en potentiel sikkerhedsrisiko for virksomheden. Baggrundskontrollen kan angå personer, der:

1) varetager følsomme opgaver i eller til fordel for virksomheden, navnlig vedrørende virksomhedens modstandsdygtighed
2) er bemyndiget til at få direkte adgang eller fjernadgang til virksomhedens enheds lokaler, oplysninger eller kontrolsystemer, herunder i forbindelse med virksomhedens sikkerhed
3) overvejes ansat i stillinger, der indebærer opgavevaretagelse efter nr. 1 og/eller nr. 2.

Kapitel 6
Gebyrer

§ 17. Virksomheder betaler halvårligt et fast beløb til Klima-, Energi- og Forsyningsministeriet til dækning af omkostninger til tilsyn med virksomhederne efter reglerne i denne lov eller efter regler udstedt i medfør af loven.

Stk. 2. Virksomheder betaler ved ad-hoc tilsyn halvårligt et beløb til Klima-, Energi- og Forsyningsministeriet til dækning af omkostningerne til ad-hoc tilsynet med virksomheden efter reglerne i denne lov eller efter regler udstedt i medfør af loven.

Stk. 3. Klima-, energi- og forsyningsministeren fastsætter regler om størrelsen, betaling og opkrævning af beløb efter stk. 1 og 2, herunder om fordelingen af omkostningerne på kategorier af virksomheder.

§ 18. Virksomheder betaler ved indgivelse af ansøgninger eller dispensationer halvårligt et beløb for behandling af ansøgninger og dispensationer efter reglerne i denne lov eller efter regler udstedt i medfør af loven.

Stk. 2. Klima-, energi- og forsyningsministeren fastsætter regler om størrelsen, betaling og opkrævning af beløb efter stk. 1.

Kapitel 7
Tilsyn

§ 19. Klima-, energi- og forsyningsministeren fører tilsyn med, om virksomhederne opfylder sine forpligtelser i henhold til loven og regler fastsat i medfør af loven.

Stk. 2. Klima-, Energi og Forsyningsministeriet kan som led i sin tilsyns forpligtigelse anvende følgende tilsyns- og kontrolforanstaltninger:

1) Foretage tilsyn og kontrol hos virksomheden, ved at inspicere de lokaler virksomheden bruger til at levere sine tjenester og foretage stikprøvekontroller.
2) Foretage regelmæssige kontrol- og tilsynsbesøg hos virksomheder.
3) Foretage ad hoc-tilsyn.
4) Foretage sikkerhedsscanninger og penetrationstest af virksomhedens net- og informationssystemer samt fysiske lokationer. Klima-, Energi- og Forsyningsministeriet er ansvarlig for eventuelle skader virksomheden pådrager sig i forbindelse med disse scanninger og tests.

5) Kræve at få udleveret oplysninger og dokumentation, der er nødvendige for at vurdere foranstaltningerne vedrørende organisatorisk beredskab, fysisk sikring og cybersikerhed, som virksomheden har indført efter loven og regler udsted i medfør af loven.
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.

Stk. 3. Klima-, energi- og forsyningsministeren kan fastsætte nærmere regler om tilsyn og kontrol af virksomhederne, herunder omfanget, udførelsen og hyppigheden af tilsyns- og kontrolbesøg.

Stk. 4. Klima-, energi- og forsyningsministeren kan fastsætte regler om udlevering og dokumentation af tilsynsmateriale og formkrav til tilsynsmateriale, herunder regler om hvilke sprog materialet skal udarbejdes på.

§ 20. Rådgivende missioner som er nedsat i medfør af CER-direktivet kan efter tilladelse fra klima-, energi-, og forsyningsministeren føre tilsyn med virksomheder som betragtes som enheder af særlig europæisk betydning efter § 5, stk. 1.

Stk. 2. Rådgivende missioner kan anvende tilsynsforanstaltninger efter § 19, stk. 2, nr. 1-7, i det omfang anvendelsen af foranstaltningerne er nødvendige for at gennemføre den pågældende rådgivende mission.

Skt. 3. Rådgivende missioners tilsynsforanstaltninger efter § 19, stk. 2, nr. 1-7, kan begrænses i det omfang, det er nødvendigt til beskyttelse af væsentlige hensyn til følgende:

1) Statens sikkerhed eller rigets forsvar.
2) Rigets udenrigspolitiske eller udenrigsøkonomiske interesser, herunder forholdet til fremmede magter eller mellemfolkelige institutioner.
3) Private og offentlige interesser, hvor hemmeligholdelse efter forholdets særlige karakter er påkrævet.

Skt. 4. Klima-, energi og forsyningsministeren træffer afgørelse om begrænsning af rådgivende missioners tilsynsforanstaltninger.

Kapitel 8
Håndhævelse

§ 21. Klima-, Energi- og Forsyningsministeriet kan over for en virksomhed anvende følgende håndhævelsesforanstaltninger:

1) Påbyde virksomheden at træffe foranstaltninger, der er nødvendige for at forhindre eller afhjælpe en hændelse.
2) Meddele påbud og forbud, der anses nødvendige for at sikre overholdelsen af krav fastsat i loven, regler i medfør af loven eller Den Europæiske Unions forordninger og direktiver, som regulerer beredskabsforhold inden for energisektoren.
3) Påbyde virksomheden at underrette de fysiske eller juridiske personer, til hvilke den leverer tjenester eller udfører aktiviteter, som potentielt kan være berørt af en væsentlig cybertrussel, om denne trussels karakter samt om eventuelle beskyttelsesforanstaltninger eller afhjælpende foranstaltninger, som de fysiske eller juridiske personer kan træffe som reaktion på denne trussel.
4) Påbyde virksomheden at udpege en person med ansvar for i en nærmere fastsat periode at føre tilsyn med virksomhedens overholdelse af §§ 6-9 og §§ 12-14, samt regler udstedt i medfør heraf.
5) Påbyde virksomheden i ikke-anonymiseret form og på en nærmere angiven måde at offentliggøre afgørelser om håndhævelsesforanstaltninger efter nr. 1-4 samt resumeer af domme eller bødevedtagelser, hvor der idømmes eller vedtages en bøde.

§ 22. Klima-, energi- og forsyningsministeren kan ved manglende opfyldelse af påbud efter § 21, stk. 1, nr. 1-5, påbyde virksomheder at få foretaget en revision af net- og informationsforanstaltninger, modstandsdygtighedsforanstaltninger og kritiske systemer ved en uafhængig revisor. Udgifterne til revisionen afholdes af virksomheden.

Stk. 2. Klima-, energi- og forsyningsministeren kan påbyde virksomheder at gennemføre tiltag, som på baggrund af en revision efter stk. 1, vurderes nødvendige for at opretholde et tilstrækkeligt beredskab.

Stk. 3. Klima-, energi- og forsyningsministeren kan fastsætte nærmere regler for, hvordan den uafhængige revisor udpeges og godkendes samt omfanget af revisionen.

§ 23. Har de håndhævelsesforanstaltninger, der er pålagt i medfør af § 21, nr. 1-4 og § 22, stk. 1 og 2, vist sig at være utilstrækkelige, kan klima-, energi- og forsyningsministeren fastsætte en frist, inden for hvilken virksomheden skal foretage de nødvendige tiltag for at afhjælpe manglerne eller opfylde myndighedernes krav. Er tiltagene ikke foretaget inden for den fastsatte frist, kan klima-, energi- og forsyningsministeren træffe afgørelse om:

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

Stk. 2. Midlertidige suspensioner eller forbud, som er pålagt i medfør af stk. 1, kan kun anvendes, indtil virksomheden træffer de nødvendige foranstaltninger til at afhjælpe de mangler eller til at opfylde de krav, som gav anledning til, at foranstaltningerne blev anvendt.

Stk. 3. En afgørelse efter stk. 1 kan af virksomheden eller den fysiske person, afgørelsen vedrører, forlanges indbragt for domstolene. Klima-, energi- og forsyningsministeren anlægger i givet fald sag mod den virksomhed eller person, som har forlangt sagen indbragt.

Stk. 4. Klima-, energi- og forsyningsministeren kan efter forhandling med forsvarsministeren fastsætte nærmere regler om, hvilke certificeringer og godkendelser der er omfattet af stk. 1, nr. 1.

§ 24. Inden Klima- Energi- og Forsyningsministeriet træffer afgørelse om at anvende håndhævelsesforanstaltninger efter §§ 21-23, underrettes den berørte virksomhed om de påtænkte håndhævelsesforanstaltninger og begrundelsen herfor. Klima- Energi- og Forsyningsministeriet skal give virksomheden en rimelig frist til at fremsætte bemærkninger, undtagen i tilfælde, hvor formålet med foranstaltningen ellers ville forspildes.

Kapitel 9
Gensidig bistand om cyber

§ 25. Hvor en enhed leverer tjenester i mere end én medlemsstat i Den Europæiske Unions, eller hvor virksomheden leverer tjenester i en eller flere medlemsstater, og virksomhedens net- og informationssystemer er

beliggende i en eller flere andre medlemsstater, samarbejder Klima-, Energi- og Forsyningsministeriet med de andre medlemsstaters kompetente myndigheder i relevant omfang. Samarbejdet, indebærer at:

1) Klima-, Energi- og Forsyningsministeriet via det centrale kontaktpunkt, der er nedsat i medfør af NIS 2-direktivet, underretter de kompetente myndigheder i relevante medlemsstater om anvendte tilsyns- og håndhævelsesforanstaltninger.
2) Klima-, Energi- og Forsyningsministeriet kan anmode en anden medlemsstats kompetente myndigheder om at anvende tilsyns- og håndhævelsesforanstaltninger.
3) Klima-, Energi- og Forsyningsministeriet yder i rimeligt omfang bistand til en anden medlemsstats kompetente myndighed efter modtagelse af en begrundet anmodning herom.

Stk. 2. Klima-, Energi- og Forsyningsministeriet kan efter nærmere aftale gennemføre fælles tilsynstiltag med kompetente myndigheder fra andre medlemsstater i Den Europæiske Union.

Kapitel 10
Fortrolighed, udveksling af oplysninger og digital kommunikation

§ 26. Informationer om sikkerhedsgodkendelse og baggrundskontrol, samt forhold vedrørende organisatorisk beredskab, fysisk sikring og cybersikkerhed i virksomheder omfattet af loven og i energisektoren generelt, er fortrolige, hvis:

1) Informationerne indgår i vurderingen af sikkerhedsgodkendelser
2) Informationerne indgår i vurderingen af baggrundskontrol
3) Informationerne er væsentlige af hensyn til driften af virksomheden
4) Informationerne er væsentlige af hensyn til driften andre virksomheder omfattet af loven
5) Informationerne er væsentlige af hensyn til driften af energiforsyningen lokalt, regionalt, nationalt eller på europæisk niveau.

Stk. 2. Klima-, energi- og forsyningsministeren fastsætter nærmere regler om, hvordan virksomheder og myndigheder opbevarer, behandler og deler informationer som nævnt i stk. 1.

§ 27. Underretning efter § 15 er undtaget fra aktindsigt efter lov om offentlighed i forvaltningen og partsaktindsigt efter forvaltningsloven.

§ 28. Klima-, Energi- og Forsyningsministeriet og andre relevante myndigheder kan videregive oplysninger til andre medlemsstaters myndigheder og til institutioner i Den Europæiske Union for at varetage de myndighedsopgaver som følger af denne lov, NIS 2-direktivet eller CER-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. Klima-, energi- og forsyningsministeren kan fastsætte regler om digital kommunikation, herunder om anvendelsen af bestemte it-systemer og særlige digitale formater samt digital signatur eller lignende.

Kapitel 11
Andre bestemmelser

§ 31. Energiklagenævnet behandler klager over afgørelser truffet af klima-, energi- og forsyningsministeren eller anden statslig myndighed efter denne lov eller regler udstedt i henhold til loven.

Stk. 2. Afgørelser nævnt i stk. 1 kan ikke indbringes for anden administrativ myndighed end Energiklagenævnet. Afgørelserne kan ikke indbringes for domstolene, før den endelige administrative afgørelse foreligger.

Stk. 3. Klagen skal være indgivet skriftligt til Energiklagenævnet inden 4 uger fra tidspunktet, hvor afgørelsen er meddelt. Er afgørelsen offentligt bekendtgjort, regnes fristen dog altid fra bekendtgørelsen. Udløber klagefristen på en lørdag eller en helligdag, forlænges fristen til den følgende hverdag.

Stk. 4. Energiklagenævnets formand kan efter nærmere aftale med nævnet træffe afgørelse på nævnets vegne i sager, der behandles efter denne lov eller regler udstedt i henhold til loven.

Stk. 5. Søgsmål til prøvelse af afgørelser truffet af Energiklagenævnet efter loven eller de regler, der udstedes efter loven, skal være anlagt inden 6 måneder efter, at afgørelsen er meddelt den pågældende. Er afgørelsen offentligt bekendtgjort, regnes fristen dog altid fra bekendtgørelsen.

Stk. 6. Energiklagenævnet kan i forbindelse med behandling af en klage, indhente oplysninger der er nødvendige for behandling af klagen fra virksomheder omfattet af loven samt myndigheder der træffer afgørelser efter loven eller regler udstedt i medfør af loven.

§ 32. Klima-, energi- og forsyningsministeren kan fastsætte regler om adgangen til at klage over afgørelser, der efter loven eller regler udstedt i henhold til loven træffes af klima-, energi- og forsyningsministeren, herunder at visse afgørelser ikke skal kunne indbringes for Energiklagenævnet,

Stk. 2. Erhvervsministeren kan fastsætte regler om

1) at kommunikation med Energiklagenævnet skal ske digitalt. Ministeren kan herunder udstede regler om anvendelse af et bestemt digitalt system. Ved fastsættelse af regler efter 1. pkt. fastsætter ministeren regler om fritagelse for obligatorisk anvendelse for visse personer og virksomheder,
2) betaling af gebyr ved indbringelse af en klage for Energiklagenævnet,
3) Energiklagenævnets sammensætning ved nævnets behandling af afgørelser efter denne lov eller regler udstedt i medfør af loven.

§ 33. Klima-, energi- og forsyningsministeren kan bemyndige en under ministeriet oprettet institution eller anden myndighed til at udøve de beføjelser, der i denne lov er tillagt ministeren.

§ 34. Klima-, energi- og forsyningsministeren kan fastsætte regler eller træffe bestemmelser med henblik på at gennemføre eller anvende internationale konventioner og EU-regler om forhold, der er omfattet af denne lov, herunder forordninger, direktiver og beslutninger om beredskab og beskyttelse af energiinfrastruktur på søterritoriet og den eksklusive økonomiske zone.

§ 35. Klima-, energi- og forsyningsministeren og Energinet kan fra virksomheder omfattet af loven indhente oplysninger, der er nødvendige for

varetagelsen af deres opgaver efter loven, efter bestemmelser fastsat i henhold til loven eller efter EU-retsakter eller internationale forpligtelser om forhold omfattet af loven.

Stk. 2. Klima-, energi- og forsyningsministeren fastsætter regler om, at virksomheder skal registrere sig, og hvilke oplysninger virksomheder i den forbindelse skal oplyse, herunder oplysninger om følgende:

1) Virksomhedens navn.
2) Adresse og ajourførte kontaktoplysninger, herunder e-mailadresser, IP-intervaller og telefonnumre.
3) Den relevante sektor og delsektor, som virksomheden er omfattet af.
4) De medlemsstater i Den Europæiske Union, hvor virksomheden leverer tjenester.

Kapitel 12
Straf

§ 36. Med bøde straffes den, der

1) overtræder §§ 6-10, § 11, stk. 2, §§ 12 og 13,
2) undlader at efterkomme en afgørelse efter § § 23, stk. 1, nr. 1 eller 2,
3) undlader at efterkomme påbud efter §§ 21 og 22,
4) undlader at efterkomme krav efter § 14, stk. 2 eller § 19, stk. 2, nr. 5-7,
5) hindrer myndighederne i at føre kontrol efter bestemmelserne i 19, stk. 2, nr. 1-4,
6) meddeler klima-, energi- og forsyningsministeren eller Energiklagenævnet urigtige eller vildledende oplysninger eller efter anmodning undlader at afgive oplysninger.

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

Stk. 3. Hvor der er pålagt en bøde for overtrædelse af forordning 2016/679/EU 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 forordning 2016/679/EU eller databeskyttelsesloven.

Stk. 4. I forskrifter, der udstedes i medfør af loven, kan der fastsættes straf af bøde for overtrædelse af bestemmelser i forskrifterne.

Kapitel 13
Ikrafttrædelse

§ 37. Loven træder i kraft d. 1. januar 2025.

Kapitel 14
Ændringer i anden lovgivning

§ 38. I olieberedskabslov jf. lov nr. 354 af 24. april 2012, foretages følgende ændringer:

1. *§ 16,* ophæves.

§ 39. I lov om elforsyning jf. lovbekendtgørelse nr. 1248 af 24. oktober 2023, foretages følgende ændringer:

1. *§ 51 d,* ophæves.

2. *Overskriften* til kapitel 12 affattes således:

»Kapitel 12

Fortrolighed, kontrol, oplysningspligt og påbud«

3. *§§ 85 b og 85 c,* ophæves.

§ 40. I lov om gasforsyning jf. lovbekendtgørelse nr. 1100 af 16. august 2023, foretages følgende ændringer:

1. *Overskriften* før § 15 a ophæves.

2. *§§ 15 a* og *15 b,* ophæves.

3. *§ 30 a, stk. 5 og 6,* ophæves.
stk. 6 og 7 bliver herefter stk. 5 og 6.

4. I *§ 30 a, stk. 7,* der bliver stk. 6, ændres »stk. 1, 2, 5 og 6.« til: »stk. 1 og 2.«

§ 41. I lov om varmeforsyning jf. lovbekendtgørelse nr. 124 af 2. februar 2024, foretages følgende ændringer:

1. I *§ 20, stk. 1, 1. pkt.,* indsættes efter »§§ 28 a, 28 b og 29«: »og omkostninger til beredskab efter lov om styrket beredskab i energisektoren,«.

2. *§ 29 a*, ophæves.

§ 42. I lov om anvendelse af Danmarks undergrund jf. lovbekendtgørelse 1461 af 29. november 2023, foretages følgende ændringer:

1. *§ 17 a* ophæves.

§ 43. I lov om energinet jf. lovbekendtgørelse nr. 271 af 09. marts 2023, foretages følgende ændringer:

1. I *§ 2, stk. 2, 1. pkt.,* indsættes efter »reglerne i denne lov«: lov om styrket beredskab «.

Kapitel 15
Territorialbestemmelser

§ 44. Loven gælder ikke for Færøerne og Grønland.

Bemærkninger til lovforslaget

Almindelige bemærkninger

Indholdsfortegnelse

1.	Indledning
2.	Lovforslagets baggrund
3.	Lovforslagets hovedpunkter
3.1.	Anvendelsesområde og identifikationsbestemmelser
3.1.1.	Gældende ret
3.1.2.	Klima-, Energi- og Forsyningsministeriets overvejelser
3.1.3.	Den foreslåede ordning
3.2.	Foranstaltninger for beredskab og modstandsdygtighed i energisektoren
3.2.1.	Gældende ret
3.2.1.1.	Organisatorisk beredskab
3.2.1.2.	Fysisk sikring
3.2.1.3.	It-beredskab
3.2.2.	Klima-, Energi- og Forsyningsministeriets overvejelser
3.2.3.	Den foreslåede ordning
3.3.	Underretning
3.3.1.	Gældende ret
3.3.2	Klima-, Energi- og Forsyningsministeriets overvejelser
3.3.3.	Den foreslåede ordning

3.4.	Sikkerhedsgodkendelser og baggrundskontrol
3.4.1	Gældende ret
3.4.2	Klima-, Energi- og Forsyningsministeriets overvejelser
3.4.3	Den foreslåede ordning
3.5.	Gebyrbestemmelser om gebyrbetaling for myndighedsbehandling
3.5.1.	Gældende ret
3.5.1.1.	Virksomhedernes gebyrbetaling for myndighedsbehandling
3.5.1.2.	Energinets gebyrbetaling for myndighedsbehandling
3.5.2.	Klima-, Energi- og Forsyningsministeriets overvejelser
3.5.2.1.	Generelle grundbeløb til finansiering af almindeligt tilsyn og administration af ordningen
3.5.2.2.	Aktivitetsberegnet beløb til finansiering af ad-hoc tilsyn
3.5.2.3.	Beløb til finansiering af behandling af virksomhedernes ansøgninger i egeninteresse
3.5.3	Den foreslåede ordning
3.6.	Tilsyn
3.6.1.	Gældende ret
3.6.2.	Klima-, Energi- og Forsyningsministeriets overvejelser
3.6.3.	Den foreslåede ordning
3.7.	Håndhævelse og sanktion
3.7.1.	Gældende ret
3.7.2.	Klima-, Energi- og Forsyningsministeriets overvejelser
3.7.2.1	Særligt om tvangsbøder

3.7.2.2.	Særligt om fysiske personer strafansvar, herunder valg af ansvarssubjekt
3.7.2.3.	Særligt om brud på persondatasikkerheden
3.7.3	Den foreslåede ordning
3.8.	Nødvendige omkostninger til beredskab efter lov om varmeforsyning
3.8.1.	Gældende ret
3.8.2.	Klima-, Energi- og Forsyningsministeriets overvejelser
3.8.3.	Den foreslåede ordning
4.	Økonomiske konsekvenser og implementeringskonsekvenser for det offentlige
5.	Økonomiske og administrative konsekvenser for erhvervslivet m.v.
6.	Administrative konsekvenser for borgerne
7.	Klimamæssige konsekvenser
8.	Miljø- og naturmæssige konsekvenser
9.	Forholdet til EU-retten
10.	Forholder til databeskyttelsesforordningen og databeskyttelsesloven
11.	Hørte myndigheder og organisationer m.v.
12.	Sammenfattende skema

1. Indledning

Mange samfundsvigtige funktioner er afhængige af, at en stabil energiforsyning opretholdes. Derfor er samfundet også særdeles sårbart, hvis dele af energiforsyningen i kortere eller længere perioder forstyrres, hvad enten det skyldes tekniske nedbrud på grund af fx systemfejl, vejrmæssige forhold eller det skyldes cyberangreb, hærværk eller sabotage.

Energisektorens beredskab har overordnet til formål at sikre, at sektoren er forberedt til at kunne beskytte og videreføre energiforsyningen i tilfælde af naturskabte, menneskeskabte og teknologiske risici. Dette lovforslag har til formål at styrke beredskabsreguleringen i den danske energisektor for at sikre, at lovgivningen på området er tidssvarende, og at virksomheder og energisektoren som helhed er robust overfor relevante risici og sårbarheder.

Desuden omfattes energisektoren af EU-direktiver, som skal implementeres som del af dette lovforslag. Det drejer sig om 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) og 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).

Lovforslaget rummer bl.a. bemyndigelsesbestemmelser til klima-, energi- og forsyningsministeren, der angår krav til virksomhedernes organisatoriske beredskab, fysisk sikring, cybersikkerhed, sikkerhedsgodkendelser, baggrundskontrol og digital kommunikation. Desuden indgår bestemmelser for fastsættelse af rammer for myndighedernes arbejde i forhold til vejledning, tilsyn, sanktioner og gebyrfinansiering af disse aktiviteter. Der redegøres nærmere herfor i de almindelige bemærkninger samt bemærkningerne til lovforslagets enkelte bestemmelser.

2. Lovforslagets baggrund

Der er ikke foretaget væsentlige ændringer i reguleringen af energisektorens almene beredskab siden 2007 og it-beredskab siden 2017. Der er dog en række forandringer i samfundet, som er med til i disse år at ændre rammerne for beredskabet, og som gør, at der er behov for at opdatere beredskabsreguleringen i energisektoren.

Den grønne omstilling betyder bl.a., at energisystemet forandres. Større dele af energiforsyningen i fremtiden vil komme fra mange decentralt placerede VE-anlæg. Produktionen af el vil således fx ikke længere være koncentreret om få kraftværker, men vil i stedet blive spredt ud på mange små og store anlæg. Tilsvarende sker der en udvikling i brugen af digitale teknologier, der skaber nye sårbarheder på især cyberområdet.. Også den geopolitiske situation i Europa og det generelle trusselsbillede har udviklet sig, og det har skabt en række afledte effekter for den danske energisektor. Der er bl.a. cyber- og spionageaktivitet mod energisektoren. Der er også ændringer i klimaet som fx større mængder regn end tidligere, som sætter nye krav til beredskabsmæssigt at robustgøre og klimatilpasse energianlæg, som kan være udsatte.

EU-direktiverne NIS 2 og CER skal implementeres i energisektoren. Direktiverne stiller krav om et højere beredskabsniveau på tværs af unionen. Overordnet stiller CER krav til kritiske enheders modstandsdygtighed, mens NIS2 stiller krav til væsentlige og vigtige enheders cybersikkerhed i kritiske sektorer. I energisektoren omfatter direktiverne el, gas, olie, fjernvarme, fjernkøling og brint. Direktiverne stiller således krav til delsektorer og virksomheder, der ikke i dag er omfattet beredskabsregulering.

Regeringen har besluttet, at Forsvarsministeriet er ansvarlig for koordineringen af implementeringen af NIS2- og CER-direktiverne. For begge direktiver er det blevet besluttet, at Forsvarsministeriet fremsætter én hovedlov, som omfatter alle berørte sektorer med undtagelse af energisektoren for så vidt angår CER og med undtagelse af energi-, tele- og finanssektoren for så vidt angår NIS2.

Det er væsentligt for et sammenhængende beredskab i energisektoren, at NIS2- og CER-direktivet tænkes sammen. Kravene som følger af direktiverne komplementerer hinanden. Et højt cybersikkerhedniveau forudsætter fx, at der bl.a. er passende fysiske sikring. I lovforslaget lægges der grundlæggende vægt på, at et robust beredskab kræver en holistisk tilgang, hvor tekniske, organisatoriske og fysiske foranstaltninger spiller sammen. Det følger også af direktiverne, at der er indbyrdes forbindelser, og at der i videst muligt omfang bør sikres en sammenhængende tilgang til implementeringen af direktiverne. Derfor lægges der op til, at opdateringen af beredskabsreguleringen i energisektoren og implementeringen af NIS 2- og CER-direktivet sker ved ét samlet lovforslag. Samtidig overføres en række beredskabsbestemmelser fra energisektorens forsyningslove til denne lov.

3. Lovforslagets hovedpunkter

3.1. Anvendelsesområde og identifikationsbestemmelser

3.1.1. Gældende ret

Reguleringen af beredskabsplanlægningen for virksomheder i den danske energisektor udspringer af sektoransvaret, der er det grundlæggende princip for organiseringen af det danske civilberedskab. Sektoransvaret er kodificeret i § 24 i lovbekendtgørelse nr. 314 af 3. april 2017 om bekendtgørelse af beredskabsloven. Det følger af beredskabslovens § 24, at hver minister inden for sit område skal stå for planlægning af det civile beredskab, som omfatter opretholdelse og videreførelse af samfundets funktioner i tilfælde af større ulykker og katastrofer. I forarbejderne til lov nr. 514 af 26. maj. 2014 om ændring af beredskabsloven gøres det ligeledes klart, at krigshandlinger, samt det at kunne yde støtte til forsvaret, fortsat er noget, den enkelte minister skal tage højde for i sin beredskabsplanlægning. Heri indgår efter praksis også at koordinere planlægningen med andre myndigheder, herunder at planlægge sammen med forsvaret og yde støtte til forsvaret, når dette findes relevant, fx. i forhold til luftfartskontrol.

Den sektoransvarlige minister har som led i sin beredskabsplanlægningsforpligtigelse ikke ansvar for den aktive beskyttelse af dansk territorium til lands, til vands eller i luften, den danske befolkning eller infrastruktur på dansk territorium mod konkrete angreb fra fremmede stater eller terrorister. Dette er afgrænset af beredskabslovens § 24, hvor civilberedskabsplanlægningen går på planlægningen for opretholdelse af og videreførelsen af samfundets funktioner efter større ulykker og naturkatastrofer herunder krigshandlinger.

Den sektoransvarlige minister har dog et ansvar for, at virksomheder inden for dennes ressort kan detektere forsøg på angreb mod disse virksomheder, har et minimum af sikring mod angreb og sabotage, og at virksomhederne har planer for opretholdelse og videreførelse af deres samfundsmæssige funktion, skulle de blive forsøgt angrebet eller faktisk angrebet, uanset hvem der står bag.

Sektoransvaret efter § 24 i beredskabsloven er for klima-, energi- og forsyningsministerens ressortområde siden Lov nr. 316 af 22. maj 2002 blevet udmøntet i forskellige forsyningslove ved bemyndigelsesbestemmelser, der i udgangspunktet er delegeret til Energistyrelsen, herunder elforsy-

ningsloven, gasforsyningsloven, varmeforsyningsloven, olieberedskabsloven, undergrundsloven og lov om forsyningsmæssige foranstaltninger. Før lov nr. 316 af 22. maj 2002 var sektoransvaret løftet ved hjælp af pålæg til de enkelte virksomheder i henhold til § 28, stk. 1 i beredskabsloven.

Beredskabsparagrafferne i disse love omhandler alle mitigering af forsyningsafbrud af energi og om nødvendigt hurtigst mulig genoprettelse af forsyningen, når denne har været afbrudt.

Ministeren har kun ansvaret for håndteringen af den civile beredskabsplanlægning i Danmark for den danske energiforsyning. Derfor finder ovennævnte forsyningslove i udgangspunktet kun anvendelse på virksomheder, der opererer som et direkte led af den forsyningskæde, der måtte være fra første produktion i Danmark (herunder i dansk eksklusiv økonomisk zone) til import til Danmark, og indtil energiarten er forbrugt i Danmark eller eksporteret. Beredskabsplanlægning for energi i transit fx. i rørledninger, kabler eller skibe, der ikke er forbundet til Danmark eller tilløber Danmark, falder således uden for klima-, energi- og forsyningsministerens ressort.

De gældende beredskabsparagraffer i de ovennævnte forsyningslove finder i elsektoren anvendelse på bevillingspligtige virksomheder efter §§ 10 og 19 i elforsyningsloven samt elforsyningsvirksomhed, der varetages af Energinet eller denne virksomheds helejede datterselskaber i medfør af § 2, stk. 2 og 3, i lov om Energinet, samt virksomheder, der yder balancering af elsystemet. I gassektoren finder de gældende beredskabsparagraffer anvendelse på selskaber, der er bevillingspligtige efter § 10 i gasforsyningsloven, samt Energinet og denne virksomheds helejede datterselskaber, der varetager gasvirksomhed i medfør af § 2, stk. 2 og 3, i lov om Energinet, samt virksomheder, som driver anlæg til produktion og fremføring af bygas. I oliesektoren finder de gældende beredskabsparagraffer anvendelse på lagringspligtige virksomheder efter olieberedskabsloven, som har en lagringspligtig omsætning større end nul og den centrale lagerenhed, der er udpeget efter olieberedskabslovens § 5, stk. 1. I offshore olie- og gassektoren finder de gældende beredskabsparagraffer anvendelse på rettighedshavere med tilladelse til efterforskning og indvinding af kulbrinter eller tilladelse til etablering og drift af rørledningsanlæg i forbindelse med indvinding af kulbrinter.

Danske love finder i udgangspunktet anvendelse alle steder, hvor den danske stat kan udøve sin autoritet, medmindre der er taget eksplicit stilling

til, at den ikke skal gælde der. Således er alle eksisterende love, der beskæftiger sig med beredskab for energisektoren gældende på land, dansk territorialfarvand, i den danske eksklusive økonomiske zone og dansk kontinentalsokkelområde. Udgangspunktet er specificeret i en række af forsyningslovene.

Ifølge bekendtgørelse om beredskab for elsektoren § 11, stk. 1 og bekendtgørelse om beredskab for gassektoren § 11, stk. 1, skal Energistyrelsen foretage en klassificering af anlæg i el og gassektoren. Det følger af bekendtgørelse om it-beredskab for el- og naturgassektoren, at Energistyrelsen skal foretage kategorisering af virksomheder. Efter gældende ret inddeles anlæg i tre klasser, og virksomheder inddeles i tre kategorier afhængig af anlæggets eller virksomhedens betydning for energiforsyningen. Klassificeringen og kategoriseringen har betydning for, hvilke krav virksomhederne skal efterleve, samt hvor ofte der føres tilsyn med virksomheden. Alle de eksisterende energiforsyningslove, der indeholder beredskabsparagraffer, indeholder også bemyndigelsesbestemmelser til klima-, energi- og forsyningsministeren, hvorefter ministeren kan fastsætte regler eller træffe bestemmelser med henblik på at gennemføre eller anvende internationale konventioner og EU-regler om forhold, der er omfattet af loven. Bemyndigelsen udnyttes ofte som en supplerende hjemmelsparagraf ved udstedelse af bekendtgørelser, der implementerer direktiver eller gennemfører dele af forordninger.

3.1.2. Klima-, Energi- og Forsyningsministeriets overvejelser

Klima-, Energi og Forsyningsministeriets vil med dette lovforslag fortsætte med at løfte sit sektoransvar, som kodificeret i beredskabslovens § 24. Der ændres med forslaget ikke på de allerede eksisterende grundprincipper i den beredskabsplanlægning, som virksomhederne skal udføre.

Lovforslaget vil samtidig implementere NIS2- og CER-direktiverne, som finder anvendelse på flere delsektorer end den gældende regulering. Beredskabet i energisektoren vil dermed blive styrket, idet lovforslaget vil omfatte flere virksomheder i flere delsektorer, og fordi kravene til virksomhederne i relevant omfang skærpes og gøres mere detaljerede, end de har været i det hidtidige lovgrundlag.

Ligeledes vil der fremover blive ført tilsyn med flere virksomheder. Hyppigheden af tilsynet gradueres efter, hvor forsyningskritiske virksomhederne er.

Lovforslaget fastsætter endvidere regler for fortrolig deling af information om sårbarheder og hændelser. Det forventes, at tilsynsmyndigheden forsat placeres hos Energistyrelsen, der fik overført tilsynsmyndigheden fra Energinet i 2019.

Af lovtekniske grunde har Klima-, Energi og Forsyningsministeriet med dette lovforslag valgt at samle hjemmelsgrundlaget for beredskabsarbejdet i energisektoren i en ny lov fremfor at have næsten enslydende hjemler i fem forskellige forsyningslove. Baggrunden herfor er bl.a., at sikre, at kravene er de samme på tværs de forskellige forsyningsarter. Derudover giver det et samlet overblik over beredskabsreguleringen for de omfattede virksomheder, hvoraf en del er multiforsyningsvirksomheder eller har aktiviteter i flere delsektorer.

Den grønne omstilling har og vil forsat medføre en større diversitet i danske forbrugeres og virksomheders energiforsyning. Den decentrale energiproduktion, som bl.a. hænger sammen med en øget integration af vedvarende energi i det danske energisystem, har bevirket, at forbrugere og virksomheder ikke blot er afhængige af en eller to energikilder. Der er ligeledes gensidige afhængigheder mellem de forskellige delsektorer, hvilket kan bevirke, at en forsyningsafbrydelse i den ene delsektor kan have betydning for forsyningen i andre delsektorer. Desuden har markedsliggørelsen og digitaliseringen af den danske og europæiske energiforsyning medført, at et langt større antal virksomheder har indflydelse på, at forsyningen er velfungerende, forudsigelig og ikke mindst sikker.

Med udbygningen af vind- og solenergi bliver elproduktionen mere decentraliseret. Produktionen af el vil således ikke længere være koncentreret om få kraftværker, men den vil i stedet blive spredt ud på mange små og store anlæg. Der vil bl.a. i de kommende år blive bygget store VE-anlæg (f.eks. land- og havvindmølleparker), som vil have en størrelse, hvor de vil få væsentlig betydning for energiforsyningen på nationalt og europæisk niveau. Nogle af disse anlæg vil være geografisk placeret steder, hvor de kan være eksponeret.

Grundet udviklingen af energisystemerne hvor produktionen er blevet mere vejrafhængigt og fluktuerende de sidste par år, vil forbrugssiden også få væsentligt indvirkning på forsyningssikkerheden af energi. Dette er særligt relevant for elforsyningen, hvor alt fra ladestanderoperatører, PtX-anlæg, varmepumper og smartstyring af virksomheder og privatpersoners elforbrug potentielt kan få indvirkning på den nationale elforsyning, såfremt

ondsindede aktører kan tage kontrollen med forbruget. Den nuværende regulering tager ikke tilstrækkeligt højde for denne udvikling inden for mangfoldigheden af aktører, der har betydning for energisektoren. Derfor foreslås det i overensstemmelse med NIS 2- og CER-direktivet, at flere aktører på forbrugssiden omfattes af reguleringen. Velfungerende og sikre markedsaktører er ligeledes essentielle for en stabil forsyning af energi i Danmark og resten af Europa, hvorfor disse også foreslås omfattet af denne beredskabsregulering.

I takt med at brint bliver en vigtigere del af det danske energisystem, bør modstandsdygtigheden af brintforsyningen også understøttes. På sigt forventes der i Danmark være en del af de danske forbrugere og virksomheder, der vil være afhængige af den brint, som produceres på de brintproducerende anlæg. Beredskabsreguleringen af brintsektoren bør tage højde for denne forudsete udvikling af brintsektorens kritikalitet, hvor brintproducerende anlæg går fra at være kritiske for elforsyningssikkerheden på baggrund af deres forbrug af el til i stigende grad også at være kritiske på baggrund af den brint og dermed de PtX-produkter, som elektriciteten omdannes til på anlæggene. På den baggrund har Klima-, Energi-, og Forsyningsministeriet vurderet, at beredskabsreguleringen af brintsektoren bør tage højde for, at brintproducerende anlæg kan være kritiske for energiforsyningen både på baggrund af forbruget af strøm og på baggrund af den brint, som anlæggene producerer.

Brintinfrastruktur kommer til at udgøre et vigtigt bindeled mellem produktion og forbrug af brint og bliver afgørende for, at brint kan handles på det indre marked. Brintinfrastruktur er i dag reguleret i gasforsyningsloven. Idet den økonomiske regulering og markedsforholdene for brint følger den model, der i en årrække har været gældende på naturgasområdet, er det nærliggende, at beredskabsreguleringen af brintinfrastrukturen følger den model, der gælder for naturgassektoren i den nuværende beredskabsregulering.

I gassystemet er der de seneste år sket en markant udvikling, hvor naturgas fra den danske del af Nordsøen eller import af naturgas i vidt omfang er blevet erstattet af decentral biogasproduktion. Opgraderet biogas svarede således i 2023 til ca. 40 pct. af det samlede danske gasforbrug, og andelen af biogas i gasnettet forventes at stige yderligere fremover.

Den danske produktion og opgradering af biogas til nettet er steget markant de seneste år. Biogasproduktionen har dermed fået en væsentlig betydning i gassystemet, og Klima-, Energi- og Forsyningsministeriet vurderer derfor, at det er væsentligt at omfatte biogasproduktionsanlæggene af reguleringen.

Det gælder for både biogasanlæg såvel som for øvrige gasproducerende anlæg og gasbehandlingsanlæg, at det enkelte anlæg ikke er kritisk i sig selv, fordi anlægget producerer til et sammenhængende gasnet. Ikke desto mindre er de gasproducerende anlæg vigtige for at gøre energiforsyningen modstandsdygtig over for uforudsete hændelser på tværs af de enkelte led.

Der sker i disse år en udfasning af fossile brændsler til opvarmning, som især erstattes af fjernvarme. Fjernvarmesektoren er karakteriseret af mange små og mellemstore anlæg, som således ikke nødvendigvis har betydning for energiforsyningen på nationalt plan. Dog er fjernvarmesektoren karakteriseret af naturlige monopoler, hvor langt størstedelen af slutbrugerne således kun har ét varmerør, der forsyner deres hus eller bygning. Dette forhold understreger fjernvarmens kritikalitet for især private boliger samt fx. hospitaler og andre samfundskritiske funktioner, hvor varmeforsyning er afgørende, og Klima-, Energi- og Forsyningsministeriet vurderer derfor, at det er væsentligt at omfatte virksomheder, der producerer eller distribuerer fjernvarme af reguleringen.

Fjernkølingssektoren i Danmark er under udvikling og forventes at få en tiltagende betydning for køling i især industrien såvel som for hospitaler og lignende samfundskritiske bygninger og anlæg, der har behov for stabil køling. På den baggrund vurderes det relevant at omfatte virksomheder, der opererer inden for fjernkøling.

Den gældende beredskabsregulering af oliesektoren omhandler primært krav om lagerberedskab af olieprodukter. Danmark er efter gældende EU-regler forpligtet til at holde beredskabslagre af olie svarende til 61 dages gennemsnitligt forbrug. Forpligtigelsen til at holde beredskabslagre er pålagt de lagringspligtige virksomheder, hvilket er den gruppe af olievirksomheder i Danmark, som foretager import eller produktion af enten råolie eller olieprodukter. Det vil sige, at virksomhederne og den centrale lagerenhed skal foretage beredskabsplanlægning, der sikrer forsyningen af olie fra egne lagre i en beredskabssituation. Fremover udvides beredskabsregu-

leringen af olievirksomheders lagre til også at omfatte flere led i olieforsyningen. Derned vil flere led i værdikæden for olieforsyning blive omfattet af beredskabskrav.

Oliesektoren i Danmark er i høj grad karakteriseret af globale markedsmekanismer og for mange af kunderne i oliesektoren, er der substitutionsmuligheder. Kritikaliteten afhænger ikke på samme måde af virksomhedernes størrelse målt på mængden af energi, de håndterer, men den afhænger i højere grad af deres rolle i værdikæden, og hvorvidt deres kunder har substitutionsmuligheder. I oliesektoren er der flere aktører i forsyningskæden, for hvilke der er få substitutionsmuligheder på nationalt plan, herunder fx. raffinaderier, olierør og offshore-platforme, og som derfor er kritiske for olieforsyningen. Ligeledes er der relativt få aktører, der ejer fx terminaler og olielagre, og hvor substitutionsmulighederne på nationalt plan er få, hvorfor det også vurderes hensigtsmæssigt, at beredskabsreguleringen omfatter disse, således at oliemarkedets funktion understøttes af krav til virksomhedernes modstandsdygtighed og beredskab.

Derudover vurderer Klima-, Energi- og Forsyningsministeriet, at tankstationsvirksomhed bør omfattes af beredskabsreguleringen, idet tankstationer er et væsentligt led i distributionen af olieprodukter. I den sammenhæng er det ikke den enkelte tankstation, der er kritisk for forsyningen af olieprodukter. Der kan derimod være risici forbundet med, at mange tankstationskæder har ét samlet IT-system, som benyttes på tværs af tankstationskæden, og som forbinder forsynings- og forretningskritiske systemer. På den måde kan fx et cyberangreb forstyrre olieforsyningen fra en større delmængde af de danske tankstationer og skabe usikkerhed omkring brændstofforsyningen. Reguleringen af tankstationsvirksomhederne skal således gøre sektoren mere modstandsdygtig og understøtte brugernes tillid til markedets funktion.

Af disse årsager foreslår klima-, energi- og forsyningsministeren at udvide beredskabsreglernes anvendelsesområde ift. gældende ret. Ligeledes foreslås det, at beredskabsreguleringen stiller ensartede krav på tværs af de omfattede delsektorer for dermed at imødekomme de gensidige afhængigheder og for at øge modstandsdygtigheden på tværs af energisektoren. Således vil reglerne fremadrettet i tillæg til el-, gas- og oliesektorerne også gælde for såvel fjernvarme-, fjernkøling- og brintsektorerne. Endvidere vil nye aktører omfattes i el-, gas og oliesektorerne. Disse aktører er hovedsageligt dikteret af NIS2 og CER-direktivernes bilag om disses anvendelsesområde.

Det er samtidig Klima-, Energi- og Forsyningsministeriets vurdering, at en del virksomheder, der vurderes kritiske i opretholdelsen af energiforsyningen, ikke nødvendigvis vil være omfattet hvis blot NIS 2-direktivets anvendelsesområde bruges som afgrænsning. Det skyldes, at mange virksomheder grundet bl.a. koncernstrukturer ikke beskæftiger minimum 50 ansatte eller har en årlig omsætning på minimum 10 mio. EUR og en årlig samlet balance på minimum 10 mio. EUR. Anvendelsesområdet for loven foreslås derfor modificeret ift. NIS2-direktivets grænser for ansatte, årlig omsætning eller balance for visse typer af virksomheder. Denne modificering er ligeledes et udtryk for kravet om identificeringen af kritiske enheder efter CER-direktivets artikel 6 inden for klima-, energi- og forsyningsministerens ressortområde. Det vurderes, at lovforslaget i denne sammenhæng går videre end minimumskriterierne for fastlæggelse af anvendelsesområdet i både NIS2- og CER-direktiverne.

I medfør af CER-direktivet skal medlemsstaterne senest den 17. juli 2026 identificere kritiske virksomheder ud fra kriterierne om, at virksomheden leverer en eller flere væsentlige tjenester, og at en hændelse vil have betydelig forstyrrende virkning for enhedens levering af tjenesten. Ved identificeringen skal medlemsstaterne tage hensyn til den nationale risikovurdering og nationale strategi, der begge skal foreligge senest den 17. januar 2026.

I lyset af et stadigt skiftende trusselsbillede og deraf væsentligt øget behov for at styrke beredskabet i energisektoren vurderer Klima-, Energi- og Forsyningsministeriet, at det vil være uhensigtsmæssigt, hvis identificering af virksomheder i energisektoren potentielt først finder sted efter januar 2026.

Det foreslås derfor, at identificering af kritiske virksomheder efter CER-direktivet sker sammen med NIS 2-direktivet, således at det er de samme virksomheder, der omfattes af krav for begge direktiver baseret på forsyningstørrelse. Baggrunden herfor skal samtidig ses i lyset af, at der er tætte forbindelser mellem direktiverne, og at kravene i direktiverne komplementerer hinanden. Når den nationale risikovurdering og strategi efter CER-direktivet på et senere tidspunkt foreligger, vil Klima-, Energi- og Forsyningsministeriet på ny forholde sig til identificeringen af kritiske virksomheder. Identificering af virksomheder vil ske på baggrund af regler fastsat på bekendtgørelsesniveau.

På den baggrund foreslås en videreførelse af den gældende regulerings anvendelse af kritikalitet som parameter for, hvornår virksomheder og anlæg

omfattes af reguleringen. Herved er det forsyningsstørrelsen og i nogle tilfælde virksomhedens eller anlæggets rolle i energisystemerne, der er afgørende for, om virksomheden omfattes af beredskabsregulering. Dette skyldes, at forsyningsstørrelsen i højere grad afspejler virksomhedens kritikalitet for energiforsyningen. For at understøtte at reguleringen er proportionel set i forhold til sikkerhedseffekten hos virksomhederne og de omkostninger, de skal afholde for at efterleve reguleringen, foreslås et differentieret reguleringstryk. Med dette vil reguleringen stille skærpede krav til de mest forsyningskritiske virksomheder. I de tilfælde hvor virksomheder ikke omfattes på baggrund af de grænseværdier, der er fastsat på baggrund af kritikalitet, men de lever op til grænseværdierne for at være omfattet af NIS2-direktivet, foreslås det, at virksomhederne også omfattes af loven. Den nuværende regulering arbejder med en klassificering af anlæg og en kategorisering af virksomheder. Det vurderes hensigtsmæssigt at videreføre inddelingen, som sikrer et differentieret reguleringstryk. Af pædagogiske årsager videreføres klassificeringen af anlæg, mens der fremover vil ske niveauinddeling af virksomheder, som erstatter den gældende kategorisering. Reglerne forventes udformet således, at antallet af niveauer og klasser kan udvides, i det omfang udviklingen af energisektoren kræver det.

3.1.3. Den foreslåede ordning

Lovforslagets foreslåede anvendelsesområde følger i høj grad NIS2- og CER-direktivernes anvendelsesområder.

Det foreslås, at loven finder anvendelse på følgende virksomheder, når disse leverer deres tjenester eller udfører deres aktivitet inden for Danmark: 1) Elektricitetsvirksomheder, 2) Distributionssystemoperatører, 3) Transmissionssystemoperatører, 4) Elproducenter, 5) Udpegede elektricitetsmarkeds-operatører, 6) Markedsdeltagere, der leverer tjenester, der vedrører aggregering, fleksibelt elforbrug eller energilagring, 7) 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, 8) Operatører af fjernvarme eller fjernkøling, 9) Olierørledningsoperatører, 10) Operatører af olieproduktionsanlæg, -raffinaderier og -behandlingsanlæg, olielagre og olietransmission, 11) Centrale lagerenheder, 12) Gasforsyningsvirksomheder, 13) Lagersystemoperatører, 14) LNG-systemoperatører, 15) Naturgasvirksomheder, 16) Operatører af naturgasraffinaderier og –behandlingsanlæg, 17) Operatører inden for brintproduktion, -lagring og –transmission. Ovenstående følger af NIS2- og CER-direktivets bilag I.

Dertil foreslås det, at 18) Operatører af tankstationer, der er ansvarlige for forvaltningen og driften af en tankstation, omfattes af loven. Tankstationer vurderes at være et væsentligt led i energiforsyningen. Tilføjelsen af tankstationer følger dog ikke direkte af NIS 2- og CER-direktiverne, selvom tankstationer kan anskues i tilknytning til olie, som er omfattet som delsektor i NIS 2- og CER-direktivet.

Klima-, energi- og forsyningsministeriet foreslår, at lovens anvendelsesområde baseres på en række grænseværdier for hver af de omfattede delsektorer, der tager udgangspunkt i virksomhedernes kritikalitet for energiforsyningen.

Det foreslås således, at loven gælder for de typer af virksomheder, der er nævnt i § 2, stk. 1, nr. 1-8, 10, 12 og 18 såfremt virksomheden; 1) årligt producerer, forbruger eller kontrollerer mere end 25 MW elektricitet, 2) i 2 ud af 3 sidste år har solgt mere end 13,9 GWh, 3) årligt producerer/injicerer mere end 26 mio. Nm^3 gas i et gasnet, 4) opererer olieterminaler eller lagre med kapacitet på 100.000 m^3 eller derover, 5) opererer en eller flere tankstationer med et samlet årligt salg af olieprodukter på 600.000 m^3 eller derover, eller som opererer flere end 100 tankstationer på nationalt plan. De foreslåede nedre grænser for disse typer af virksomheder er udtryk for en fastholdelse af den eksisterende afgrænsning af virksomheder, som i høj grad er baseret på forsyningsstørrelse og kritikalitet. Dette er grænseværdier, som i de fleste tilfælde er vurderet af Klima-, Energi- og Forsyningsministeriet til at være lavere, og derfor omfatter de flere virksomheder, end hvis NIS 2-direktivets kriterier var blevet anvendt, hvorfor det også implementerer CER-direktivets artikel 6 for klima-, energi- og forsyningsministerens ressortområde.

Der kan dog være enkelte tilfælde, hvor virksomheden falder for disse foreslåede grænser, men virksomheden ville leve op til grænsen for at være omfattet af NIS 2-direktivet. Det foreslås således, at hvis de nævnte virksomhedstyper alligevel lever op til grænsen for at være omfattet af NIS 2-direktivet, vil de også være omfattet denne lov, uagtet at de ellers var faldet for et af de førnævnte kriterier. Dette sikrer, at der uagtet de ellers udvidende nedre grænser forsat kan ske EU-konform implementering af NIS 2- og CER-direktiverne.

Endvidere foreslås det, at virksomheder med positiv lagringsforpligtigelse efter Olieberedskabsloven altid er omfattet den foreslåede lov, selvom de ikke selv ejer lageret eller terminalen, som beredskabsolien befinder sig i,

eller hvis de har en kapacitet på mindre end 100.000 m^3. Det er essentielt, at de virksomheder med positiv lagringsforpligtigelse efter olieberedskabsloven er omfattet af denne lov, idet tilgængeligheden af beredskabslagrene, som disse virksomheder holder, er et grundlæggende krav for at have et velfungerende og brugbart olielagerberedskab.

For de bestemmelser, der gælder muligheden for at få foretaget sikkerhedsgodkendelse eller baggrundskontrol og gebyrbetaling for behandling af sådanne ansøgninger, forslås et stadig større anvendelsesområde en for de resterende bestemmelser i loven. Det foreslås således, at virksomheder, organisationer, fonde og erhvervsdrivende fonde kan få foretaget sikkerhedsgodkendelser af personer ansat af disse, såfremt disse personer varetager opgaver som direkte led eller i forbindelse med leveringen af de tjenester, der er nævnt i § 2, stk. 1.

Endeligt foreslås det, at loven og regler udstedt i medfør af loven gælder på land- og søterritoriet, den eksklusive økonomiske zone samt kontinentalsokkelen.

For nærmere om den foreslåede ordning for lovens anvendelsesområde henvises der til lovforslagets § 2 og bemærkningerne hertil.

3.2. Foranstaltninger for beredskab og modstandsdygtighed i energisektoren

3.2.1. Gældende ret

Efter gældende ret skal virksomheder med bevilling til netvirksomhed efter elforsyningslovens § 10, virksomheder med bevilling til elproduktion efter elforsyningslovens § 19, virksomheder med tilladelse til elproduktion over 25 MW efter elforsyningslovens § 11 eller efter § 29 i lov om fremme af vedvarende energi, virksomheder med bevilling til distribution af gas efter § 10 i gasforsyningsloven, Energinet og Energinet's helejede datterselskaber, balanceansvarlige virksomheder, Centrale Lagerenheder, virksomheder med positiv lagringspligt efter olieberedskabsloven, virksomheder der driver anlæg til produktion og fremføring af bygas, samt rettighedshavere med tilladelse til efterforskning og indvinding af kulbrinter eller tilladelse til etablering og drift af rørledningsanlæg i forbindelse med indvinding af kulbrinter planlægge og gennemføre beredskab for deres forsyning af elektricitet, naturgas, råolie, mineralolieprodukter, bygas og kulbrinter.

Forpligtigelserne for disse virksomheder er i dag overordnet set fastsat i en række forsyningslove, som for visse delsektorer i energisektoren er yderligere udmøntet i en eller flere bekendtgørelser. Der er således tale om §§ 85 b og c i lov om elforsyning, §§ 15 a og b i lov om gasforsyning, § 16 i olieberedskabsloven, § 29 a i lov om varmeforsyning, § 17 a i lov om anvendelse af Danmarks undergrund, der individuelt eller sammen er udmøntet i bekendtgørelse om beredskab for elsektoren, bekendtgørelse om beredskab for naturgassektorerne, bekendtgørelse om it-beredskab for el- og naturgasvirksomhederne, bekendtgørelse om beredskab for oliesektoren samt bekendtgørelse om identifikation og udpegning af europæisk kritisk infrastruktur på energiområdet og vurdering af behovet for bedre beskyttelse.

Beredskab forstås bredt, idet forpligtigelsen angår både organisatorisk beredskab, fysisk sikring af bygninger og anlæg samt cybersikkerhed for forsyningskritiske systemer, som virksomhederne benytter sig af i deres produktion, transmission, distribution, lagring, indvinding eller levering af elektricitet, naturgas, bygas, råolie, mineralolieprodukter eller kulbrinter.

3.2.1.1. Organisatorisk beredskab

Det følger af de ovennævnte paragraffer og bekendtgørelser, at virksomhederne skal foretage den nødvendige planlægning for at sikre forsyningen i beredskabssituationer og andre ekstraordinære situationer. Denne planlægningsforpligtigelse er gældende for de fysiske aspekter af virksomheden, for de logiske systemer og for den organisatoriske styring, som virksomhederne benytter i deres forsyning.

Beredskabsplanlægningen indebærer således organisatoriske forhold forstået som udpegelse af ansvarlige personer for beredskabsplanlægning, fysisk sikring og cybersikkerhed, risiko- og sårbarhedsvurderinger, beredskabsplaner, øvelser, underrettelsesforpligtelser, operative forhold samt uddannelse af ledelse og personale. De gældende krav til de organisatoriske forhold i virksomhederne betyder, at virksomhederne bl.a. skal udpege en beredskabskoordinator, en it-beredskabsansvarlig medarbejder, en operationel kontakt og en eller flere sikringsansvarlige medarbejdere.

Beredskabskoordinatoren varetager sammen med den sikringsansvarlige medarbejder virksomhedens beredskabsopgaver, herunder kontakt til myndigheder inkl. politiet. Den it-beredskabsansvarlige medarbejder skal koordinere virksomhedens sikring af forretnings- og forsyningskritiske it-systemer og skal sammen med beredskabskoordinatoren og ledelsen mindst fire

gange om året koordinere mellem det klassiske beredskab og it-beredskabet. Der må af samme årsag ikke være personsammenfald mellem beredskabskoordinatoren, den it-beredskabsansvarlige og ledelsen.

Den operationelle kontakt skal når som helst kunne fungere som forbindelsesled til virksomheden, hvilket betyder, at kontakten skal kunne modtage informationer fra myndighederne og/eller Energinet og sikre, at virksomheden iværksætter de nødvendige foranstaltninger, herunder videreformidling af informationer internt i virksomheden.

Den/de sikringsansvarlige medarbejder(e) er en konkret medarbejder, der skal varetage beredskabs- og sikringsopgaver for et eller flere individuelle anlæg. Mens de andre roller har et bredere ansvar for virksomhedens beredskab, har den sikringsansvarlige medarbejder et ansvar for et eller flere anlæg, som virksomheden ejer.

I tillæg til udpegelsen af diverse beredskabsroller fastsætter gældende ret krav til, at virksomhederne skal sikre, at de medarbejdere, som skal indgå i beredskabet, løbende modtager den fornødne instruktion, uddannelse og træning i disse opgaver. Der er ligeledes krav om, at virksomhederne skal udarbejde og gennemføre awareness-tiltag om it-sikkerhed, herunder formidle oplysning om hvordan it-sikkerheden skal varetages af den berørte gruppe af medarbejdere eller af eksterne. De mest kritiske virksomheder skal gennemføre årlige awareness-tiltag, mens de mindre kritiske kun skal gennemføre dem minimum hvert tredje år.

Risiko- og sårbarhedsvurderinger

Efter gældende ret skal virksomheder, der i dag er omfattet af beredskabsreguleringen, udarbejde en vurdering af virksomhedens risici og sårbarheder, herunder sårbarheder i forhold til virksomhedens kontinuitet og forsyningskritiske it-systemer. Det foregår ved, at Energistyrelsen sender en samling af risiko- og sårbarhedsscenarier til virksomhederne, som virksomhederne skal forholde sig til i udarbejdelsen af deres risiko- og sårbarhedsvurderinger. I disse vurderinger skal virksomhederne vurdere konsekvenserne for virksomheden, såfremt scenarierne udspiller sig og kan på den baggrund identificere virksomhedens sårbarheder og identificere, udvælge og prioritere beredskabet i forhold til de identificerede risici og sårbarheder.

Overordnet set er en risiko- og sårbarhedsanalyse virksomhedens vurdering af forskellige trusselscenariers konsekvenser for egen forsyningsevne.

Konklusionerne på risiko- og sårbarhedsanalyserne (ROS) giver dermed et billede af virksomhedens sårbarheder. For virksomheden skal denne indsigt i egne sårbarheder hjælpe med at afgøre, hvor virksomheden bør lægge sit fokus i beredskabsarbejdet og afdække behovet for internt at prioritere ressourcer til beredskabsarbejdet.

Beredskabsplanlægning og øvelser

Efter gældende ret er det et krav, at virksomhederne skal udarbejde beredskabsplaner og it-beredskabsplaner for håndtering af beredskabssituationer, som baseres på risiko- og sårbarhedsvurderingerne. Beredskabsplanerne skal bl.a. beskrive virksomhedens krisehåndtering, hvordan virksomhedens krisehåndteringsorganisation aktiveres, etableres og driftes, og hvordan der koordineres og udsendes information. Beredskabsplanen skal kunne bruges som en operativ vejledning, når en beredskabssituation bliver varslet eller opstår.

Virksomhederne i el- og naturgassektoren skal efter bekendtgørelserne om beredskab for elsektoren (Bek 2646) og om beredskab for naturgassektoren (Bek 821) afholde øvelser, som træner virksomhedens beredskab. De gældende krav til øvelser indebærer, at virksomhederne skal afholde beredskabsøvelser, der både træner virksomhedens it-sikkerhed og anvendelsen af deres beredskabsplaner. Bek 2646 og Bek 821 stiller krav om, at der mindst hvert andet år holdes en øvelse, og at øvelserne skal være planlagt, så de over en 5-årig periode dækker de væsentligste dele af virksomhedens beredskab.

Bekendtgørelse om it-beredskab for el- og naturgassektorerne (Bek 2647) stiller forskellige krav til øvelsesaktivitet alt efter, hvilken kategori virksomheden befinder sig i; Kategori 1-virksomheder skal som minimum afholde én årlig it-beredskabsøvelse, samt gennemføre awareness-tiltag årligt, Kategori 2- og 3-virksomheder skal tilsikre, at it-beredskab trænes i forbindelse med det almene beredskabsarbejde i relevant omfang, samt gennemføre awareness-tiltag minimum hvert andet år.

For at sikre at virksomhederne lever op til kravene i bekendtgørelserne, skal alle lave en 5-årig øvelsesplan. Den 5-årige øvelsesplan er tentativ, forstået på den måde at den må og skal tilpasses løbende. Øvelsesplanerne indgår som en del af Energistyrelsens tilsyn med virksomhederne, men de skal dog ikke fremsendes til godkendelse. Øvelsesplanen skal indeholde

elementer for både it-beredskab og klassisk beredskab og skal opdateres minimum årligt.

Når virksomhederne har afholdt en øvelse, skal den evalueres af Energistyrelsen. Derfor skal Energistyrelsen senest tre måneder efter øvelsen have en rapport, der beskriver øvelsens forløb og de erfaringer, virksomheden har fået undervejs. Rapporten skal også beskrive, hvordan og hvornår virksomheden har planlagt at følge op på øvelsen.

Energistyrelsen kan i særlige tilfælde godkende, at en evaluering af en hændelse kan erstatte en planlagt øvelse. Det forudsætter dog, at virksomheden ansøger om at få hændelsen godkendt som en øvelse, at Energistyrelsen har modtaget en øvelsesplan, og at hændelsen er indarbejdet i den, at hændelsen i væsentligt omfang har afprøvet konkrete forhold i beredskabsplanen, at hændelsen har den samme værdi som en planlagt øvelse, og at der er udarbejdet en tilfredsstillende evaluering.

For el- og gassektoren skal Energinet efter gældende ret afholde beredskabsøvelser i anvendelse af sektorberedskabsplanen.

Hændelsesrapporteringer

Virksomheder i el- og gassektorerne skal omgående underrette Energinet om beredskabshændelser og alvorlige it-sikkerhedshændelser, der er af relevans for beredskabssituationen i el- og naturgassektoren. Energinet skal omgående underrette Energistyrelsen, såfremt indberetningen er af betydning for el- eller naturgasforsyningen på nationalt niveau, samt vurdere om information om hændelsen skal viderebringes til Center for Cybersikkerhed eller andre virksomheder i el- eller naturgassektorerne jf. Bek 2646/821 § 23. og Bek 2647 §21.

Virksomheder i oliesektoren skal uden ugrundet ophold underrette Energistyrelsen om hændelser, der i væsentlig grad reducerer virksomhedens eller den centrale lagerenheds funktionalitet eller funktionaliteten af andre dele af oliesektoren. Virksomhederne skal uden ugrundet ophold underrette Energistyrelsen og Center for Cybersikkerhed om it-sikkerhedshændelser, der påvirker forsyningskritiske it-systemer, gennem en af Erhvervsstyrelsen dertil indrettede internetbaserede portal.

3.2.1.2. Fysisk sikring

Efter den gældende regulering klassificerer Energistyrelsen el- og gassektorernes anlæg efter anlæggenes betydning for at opretholde henholdsvis el- og gasforsyningen på nationalt, regionalt og lokalt niveau. Her er klasse 1-anlæg de mest forsyningskritiske, mens klasse 3-anlæg er de mindst forsyningskritiske. Klassificeringen af et anlæg afgør hvilke krav, der stilles til sikringen af det pågældende anlæg. Efter den nuværende regulering er det udelukkende ubemandede klasse 1-anlæg, der skal have etableret fysisk sikring mod uautoriseret adgang i form af mekaniske og elektroniske sikrings- og overvågningsforanstaltninger samt styret adgangskontrol, således at der tages stilling til hvem, der kan få adgang til hvilke dele af anlægget, samt at denne adgang logges.

For både klasse 1- og 2 anlæg skal det sikres, at virksomhedernes planmateriale indeholder sikringsplaner, der bl.a. omfatter relevant kortmateriale, beskrivelse af anlæggets sårbarhed og afhængighed af andre anlæg og funktioner, muligheder for reetablering, hvorvidt der er sikkerhedsfølsomme oplysninger om anlægget og kontaktoplysninger om beredskabskoordinatoren og en sikringsansvarlige medarbejder. Derudover skal virksomhederne bl.a. sikre, at klasse 1- og 2-anlæg har lav sårbarhed over for funktionssvigt af offentligt udbudte net og tjenester for elektronisk kommunikation, har lav sårbarhed over for funktionssvigt af væsentlige it-systemer, og at anlægget har nødstrømsforsyning, der sikrer anlæggets funktionalitet i tilfælde af en strømafbrydelse.

3.2.1.3. It-beredskab

I tillæg til de ovennævnte foranstaltninger stiller den gældende regulering krav til virksomhedernes it-beredskabsplanlægning. Virksomhederne skal således identificere forsyningskritiske it-systemer samt afhængigheden af andre systemer, beskrive forebyggende foranstaltninger til at imødegå utilsigtede it-hændelser, herunder muligheden for segmentering af it-infrastruktur og alternative driftsformer. Virksomheder, der anvender fjernadgang til forsyningskritisk it, skal have en plan for, hvordan angreb på disse systemer opdages og håndteres. Derudover skal bl.a. den interne ansvarsplacering under krisestyring, ansvaret for systemansvar for forsyningskritiske it-systemer, kommunikation med Energinet eller Energistyrelsen og virksomhedens it-sikkerhedstjeneste beskrives. Planerne skal endvidere beskrive procedurer for alternativ drift, genopretning af forsyningskritiske it-systemer, planer for dokumentation og opfølgning på hændelser samt

beskrivelse af den operative ansvarsdeling mellem virksomhedens og dens samarbejdsparter. It-beredskabsplanerne skal herudover være en del af virksomhedens samlede beredskabsplanlægning.

Der stilles i gældende ret krav om, at virksomhederne skal gennemføre awareness-tiltag om it-sikkerhed, herunder formidle oplysninger om hvordan it-sikkerheden skal varetages af de relevante medarbejdere såvel som af eksterne. Derudover skal virksomhederne gennemføre awareness-tiltag årligt eller hvert andet år afhængig af virksomhedens kategorisering.

Ud over it-beredskabsplanlægningen skal virksomhederne efter gældende ret sikre den fysiske opbevaring af forsyningskritiske it-systemer i forhold til deres kritikalitet for forsyningen på lige vilkår med den fysiske beskyttelse af fysiske anlæg. I det omfang at virksomhederne anvender leverandører til virksomhedens it-systemer, har virksomheden efter gældende ret ansvar for at it-sikkerheden og skal etablere procedurer for adgangsstyring for leverandører af forsyningskritiske it-systemer. Derudover stilles der bl.a. krav om, at virksomhederne skal bevare ejerskab af data og at adgangen til data logges og opbevares i sikre lokaler.

Det følger af den gældende regulering, at virksomhederne skal være tilmeldt en proaktiv it-sikkerhedstjeneste, der yder vejledning og mitigering af sårbarheder samt giver informationer og varsler om it-sikkerhedstrusler. Derudover skal kategori 1-virksomheder, der er de mest forsyningskritiske virksomheder, være tilmeldt en reaktiv it-sikkerhedstjeneste, der bistår virksomheden ved nedbrud eller angreb på it-systemer. Hertil kommer at virksomhederne skal sikre, at oplysninger, der har sikkerhedsmæssig betydning for andre virksomheder i energisektoren, kan viderebringes til disse, samt at oplysninger, der tilvejebringes gennem en it-sikkerhedstjeneste, skal kunne videreformidles til andre virksomheder.

3.2.2. Klima-, Energi- og Forsyningsministeriets overvejelser

Det hybride trusselsbillede giver anledning til at nytænke samfundets beredskab, herunder hvordan kritiske anlæg og net- og informationssystemer gøres modstandsdygtige over for både cybertruslen, fysiske trusler og konsekvenserne af klimaforandringerne samt andre hændelser, så forsyningssikkerheden opretholdes.

I den sammenhæng vurderes det hensigtsmæssigt, at den fysiske sikring tænkes sammen med et højt cybersikkerhedsniveau, samt at disse understøttes af det organisatoriske beredskab og at virksomhederne i deres risikostyring løbende forholder sig til nye trusler og sårbarheder. Således er det formålet med loven, at virksomhederne øger robustheden, og risikobaseret minimerer sårbarheder over for fx fysisk spionage, og sabotage, uautoriseret adgang, manipulation af og data samt kompromittering af kritiske systemer og følsomme dokumenter.

Organisatorisk beredskab og ledelsens ansvar

Det organisatoriske beredskab er et afgørende led i at etablere en organisation, der i tilstrækkelig grad kan identificere og mitigere potentielle risici for energiforsyningen. Det vurderes derfor hensigtsmæssigt, at der stilles krav om, at omfattede virksomheder skal have klare rammer for risikostyring, hvor både relevante trusler og sårbarheder løbende kan identificeres og styres, og hvor tekniske, fysiske og organisatoriske foranstaltninger evalueres. Denne form for risikostyring, hvor sikkerhedsrisici indgår som et centralt element i virksomhedens beslutninger, bør ligeledes indgå som en del af virksomhedens beslutninger om væsentlige ændringer i deres systemer, i deres leverandørforhold og i beslutninger vedrørende nye projekter, der vurderes at have betydning for forsyningskritiske processer eller funktioner.

Det er også væsentligt, at beredskabet ledelsesforankres. Det følger bl.a. af NIS2-direktivet, at ledelsesorganer godkender foranstaltninger til styring af cybersikkerhedsrisici og fører tilsyn med deres gennemførelse. Klima-, Energi- og Forsyningsministeriet lægger vægt på, at det er væsentligt, at ledelsesorganer er sikkerhedsmæssigt bevidste, og har en generel forståelse for beredskabet i deres organisation samt kender deres ledelsesmæssige ansvar. Dette skal være med til at sikre at arbejdet med virksomhedens modstandsdygtighed tildeles ledelsesfokus, og at ledelsen såvel som medarbejdere har de nødvendige faglige kompetencer og viden til at træffe beslutninger vedrørende risikostyring i forhold til sikkerhedstrusler og sårbarheder.

Hændelseshåndtering og genopretning

Som det også understreges i NIS 2- og CER-direktiverne, er klare procedurer for hændelseshåndtering essentielt i en beredskabssituation og skal bidrage til, at organisationen kan opretholde eller genoprette driften oven på hændelsen. Det er ligeledes væsentligt, at ledelsen prioriterer midler til hændelseshåndtering og genopretning, samt at ledelsen er bevidst om dennes rolle i organisationens krisestyring. Samtidig skal hændelseshåndteringen muliggøre koordination på tværs af aktører og myndigheder, således at andre organisationer er informeret om truslen, og risikoen for at denne kan sprede sig til andre organisationer.

I energisektoren er det ikke altid muligt at skelne mellem en beredskabssituation, der aktiverer det fysiske beredskab eller cyberberedskabet eller udvikler sig på en måde, der involverer begge typer beredskaber. For at imødekomme dette og for at understøtte en effektiv krisestyring vurderer Klima-, Energi-, og Forsyningsministeriet, at man med fordel kan stille ens krav til begge typer hændelseshåndteringer og -indberetninger. Ligeledes bør der i risikostyringen og i beredskabsplanlægningen være en højere grad af sammenhæng mellem den fysiske sikkerhed og cybersikkerhed, end det er tilfældet efter den gældende regulering.

Af samme årsag foreslås det, at der sikres sammenhæng mellem træningen af det klassiske beredskab og cyberberedskabet. Klima-, Energi- og Forsyningsministeriet foreslår således, at der sker koordinering af øvelser, der træner henholdsvis det klassiske beredskab og cyberberedskab, og at de fremover følger samme kadence for afholdelse, evaluering og indsendelse til Energistyrelsen.

Det foreslås desuden, at Energinet fortsat skal afholde beredskabsøvelser for el- og gassektoren, og atEnergistyrelsen er ansvarlig for at afholde beredskabsøvelser for de nyomfattede sektorer.

Fysisk sikring

Fysisk sikring af anlæg medvirker til at forsinke eller besværliggøre hændelser, herunder spionage og anden uautoriseret adgang, der kan kompromittere anlæggets sikkerhed og potentielt påvirke forsyningssikkerheden. Derudover kan en helhedsorienteret fysisk sikring af anlæg medvirke til at understøtte den logiske sikkerhed af energiinfrastrukturen. I den gældende

beredskabsregulering stilles udelukkende krav om fysisk sikring af ubemandede klasse 1-anlæg, som er de mest forsyningskritiske anlæg efter gældende regulering. Klima-, Energi- og Forsyningsministeriet vurderer imidlertid, at bemanding af anlæg ikke nødvendigvis giver en tilstrækkelig sikkerhed, hvorfor der fremover også bør stilles krav til den fysiske sikring af bemandede anlæg.

Klimaforandringerne introducerer en øget fysisk risiko i form af naturkatastrofer og ekstreme vejrforhold samt langsigtede ændringer i klimaforholdene. Dette kan have betydning for energiinfrastrukturens kapacitet, effektivitet og levetid. Det følger af CER-direktivet, at virksomhederne i deres beredskab skal forholde sig til bl.a. klimatilpasningsforanstaltninger.

Digitaliseringen af energiinfrastruktur betyder, at infrastrukturen er forbundet i netværk. Dermed kan en hændelse i ét anlæg have konsekvenser for andre anlæg. Dette gør energiinfrastruktur sårbar over for cyberangreb, men det betyder også, at den fysiske sikkerhed er afgørende for at forhindre adgang til de dele af anlæggene, der er tilkoblet et samlet system. I det omfang et anlæg har netværksadgang til et større net eller system, introducerer disse også en potentiel sårbarhed. I denne sammenhæng kan mindre anlæg, der ikke er tilstrækkeligt sikret, være medvirkende til en kompromittering af fx. et sammenhængende elnet.

Industrielle kontrolsystemer

Inden for en række energivirksomheders net- og informationssystemer er der industrielle kontrolsystemer, som benyttes til at overvåge og styre forsyningsprocesser (fx spændingsniveau, temperatur og tryk). Industrielle kontrolsystemer forstås her som digital overvågning og styring af fysiske systemer. Således kan industrielle kontrolsystemer fx forstås som en betegnelse for it-systemer (informationsteknologi) eller elementer heraf, der overvåger og kontrollerer enkelte OT-systemer (operationel teknologi). Operationel teknologi er de programmerbare digitale systemer eller enheder, der interagerer med det fysiske miljø eller styrer enheder, der interagerer med det fysiske miljø. Dette kan fx være SCADA-systemer, SRO-systemer samt PLC'er og RTU'er.

Nogle af disse industrielle kontrolsystemer har – i modsætning til normale it-systemer – typisk en lang levetid på op mod 30-40 år, og de er nogle

gange ikke mulige at hærde, da det kan forstyrre produktionen at sikkerhedsopdatere produkterne. Det gør, at systemerne er særligt sårbare, hvis en angriber får adgang til systemerne. Udviklingen går i retning af, at det forsyningskritiske netværk smeltes sammen med øvrige dele af virksomhedernes netværk, og at der skabes flere indgange til kontrolsystemerne end tidligere. Det vurderes væsentligt, at de industrielle kontrolsystemer beskyttes, og at virksomhederne har overblik og styring i forhold til bl.a. netværksarkitektur, adgang, integrationspunkter, autentificering og logning.

Internetforbundne enheder og fjernadgange

Desuden ses et øget brug af internetforbundne enheder, som skal understøtte øget produktions- og forbrugsfleksibilitet samt datadeling. Større dele af den infrastruktur og de systemer, som understøtter produktion, transmission, distribution og monitorering af energi, forbindes enten direkte eller indirekte til internettet. Denne udvikling er med til at skabe nye angrebsvinkler og mulige sårbarheder, som kan påvirke forsyningskritiske processer. Det er samtidig gradvist blevet mere udbredt at udføre opgaver inden for det forsyningskritiske miljø via fjernadgange. Det er således ofte ikke nødvendigt, at operatører befinder sig i virksomhedens kontrolcenter eller på transformerstationen for at udføre systemopgaver, da det i flere tilfælde kan udføres fx hjemmefra hos leverandøren. Det betyder dog samlet set, at angrebsfladen vokser. Derfor er det nødvendigt fremover at stille skærpede tekniske og organisatoriske krav til, hvordan fjernadgang kan benyttes på en sikker måde.

Leverandørstyring

Dernæst er mange energiselskaber afhængige af leverandører, som selv typisk er afhængige af underleverandører, hvilket skaber lange leverandørkæder. Dette gør energiselskaberne sårbare over for supply chain-angreb og udbredelsen af sårbarheder i leverandørernes produkter. Sårbarhederne i forhold til angreb i leverandørkæden understreger, at der er behov for at stille skærpede krav til leverandørforhold ligesom NIS2-direktivet stiller krav om forsyningskædesikkerhed. Det er væsentligt, at beredskabsreguleringen stiller krav på en måde, der understøtter, at virksomhederne inddra-

ger vurderingen af eventuelle risici for forsyningssikkerheden i beslutninger om leverandøraftaler, samt at leverandørerne bliver bevidste om deres betydning for forsyningssikkerheden og i en eventuel beredskabssituation.

Derudover ses en tendens hos nogle virksomheder i energisektoren mod outsourcing, hvilket kan medføre at net- og informationssystemernes sårbarhed over for cyberspionage og cyberkriminalitet øges. For at understøtte en tilstrækkelig sikkerhed i forhold til hvem, der har adgang til virksomhedernes net- og informationssystemer og for at undgå kompromittering af disse, vurderes det hensigtsmæssigt, at stille krav til hvordan outsourcing kan ske på forsvarlig vis, herunder en afgrænsning af til hvilke lande der kan foretages outsourcing af driften af kritiske net- og informationssystemer.

3.2.3. Den foreslåede ordning

Klima-, energi-, og forsyningsministeriet foreslår med dette lovforslag at indføre en beredskabsregulering af energisektoren, der modsvarer det hybride trusselsbillede og de nye sårbarheder, som især digitaliseringen af energiinfrastrukturen har introduceret, samtidig med at reguleringen tager højde for nye teknologier, som introduceres i forbindelse med den grønne omstilling. Derudover foreslår Klima-, energi-, og forsyningsministeriet, at beredskabsreguleringen skal stille krav om etableringen af et organisatorisk beredskab, der sikrer ledelsesmæssig forankring af arbejdet med risikostyring i forhold til cybersikkerhed og fysisk sikkerhed.

Ledelsens ansvar

Det foreslås, at virksomhedernes ledelse tager stilling til virksomhedens vurdering af cybersikkerhedsrisici og sikkerhedsrisici mod kritisk infrastruktur som en fast del af virksomhedens arbejde med risikostyring. Den foreslåede ordning vil medføre, at virksomhedens ledelse har et samlet risikobillede, der repræsenterer kendte og mulige risici mod produktionen, forsyningen eller leveringen af tjenesten. Ordningen vil desuden sikre, at den løbende stillingtagen til sikkerhedsrisici forankres hos virksomhedernes beslutningstagere.

Ligeledes foreslås det, at ledelsen deltager i virksomhedens beredskabskoordinering med henblik på, at ledelsen har overblik over og kan gøres ansvarlig for, hvordan virksomheden organiserer virksomhedens beredskab. I tråd med NIS 2-direktivets krav om at ledelsen skal gøres ansvarlige for foranstaltninger til styring af cybersikkerhedsrisici, foreslås det, at ledelsens skal godkende virksomhedens foranstaltninger til styring af risici mod forsyningen og gøres retligt ansvarlige for virksomhedens overtrædelse af forpligtelserne i beredskabsreguleringen. Med den foreslåede ordning går Klima-, Energi-, og Forsyningsministeriet dog videre end direktivet ved at foreslå, at ledelsen både skal kunne gøres ansvarlige for foranstaltninger til styring af organisatorisk sikkerhed, fysisk sikring og cybersikkerhed. Heraf følger at ledelsen også kan gøres retligt ansvarlige for virksomhedernes overtrædelser af beredskabsreguleringen uanset, om der er tale om overtrædelser, der relaterer sig til den organisatoriske sikkerhed, den fysiske sikring af kritiske energiinfrastruktur eller om der er tale om cybersikkerhed. Dette foreslås ud fra en betragtning om, at organisatoriske forhold, cybersikkerhed og fysisk sikring er lige kritiske, samt at det i praksis kan være svært at sondre mellem en overtrædelse, der vedrører det organisatoriske, cybersikkerhed eller fysik sikring.

NIS 2-direktivet stiller derudover krav om, at ledelsen følger kurser, der gør dem i stand til at vurdere risici og styring af cybersikkerhedsrisici. Beredskabsreguleringen vil udvide dette ved at stille krav om, at ledelsen i danske energiselskaber skal tilegne sig en tilstrækkelig viden inden for styring af risici, der relaterer sig til cybersikkerhed såvel som fysisk sikring, god sikkerhedskultur og beredskab. Dette vil understøtte, at vurderingen af sikkerhedsrisici indgår i virksomhedens løbende risikostyring. Den foreslåede ordning vil således sikre, at ledelsen er i stand til at træffe beslutninger på et oplyst grundlag og stille kritiske spørgsmål.

Awareness og uddannelse

For at sikre et højt niveau af sikkerhed af virksomhedens kritiske systemer, infrastruktur og anlæg foreslås det, at virksomhederne stilles krav om at indføre cybersikkerhedsuddannelse og awareness-tiltag for virksomhedens medarbejdere. På den måde vil loven indføre et ambitiøst niveau for, hvordan sikkerhedshensyn og de risici, der er forbundet med det hybride trusselsbillede, gøres til en central del af medarbejdernes bevidsthed, samt

hvordan medarbejderne bør agere for at beskytte kritiske systemer, informationer, infrastruktur og anlæg.

Risikostyring

Med henblik på at forankre risikostyringen på det organisatoriske plan i virksomhederne foreslås det, at virksomhederne skal udarbejde en politik for risikostyring, der skal identificere og vurdere de væsentligste risici for virksomhedens organisation, kritiske net- og informationssystemer og infrastruktur med henblik på opretholdelsen af energiforsyningen.

Som led i dette foreslås det, at der stilles krav om, at virksomhederne skal underrette relevante medarbejdere om de identificerede risici, og identificere hvem der er ansvarlige for at implementere foranstaltningerne. Således vil ordningen sikre en tydelig ansvarsdeling og understøtte, at der vil kunne iværksættes passende tiltag til styring af risici. Det foreslås derudover, at virksomhederne stilles krav om at udpege en beredskabskoordinator, en cyberberedskabskoordinator og et operationelt kontaktpunkt, som bl.a. skal sikre en effektiv kommunikation med myndighederne i krisesituationer. Det foreslås således, at nuværende ordning for udpegelsen af beredskabsroller bør videreføres i vidt omfang. Dog vurderes det hensigtsmæssigt, fremover at ændre betegnelsen it-beredskabsansvarlig til cyberberedskabskoordinator.

Med henblik på at understøtte en bredt forankret sikkerhedsorganisation foreslås det, at der stilles krav om, at virksomhederne indfører procedurer, der følger en fast kadence, og som skal understøtte de tekniske foranstaltninger, som virksomhederne iværksætter. Dette vil bl.a. indebære, at virksomhederne løbende skal tage stilling til risici- og sårbarheder i bl.a. firewalls, leverandørforhold og informationsstrømme, og at virksomhederne har politikker og procedurer for fx patching og opdateringer, der skal imødegå sårbarheder.

Det foreslås, at disse procedurer indgår i virksomhedens politik for risikostyring og skal bl.a. understøtte sikkerheden af virksomhedernes net- og informationssystemer og kritiske anlæg.

For at sikre at det kun er de medarbejdere, der har arbejdsbetinget behov, som har adgang til kritiske anlæg og net- og informationssystemer, fore-

slås det, at virksomhederne skal have politikker og foranstaltninger for adgangsstyring. Der vil således skulle være klart definerede regler for hvilke medarbejdere eller medarbejdergrupper, der kan tilgå forskellige dele af et anlæg eller net- og informationssystemer. Dette indebærer, at virksomhederne vil skulle have procedurer for, hvordan adgange til kritiske anlæg og net- og informationssystemer tildeles, ændres og lukkes for både virksomhedens egne medarbejdere såvel som leverandører. Samtidig foreslås det, at virksomhederne fører log over denne adgang.

Med henblik på at gøre disse sikkerhedsforanstaltninger til en fast del af virksomhedens drift foreslås det, at disse procedurer og de etablerede foranstaltninger skal være genstand for et fast kontrolregime.

Risiko- og sårbarhedsvurderinger

Det foreslås desuden, at virksomhedernes risiko- og sårbarhedsvurderinger og handlingsplaner skal gennemgås med fast interval, eller når nye risici, trusler eller sårbarheder erkendes samt ved væsentlige ændringer af virksomhedens organisation, kritiske net- og informationssystemer eller infrastruktur eller ved ændringer i trusselsbilledet. Det foreslås samtidig, at vurderingen af cybersikkerhedsrisici, organisatoriske risici og fysiske risici kobles sammen ved, at virksomhedernes opdateringer af deres risiko- og sårbarhedsvurderinger af henholdsvis virksomhedens cybersikkerhed og fysiske sikring følger samme kadence for udarbejdelse og indsendelse til Energistyrelsen. Den foreslåede ordning vil således understøtte virksomhedernes modstandsdygtighed, ved at der sikres sammenhæng i virksomhedernes risikostyring af fysiske og cyberrelaterede trusler og sårbarheder.

Leverandørstyring

Det er essentielt, at virksomhederne vurderer risici for forsyningssikkerheden ved indgåelse af leverandøraftaler. Det foreslås derfor, at virksomhederne stiller krav til deres leverandører af tjenester, net- og informationssystemer, komponenter og anlæg, der understøtter processer med betydning for leveringen af tjenesten, således at leverandøren overholder beredskabsreguleringen, samt at virksomhederne fører kontrol hermed. For at understøtte at sikkerhedsrisici udgør et væsentligt parameter i beslutninger vedrørende leverandøraftaler, foreslås det, at virksomhederne skal stille krav

til deres leverandører på baggrund af en risikovurdering af den pågældende aftale, herunder en vurdering af leverandøren samt kritikaliteten af de tjenester, net- og informationssystemer, komponenter eller anlæg, der vil blive påvirket af den pågældende aftale. Derudover bør de sikkerhedsrisici, der er forbundet med leverandør- og outsourcingaftaler, gøres klart for ledelsen i den pågældende virksomhed, således at denne kan træffe beslutninger på et oplyst grundlag.

Risikovurdering af projekter

Det er et væsentligt element i den foreslåede ordning, at virksomhedernes arbejde med risikostyring indebærer, at virksomhederne vil skulle tage stilling til relevante sikkerhedsrisici i forbindelse med projekter og leverandøraftaler, der har mulighed for at påvirke forsyningssikkerheden. Denne påvirkning kan enten være på grund af mulig påvirkning af kritiske dele af organisationen, net- og informationssystemer, der har betydning for leveringen af tjenesten eller som følge af større anlægsprojekter. Derfor foreslås det, at virksomhederne skal foretage en risikovurdering af det pågældende projekt eller af leverandøraftalen, som omfatter en vurdering af eventuelle sikkerhedsrisici.

Derudover foreslås det, at risikovurderingen indgår i ledelsens beslutningsprocedurer, samt at ledelsen gøres ansvarlig for eventuelle risici for forsyningen, der er forbundet hermed. Den foreslåede ordning vil således understøtte, at sikkerhedshensyn tænkes ind i projekter fra starten, samt at risici for forsyningen og herved samfundet minimeres med direkte involvering af ledelsen.

Beredskabsplanlægning

Det foreslås, at der stilles krav om, at virksomhederne foretager den nødvendige beredskabsplanlægning, således at virksomhederne skal udarbejde beredskabsplaner, der er baseret på risiko- og sårbarhedsvurderingerne, og som beskriver relevante tiltag, der skal sikre virksomhedens modstandsdygtighed og kontinuiteten af forsyningen. Beredskabsplanlægningen skal derudover omfatte beredskabssituationer, der i væsentlig grad reducerer funktionaliteten i virksomheden og eventuelt øvrige dele af energisektoren

eller af samfundet. Den foreslåede ordning vil i vidt omfang videreføre gældende ret for udarbejdelse og indhold af beredskabsplaner.

Modstandsdygtighed og krisestyring

Her er krisestyring, hændelseshåndtering og genopretning vitalt for at øge samfundets robusthed og opretholde forsyningssikkerheden. På den baggrund foreslås det, at der stilles krav til virksomhedernes planer for genoprettelse af virksomhedens tjenester, herunder net- og informationssystemer, komponenter og anlæg samt til de tekniske og organisatoriske foranstaltninger, der skal sikre en effektiv hændelseshåndtering. Dette indebærer, at der er etableret og dokumenteret procedurer for hændelseshåndtering.

På den baggrund foreslås det, at gældende krav til øvelsesplanlægning, afholdelse og –evaluering i vidt omfang videreføres. Dertil foreslås det, at der stilles krav om, at relevante leverandører deltager i de øvelser, hvor de vurderes at have en rolle i tilfælde af en hændelse. Dette vil understøtte, at både virksomhederne og deres leverandører er bevidste om deres ansvar i tilfælde af en hændelse. Det er væsentligt, at beredskabsplanlægningen klart definerer roller og ansvar for de involverede i håndteringen af en beredskabssituationen. Ligeledes er det væsentligt, at disse roller koordinerer virksomhedens beredskabsforanstaltninger på tværs af forretningsområder. For el- og gassektorerne videreføres den nuværende praksis med hensyn til Energinets ansvar for at udarbejde risiko- og sårbarhedsvurderinger, sammenfattende beredskabsplaner og sektorberedskabsplaner for henholdsvis det sammenhængende elforsyningssystem og gasforsyningssystem.

Fysisk sikring

Det hybride trusselsbillede bevirker, at virksomheder i energisektoren skal have et højt niveau af modstandsdygtighed over for både naturlige og menneskeskabte farer, hvad enten de er hændelige eller tilsigtede. Dette indebærer også, at virksomhederne skal sikre, at deres anlæg og infrastruktur kan modstå stadigt hyppigere ekstreme vejrhold, som intensiveres af klimaforandringerne. På den baggrund foreslår Klima-, Energi-, og Forsyningsministeriet, at der indføres krav om, at virksomhederne skal vurdere de risici mod deres infrastruktur, der er forbundet med naturkatastrofer og

ekstreme vejrforhold, som klimaforandringerne intensiverer. Således foreslås det, at virksomhedernes sikringsforanstaltninger skal minimere risikoen for hændelser ved at sikre, at deres anlæg og kritiske systemer har lav sårbarhed gennem katastroferisikoreduktions- og klimatilpasningsforanstaltninger. Kravet er således en udmøntning af CER-direktivets krav til samme.

Virksomhedernes sikringsforanstaltninger skal derudover understøtte, at anlæg og forsyningskritiske systemer beskyttes mod uautoriseret adgang. Den fysiske sikring af anlæg og kritiske systemer skal medvirke til at forsinke eller besværliggøre uautoriseret adgang inden for rammerne af sektoransvaret. Det foreslås, at virksomhederne på baggrund af egne risikovurderinger etablerer den nødvendige fysisk sikring i form af passende perimetersikring rund om anlægget, skalsikring af selve anlægget og cellesikring af udvalgte rum eller komponenter i anlægget.

Det betyder, at virksomhederne vil skulle sikre, at de får en alarm, hvis nogen forsøger uautoriseret at tilgå deres anlæg, bygninger og installationer. Virksomheden vil skulle kunne verificere, at der er tale om forsøg på uautoriseret adgang, samt kunne alarmere vagtselskaber, politi eller lignende afhængig af karakteren af uautoriseret adgang. Både detektion, verifikation og alarmering vil skulle ske hurtigt og kvalificeret.

Med henblik på at sikre sammenhæng mellem den logiske og fysisk sikring af energiinfrastrukturen foreslås det, at der stilles krav om at netværksudstyr, der ikke i sig selv er forsyningskritisk, men som giver mulighed for logisk adgang til det forsyningskritiske miljø, skal have fysisk sikring. Dette krav skal medvirke til at minimere risikoen for, at uvedkommende kan få adgang til net- og informationssystemer med betydning for leveringen af tjenesten gennem netværksudstyret placeret på andre lokationer. Tilstrækkelig fysisk sikring kan bidrage til at minimere konsekvenserne af uautoriseret adgang. I den sammenhæng foreslås det, at der stilles krav om, at virksomhederne skal være i stand til at detektere og alarmere.

Derudover fordres det, at virksomhederne har etableret procedurer for hændelseshåndtering, som sikrer at deres anlæg og kritiske systemer er i stand til at videreføre forretningen eller hurtigst muligt komme på fode igen. Det foreslås derfor, at beredskabsplanlægningen skal indeholde planer og procedurer for, hvordan de reagerer på en sådan alarm. Det foreslås desuden, at de nuværende krav til sikringsplaner og genopretning i vidt omfang videreføres.

Cybersikkerhedsforanstaltninger

For at sikre tilstrækkelig og hurtig reetablering efter en hændelse er det centralt, at virksomheden har backup-styring, da backup fungerer som virksomhedens livslinje i tilfælde af fx et cyberangreb, hvor virksomheden har mistet data. Idet nedetid typisk er kritisk i energisektoren, er genopretelse af systemer fra backup, samt procedurer for hvordan man sikrer netværket mod yderligere kompromittering, essentiel. Det foreslås derfor, at der stilles krav til virksomhederne om at have backup-styring. Derudover foreslås det, at virksomhederne skal have en logpolitik for hvilke aktiviteter og datastrømme, der skal logges, samt have etableret tekniske værktøjer, der foretager den relevante logning, som bl.a. kan understøtte hændelseshåndtering og efterfølgende hændelsesopklaring. For de mere forsyningskritiske virksomheder foreslås det derudover, at der stilles krav om, at virksomheden løbende og risikobaseret monitorerer netværket, således at man er i stand til at opdage uregelmæssigheder i net- og informationssystemer i realtid.

Netværkssikkerhed

Det foreslås, at der vil blive stillet krav til virksomhedernes netværkssikkerhed, herunder at virksomhederne skal indføre passende netværkssegmentering, der opdeler net- og informationssystemer i netværk eller zoner ud fra en vurdering af systemernes relationer og funktioner. Gennem segmentering sikrer virksomhederne sig, at de kritiske dele af netværket bliver adskilt fra fx internettet. På den måde sikrer virksomheden sig bedre imod, at et angreb ikke spreder sig og dermed påvirker leveringen af tjenesten. For de mere forsyningskritiske virksomheder foreslås det, at segmenteringen skal være fysisk. Med henblik på at understøtte netværkssikkerheden foreslås det desuden, at virksomhederne skal have overblik og styring over arkitektur og datatrafik, herunder eventuelle integrationspunkter, internetvendte enheder og firewall-regler.

Med den foreslåede ordning vil der blive stillet krav til virksomhedernes brug af fjernadgang til net- og informationssystemer med betydning for leveringen af tjenesten. Det er blevet mere udbredt at benytte fjernadgange til at tilgå net- og informationssystemer, og det kan i mange tilfælde også være med til at højne sikkerheden. Denne udvikling bevirker imidlertid, at

angrebsfladen vokser, hvorfor det foreslås, at der bl.a. stilles krav om, at fjernadgang til virksomhedernes net- og informationssystemer gør brug af multifaktorgodkendelsesløsninger. Samtidig foreslås det, at fjernadgang til forsyningskritiske kontrolrum kun må ske under specifikke forudsætninger såsom kryptering, tidsbegrænset og personlige adgange. På den måde etableres der sikre procedurer for, hvordan fx leverandører får adgang til de kritiske systemer.

Derudover foreslås det, at datatrafik på virksomhedens trådløse netværk skal være krypteret med en tidssvarende løsning. Det foreslås således, at der kan fastsættes regler om kryptering og politikker og procedurer, der skal understøtte, at virksomhedens net- og informationssystemer behandles med den nødvendige fortrolighed, og at risikoen for kompromittering minimeres. Virksomhederne vil ligeledes skulle forholde sig til beskyttelse på mobile enheder. Dette kan være på fx PC, mobiltelefoner og tablets. Dette krav stilles ud fra en betragtning om, at beskyttelse på mobile enheder er et væsentligt element for virksomhedernes samlede sikkerhed. Konkret foreslås det at der stilles krav om, at mobile enheder bl.a. er adgangskodebeskyttet, softwareopdateret og efter relevans antivirusbeskyttet.

Outsourcing

I den nuværende regulering stilles der krav om ejerskab af data, men der stilles ikke krav til hvem og hvor, outsourcingen sker til. I direktiverne sættes der nye krav til virksomhedernes forsyningskædesikkerhed og leverandørstyring, men der sættes ikke krav til placeringen af drift af net- og informationssystemer. Den foreslåede ordning går således videre end direktiverne, idet der vil blive stillet krav om, at net- og informationssystemer af betydning for leveringen af tjenesten på nationalt og europæisk niveau er underlagt EU/EØS-jurisdiktion, og at der ikke skabes afhængigheder, som kan sætte leveringen af tjenesten under pres. Dette kan fx være i tilfælde af en ændret geopolitisk situation. Formålet er bl.a., at det er EU/EØS-regulering – og dermed ikke andre landes lovgivning – der regulerer adgang til og drift af net- og informationssystemer med betydning for leveringen af tjenesten.

3.3. Underretning

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 gennemført sektorvist i regulering gældende for de specifikke sektorer, hvor direktivet finder anvendelse. For energisektoren blev reglerne gennemført i bekendtgørelse om it-beredskab for el og naturgassektoren og bekendtgørelse om beredskab for oliesektoren.

EPCIP-direktivet fastsætter i artikel 6, at ejere og operatører af europæisk kritisk infrastruktur skal udpege en sikkerhedsforbindelsesofficer, der fungerer som kontaktpunkt i forbindelse med sikkerhedsmæssige spørgsmål mellem ejeren og operatøren af den europæiske kritiske infrastruktur og medlemsstatens relevante myndighed.

Endvidere fremgår det bl.a. af EPCIP-direktivet, at hver medlemsstat indfører en passende kommunikationsmekanisme mellem medlemsstatens relevante myndighed og sikkerhedsforbindelsesofficeren eller tilsvarende med henblik på at udveksle relevante oplysninger, om de identificerede risici og trusler i forbindelse med den pågældende europæiske kritiske infrastruktur.

Direktivet indeholder derimod ikke en forpligtelse for ejere og operatører til at underrette myndighederne om hændelser.

For energisektoren er der fastsat regler om underretning af hændelser for klassisk beredskab i bekendtgørelse om beredskab for elsektoren, bekendtgørelse om beredskab for gassektoren og bekendtgørelse om beredskab i oliesektoren.

Det fremgår af bekendtgørelserne for både it-beredskab og klassisk beredskab, at der skal foretages meddelelse om hændelser, der i væsentlig grad reducerer funktionaliteten hos den berørte juridiske person. Bekendtgørelserne stiller også krav om, at de berørte juridiske personer efter en hændelse skal udarbejde en hændelsesevaluering, som skal fremsendes til myndighederne.

Der stilles kun krav om underretning af hændelser i el-, gas- og oliesektoren inden for energisektoren.

3.3.2. Klima-, Energi- og Forsyningsministeriets overvejelser

NIS 2-direktivets artikel 23 indeholder en forpligtelse 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.

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.

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 vurderes mest hensigtsmæssigt, at den nuværende rollefordeling i forhold til at informere

offentligheden videreføres, således at det som udgangspunkt er Energistyrelsen, der foretager dette. CFCS inddrages ved hændelser, der kan påvirke flere sektorer, offentligheden, eller som har grænseoverskridende karakter.

Det vil skulle sikres, at offentligheden informeres på en ansvarlig måde, som ikke kompromitterer fortrolige oplysninger.

3.3.3. Den foreslåede ordning

Det foreslås, at der kan fastsættes nærmere regler om underretning og indrapportering af hændelser. Efter forslået vil de nærmere regler gennemføre NIS 2-direktivets artikel 23 om hændelsesrapporteringer og CER-direktivets artikel 15 om kritiske enheders underretningspligt. Med bemyndigelsen kan der således fastsættes nærmere regler for, til hvem underretning skal ske, hvornår og hvor udførligt underretning skal ske. Desuden kan der fastsættes nærmere regler for, hvilke hændelser der skal indrapporteres.

Det foreslås herudover i overensstemmelse med artikel 23, stk. 1, 2. pkt., i NIS 2-direktivet, at ministeren kan fastsætte nærmere regler om, at virksomheder skal underrette modtagerne af deres tjenester om væsentlige hændelser, der sandsynligvis vil påvirke leveringen af deres tjenester negativt. Der kan endvidere fastsættes regler om, at virksomheder skal oplyse modtagerne af deres tjenester, som potentielt er berørt af en væsentlig hændelse, 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 Klima-, Energi- og Forsyningsministeriet under visse betingelser kan informere offentligheden om den væsentlige hændelse eller kræve, at virksomheden 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 høres virksomheden, der har underrettet om hændelsen, herunder med henblik på vurdering af, hvilke oplysninger der må betragtes som fortrolige. Ved overvejelse om orientering af offentligheden om en hændelse skal det sikres, at 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.

Der sikres også muligheden for, at personer og virksomheder, der ikke ellers er omfattet af lovens anvendelsesområde, frivilligt kan underrette klima-, energi- og forsyningsministen om hændelser, der har betydning for energisektoren.

Der henvises i øvrigt til bemærkninger til de foreslåede §§ 12-15.

3.4. Sikkerhedsgodkendelser og baggrundskontrol

3.4.1. Gældende ret

Der er i Rådets direktiv 2008/114/EF af 8. december 2008 om indkredsning og udpegning af europæisk kritisk infrastruktur og vurdering af behovet for at beskytte den bedre (EPCIP-direktivet) ikke regler om, at der skal være mulighed for at få foretaget baggrundskontrol af personer i kritiske enheder.

For at få adgang til klassificeret information stilles der krav om sikkerhedsgodkendelse i medfør af Justitsministeriets cirkulære nr. 10338 af 17. december 2014 om sikkerhedsbeskyttelse af informationer af fælles interesse for landene i NATO eller EU, andre klassificerede informationer samt informationer af sikkerhedsmæssig beskyttelsesinteresse i øvrigt (sikkerhedscirkulæret). Kravet om sikkerhedsgodkendelse efter sikkerhedscirkulæret gælder for ansatte i offentlige myndigheder, ansatte i private virksomheder, der løser opgaver for offentlige myndigheder, og ansatte i private virksomheder, hvis der i øvrigt i medfør af særlovgivning stilles krav om sikkerhedsgodkendelse for at udføre deres funktion.

På luftfartsområdet er der i Europa-Parlamentet 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 fastsat regler om baggrundskontrol af visse personer, der udfører funktioner inden for luftfartssikkerhed.

Energistyrelsen træffer i dag afgørelser om sikkerhedsgodkendelser for så vidt angår ansatte og konsulenter i Energinet samt konsulenter som indgår i samarbejdsforhold med Energistyrelsen i regi af den Nationale Operative Stab eller Lokale Beredskabsstabe efter lov om Energinet og Sikkerhedscirkulæret.

Energistyrelsen har i dag ikke hjemmel til at sikkerhedsgodkende personer inden for energisektoren, der ikke er ansat i eller udfører opgaver for Energistyrelsen eller en anden offentlig myndighed. Desuden har klima- energi- og forsyningsministeren ikke bemyndigelse til at fastsætte nærmere regler om sikkerhedsgodkendelse i energisektoren.

I perioden fra 2019 til 2023 har Energistyrelsen truffet afgørelser om sikkerhedsgodkendelse af personer inden for energisektoren, der ikke var ansat i eller udførte optager for Energistyrelsen, ud fra en retsvildfarelse om, at sikkerhedscirkulæret indeholder en hjemmel hertil.

3.4.2. Klima-, Energi- og Forsyningsministeriets overvejelser

Det følger af CER-direktivets artikel 14, stk. 1, at medlemsstaterne angiver, på hvilke betingelser en kritisk enhed har tilladelse til at indgive anmodninger om baggrundskontrol af personer, der a) varetager følsomme opgaver i eller til fordel for en kritisk enhed, navnlig vedrørende den kritiske enheds modstandsdygtighed, b) er bemyndiget til at få direkte adgang eller fjernadgang til en kritisk enheds lokaler, oplysninger eller kontrolsystemer, herunder i forbindelse med den kritiske enheds sikkerhed, c) overvejes ansat i stillinger, der hører under kriterierne i litra a) eller b).

Det følger yderligere af CER-direktivets artikel 14, stk. 3, at en baggrundskontrol som minimum skal bekræfte identiteten af den person, der er genstand for baggrundskontrollen og kontrollere strafferegistret for den pågældende person for så vidt angår lovovertrædelser, der ville være relevante for en bestemt stilling. Ifølge præambelbetragtning 32, bør medlemsstaterne anvende det europæiske informationssystem vedrørende strafferegistre i overensstemmelse med procedurerne i Rådets rammeafgørelse 2009/315/RIA og, hvor det er relevant og finder anvendelse, Europa-Parlamentets og Rådets forordning (EU) 2019/816 med henblik på indhentning af oplysninger fra andre medlemsstaters strafferegistre. Medlemsstaterne kan også, hvor det er relevant og finder anvendelse, trække på anden generation af Schengeninformationssystemet (SIS II), der blev oprettet ved Europa-Parlamentets og Rådets forordning (EU) 2018/1862, efterretninger og alle andre tilgængelige objektive oplysninger, som måtte være nødvendige for at fastslå, om den berørte person er egnet til at beklæde den stilling, for hvilken den kritiske enhed har anmodet om en baggrundskontrol.

Baggrundskontrol må kun ske i behørigt begrundede tilfælde og under hensyn til medlemsstatsrisikovurderingen. Baggrundskontrol skal desuden

være forholdsmæssig og strengt begrænset til, hvad der er nødvendigt. Baggrundskontrollen må endvidere udelukkende foretages med henblik på at vurdere en potentiel sikkerhedsrisiko for den berørte kritiske enhed.

Klima-, Energi- og Forsyningsministeriet vurderer, at baggrundskontrol i visse tilfælde ikke vil være tilstrækkeligt til at sikre den fornødne personelsikkerhed i energisektoren. Det vurderes, at der for personer med direkte adgang til at påvirke energiforsyningen i energisektoren er behov for en hjemmel sikkerhedsundersøgelse med henblik på sikkerhedsgodkendelse.

3.4.3. Den foreslåede ordning

Som anført ovenfor vurderer Klima-, Energi- og Forskningsministeriet, at CER-direktivets minimumskrav om baggrundskontrol ikke er tilstrækkeligt til at sikre den fornødne personelsikkerhed i energisektoren.

Det følger derfor af den foreslåede § 16, stk. 1, at klima-, energi- og forsyningsministeren efter forhandling med justitsministeren kan fastsætte regler om sikkerhedsgodkendelse af personer i energisektoren, der har direkte adgang til at påvirke forsyningen i energisektoren, herunder regler om ansøgning om, betingelser for og meddelelse og tilbagekaldelse af sikkerhedsgodkendelser, jf. lovforslagets § 16, stk. 1.

Personer med direkte adgang til at påvirke forsyningen i energisektoren kan f.eks. være ansatte og konsulenter med væsentlige fysiske eller logiske adgange og rettigheder, herunder bl.a. fysisk adgang til virksomhedens kontrolrum eller virksomhedens forsyningskritiske anlæg, eller domænerettigheder eller lignende privilegerede rettigheder til virksomhedens kritiske systemer og netværk.

Det følger derfor af den foreslåede § 16, stk. 2, at klima-, energi- og forsyningsministeren efter forhandling med justitsministeren kan fastsætte regler om baggrundskontrol af personer i energisektoren, der: 1) varetager følsomme opgaver i eller til fordel for en virksomhed, navnlig vedrørende virksomhedens modstandsdygtighed, 2) er bemyndiget til at få direkte adgang eller fjernadgang til virksomhedens lokaler, oplysninger eller kontrolsystemer, herunder i forbindelse med virksomhedens sikkerhed eller 3) overvejes ansat i stillinger, der indebærer opgavevaretagelse efter nr. 1 og/eller nr. 2.

Den foreslåede bestemmelse i § 16, stk. 2, gennemfører artikel 14, stk. 1, i 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), hvorefter medlemsstaterne angiver,

på hvilke betingelser en kritisk enhed i behørigt begrundede tilfælde og under hensyntagen til medlemsstatsrisikovurderingen har tilladelse til at indgive anmodninger om baggrundskontrol af personer, der a) varetager følsomme opgaver i eller til fordel for en kritisk enhed, navnlig vedrørende den kritiske enheds modstandsdygtighed, b) er bemyndiget til at få direkte adgang eller fjernadgang til en kritisk enheds lokaler, oplysninger eller kontrolsystemer, herunder i forbindelse med den kritiske enheds sikkerhed, c) overvejes ansat i stillinger, der hører under kriterierne i litra a) eller b).

Den foreslåede bestemmelse svarer indholdsmæssigt til CER-direktivets artikel 14, stk. 1, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Baggrunden for CER-direktivets artikel 14, stk. 1, beskrives i præambelbetragtning nr. 32, hvoraf det bl.a. fremgår, at risikoen for, at ansatte i kritiske enheder eller deres kontrahenter misbruger for eksempel deres adgangsret inden for den kritiske enheds organisation til at skade og forvolde skade, giver anledning til stigende bekymring.

Efter den foreslåede bestemmelse vil klima-, energi- og forsyningsministeren efter forhandling med justitsministeren kunne fastsætte nærmere regler, der sammen med bestemmelsen vil skulle gennemføre CER-direktivets artikel 14.

Det foreslås, at klima-, energi- og forsyningsministeren bemyndiges til at fastsætte nærmere regler om, på hvilke betingelser en virksomhed vil kunne anmode om baggrundskontrol af en person, således at særlige sektorspecifikke hensyn kan varetages.

Det bemærkes i den forbindelse, at gennemførelse af baggrundskontrol vil ske på grundlag af en anmodning fra virksomheden og forudsætter, at den pågældende person har meddelt samtykke dertil.

Det forudsættes i øvrigt, at udstedelse af nærmere regler og den efterfølgende administration af ordningen vil ske i overensstemmelse med kravene i CER-direktivets artikel 14, stk. 2 og 3.

Klima-, Energi- og Forsyningsministeriet vurderer, at den foreslåede ordning vil give mulighed for at sikre den fornødne personelsikkerhed i hele energisektoren.

Der ændres ikke i gældende ordning, hvor Energistyrelsen kan træffe afgørelser om sikkerhedsgodkendelser for så vidt angår ansatte og konsulenter i

Energinet samt konsulenter som indgår i samarbejdsforhold med Energistyrelsen i regi af den Nationale Operative Stab eller Lokale Beredskabsstabe efter Lov om Energinet og Sikkerhedscirkulæret.

Der henvises i øvrigt til bemærkningerne til den foreslåede § 16.

3.5. Gebyrbestemmelser om gebyrbetaling for myndighedsbehandling

3.5.1. Gældende ret

3.5.1.1. Virksomhedernes gebyrbetaling for myndighedsbehandling

Det følger af elforsyningslovens § 51d og gasforsyningslovens § 30 a, stk. 5-7, at de virksomheder, der i dag er pålagt krav om beredskabsplanlægning, fysisksikring og cybersikkerhed i el- og gassektorene, halvårligt skal betale et beløb til Klima-, Energi- og Forsyningsministeriet til dækning af omkostningerne af ministeriets tilsyn med virksomhedernes overholdelse af regler udstedt i medfør af elforsyningslovens § 85 b, stk. 4 og 85 c, stk. 6, samt gasforsyningslovens § 15 a, stk. 4 og 15 b, stk. 6.

Denne betalingsforpligtigelse trådte i kraft d. 1. juli 2019 ved lov nr. 494 af 1. maj 2019 om ændring lov om Energinet, lov om elforsyning og lov om naturgasforsyning. Med denne lov sørgedes der for, at den planlagte virksomhedsoverdragelse, der skulle ske af tilsynsforpligtigelsen med de ovennævnte beredskabsregler fra Energinet til Energistyrelsen d. 1. juli 2019, kunne finansieres gennem en betaling fra de virksomheder, der modtog dette tilsyn.

Forpligtelsen til at føre tilsyn med el- og naturgassektorernes almene beredskaber blev i 2005 lagt hos Energinet. Placeringen skyldtes, at lovgiver dengang fandt, at Energinet modsat Energistyrelsen havde den faglige viden til at varetage tilsynet med virksomhedernes beredskab. Denne tankegang blev sidenhen videreført, da man ved lov nr. 1755 af 27. december 2016 om ændring af lov om elforsyning og lov om naturgasforsyning indførte krav om it-beredskab for el- og naturgassektorerne. Samtidigt blev det påpeget, at der ville være synergi, hvis tilsynet med det klassiske beredskab og it-beredskabet blev placeret det samme sted hos Energinet.

I forbindelse med folketingsbehandlingen af ovennævnte lovændring i 2016 oplyste energi-, forsynings- og klimaministeren over for Energi-, Forsynings- og Klimaudvalget, at ministeren senest med udgangen af 2018 ville

gennemføre en evaluering af placeringen af tilsynet med el- og naturgasvirksomhedernes it-beredskab. Den færdige evaluering blev oversendt til Energi-, Forsynings- og Klimaudvalget den 13. september 2018 og indeholdt bl.a. en anbefaling om, at tilsynsopgaver med det almene beredskab og tilsynet med it-beredskabet skulle flyttes fra Energinet til Energistyrelsen. Evalueringen konkluderede således, at Energistyrelsen siden 2016 havde opbygget et fagligt miljø, der kunne understøtte varetagelsen af opgaven med at føre tilsyn med el- og naturgasvirksomhedernes it-beredskab.

Ministeren besluttede på baggrund af evalueringen at overføre tilsynet med el- og naturgasvirksomhedernes almene beredskab og it-beredskab fra Energinet til Energistyrelsen med virkning fra den 1. juli 2019. Hovedformålet med at flytte tilsynet med det almene beredskab og it-beredskabet fra Energinet til Energistyrelsen var, at det derved kunne undgås, at Energinet havde en dobbeltrolle som koordinerende funktion i beredskabet på den ene side og tilsynsførende myndighed over for el- og naturgasvirksomhederne på den anden side. Ved at flytte myndighedstilsynet til Energistyrelsen fjernede ministeren en hindring for Energinets mulighed for at samarbejde med virksomhederne, særligt i forbindelse med evaluering af hændelser og forebyggelse og forberedelse af eventuelle fremtidige hændelser.

De ovennævnte § 51 d i elforsyningsloven og § 30 a, stk. 5-7 i gasforsyningsloven er bemyndigelsesbestemmelser, hvorefter ministeren kan fastsætte nærmere regler om størrelsen af de beløb, som de nævnte virksomheder skal betale og nærmere regler om betaling og opkrævning af disse beløb.

Gebyrernes størrelse er blevet fastsat ved bekendtgørelse i bekendtgørelse nr. 805 af 15. juni 2023 om betaling for myndighedsbehandling i Energistyrelsen. Gebyrerne er fastsat som generelle grundbeløb fordelt på 4 kategorier og gradueret således, at gebyret er størst for virksomheder i kategori 1 og lavest for virksomheder i kategori 4. De 4 gebyrkategorier for gebyropkrævningen er baseret på den kategorisering, der foretages af virksomhederne efter it-beredskabsbekendtgørelsen dog under hensyntagen til antallet af klasse 1 anlæg, som virksomheden ejer. Klassificeringen af anlæg foretages efter elberedskabsbekendtgørelsen og naturgasberedskabsbekendtgørelsen.

Virksomheder har i dag mulighed for at få samordnet beredskab, hvor en virksomhed forestår beredskabsplanlægningen og udførelsen på vegne af to eller flere virksomheder, som regel fordi der er en koncernforbindelse, tæt geografisk tilknytning eller afhængighed eller at ejeren af et energianlæg,

fx. en solcellepark, også er operatør af en lang række andre solparker, som den tidligere har ejet, men solgt fra til investorer. Når virksomheder har fået samordnet beredskab på både det almene beredskab og it-beredskab, har Energistyrelsen kun ført tilsyn med den virksomhed, der forestår beredskabsplanlægningen og udførelsen heraf, hvorfor kun denne virksomhed skal betale det generelle grundbeløb for tilsyn med virksomhedens beredskab, alt i mens at den anden virksomhed har sluppet for at betale det generelle grundbeløb.

Endvidere har klima-, energi- og forsyningsministeren i førnævnte bekendtgørelse om betaling for myndighedsbehandling i Energistyrelsen udnyttet sin bemyndigelse i § 90 i lov om elforsyning og § 52 i lov om naturgasforsyning til at afskære klageadgang til Energiklagenævnet for afgørelser truffet efter reglerne udstedt i medfør af de § 51 d, og 30 a, stk. 5-7. Det er ikke vurderet at være retssikkerhedsmæssigt betænkeligt at fravige udgangspunktet om klageadgang i dette konkrete tilfælde, da afgørelser om opkrævning af beløb ikke vil være egnede til at blive gjort til genstand for prøvelse ved Energiklagenævnet, som normalt er klageinstans for Energistyrelsens afgørelser, eller ved anden klagemyndighed.

Det er endvidere ikke vurderet betænkeligt at afskære klageadgangen til Energiklagenævnet, da afgørelserne vedrører opkrævning af fakturaer, der er udstedt på baggrund af regler fastsat i bekendtgørelsen om betaling for myndighedsbehandling i Energistyrelsen. Spørgsmålet om afgørelsens lovlighed og rigtighed vil derfor typisk være et spørgsmål om, hvorvidt beregningen, der ligger til grund for opgørelsen af det opkrævede beløbet, er korrekt. Sådanne spørgsmål ligger ikke oplagt inden for Energiklagenævnets særlige kompetenceområde som prøveinstans for energifaglige og juridiske spørgsmål, navnlig energiretlige spørgsmål, og rekursordningens styringsfunktion vil således være begrænset.

Energistyrelsens afgørelser om opkrævning vil kunne prøves ved domstolene ligesom alle andre myndighedsafgørelser jf. grundlovens § 63. På den baggrund vurderes det, at hensynet til virksomhedernes retssikkerhed ift. gebyrbetaling, for den myndighedsbehandling de modtager, er tilstrækkeligt tilgodeset.

3.5.1.2. Energinets gebyrbetaling for myndighedsbehandling

Klima-, energi- og forsyningsministerens tilsyn med det almene beredskab og it-beredskabet hos Energinet er siden den 1. juli 2019 blevet finansieret

via lovfastsat grundbeløb i elforsyningslovens § 51 b og gasforsyningslovens § 30 a, stk. 3, hvor beløbet er en delmængde af et større beløb, der opkræves for tilsyn med Energinets aktiviteter efter de to love.

Fra 2017 frem til 2019 var det kun tilsynet med Energinets it-beredskab, der var gebyrfinansieret, da der blev indført separat hjemmel til dette i den dagældende § 51, stk. 2 i elforsyningsloven og § 30, stk. 2 i naturgasforsyningsloven i forbindelse med indførelsen af kravene om it-beredskab i el- og naturgassektorerne i lov nr. 1755 af 12. december 2016 om ændring af lov om elforsyning og lov om naturgasforsyning.

Disse paragraffer blev sidenhen ændret ved lov nr. 1399 af 5. december 2017 om ændring af lov om elforsyning, lov om fremme af vedvarende energi, lov om naturgasforsyning, lov om Energinet.dk og lov om varmeforsyning. Her ændredes gebyrerne for klima-, energi- og forsyningsministerens tilsyn fra kun at have været opkrævet fra Energinet til at være opkrævet hos de individuelle virksomheder, således det kunne sikres, at virksomhederne kun betalte for den myndighedsbehandling, som de fik. I den forbindelse ændredes gebyropkrævningen for tilsynet med Energinet og denne virksomheds helejede datterselskaber til at være lovfikseret grundbeløb fastsat i hhv. elforsyningslovens § 51 b, stk. 2, på 4,5 mio. kr. og naturgasforsyningslovens § 30 a, stk. 3 på 0,7 mio. kr.

I 2019 ændredes de to paragraffer igen ved lov 494 af 1. maj 2019 om ændring af lov om Energinet, lov om elforsyning og lov om naturgasforsyning. Her ændredes beløbene således, at Energistyrelsens tilsyn med Energinets almene beredskab også kunne finansieres af Energinet, på samme måde som tilsynet med it-beredskabet var finansieret. På den måde sikredes ensartethed i finansieringen af Energistyrelsens beredskabstilsyn med Energinet.

Klima-, energi- og forsyningsministeren opkræver i dag årligt gebyr for 1000 timers tilsyn med Energinets almene beredskab og it-beredskab. De 1000 timer er lovmæssigt fordelt med 600 timer til Energinets El TSO og 400 timer til Energinets Gas TSO, hvilket efter Energistyrelsens 2024 timetakts for en gennemsnitsmedarbejder på 746,68 kr. svarer til 746.680 kr. Der er i tillæg til de 1000 timeres tilsyn, som Energistyrelsen fører, også finansieret 50 timers ekstern konsulentbistand til tilsyn med it-beredskab pga. områdets særlige tekniske karakter. Denne udgift udgjorde 62.500 kr., da man anlagde en formodning om at en konsulent kostede 1250 kr. i timen

3.5.2. Klima-, Energi- og Forsyningsministeriets overvejelser

3.5.2.1 Generelle grundbeløb til finansiering af almindeligt tilsyn og administration af ordningen

Klima-, Energi- og Forsyningsministeriet vurderer, at den nuværende gebyrordning for dækning af de omkostninger, der er til administration af ordningen og tilsynet med virksomhedernes organisatoriske beredskab, fysiske sikring og cybersikkerhed, er en god og gennemsigtig ordning, der bedst muligt sikrer, at virksomhederne kun betaler for det tilsyn, de modtager, samtidig med at Energistyrelsen har en let administrerbar gebyrordning, der samtidig er fleksibel nok til, at der kan ske justering af gebyrerne, såfremt tilsynsmængden for virksomhederne generelt set skal op- eller nedjusteres.

Klima-, Energi- og Forsyningsministeriet foreslår derfor, at den eksisterende gebyrordning for tilsynet med el- og naturgasvirksomhedernes organisatoriske beredskab, fysiske sikring og cybersikkerhed og dækning af de omkostninger der er til administration af ordningen videreføres i dette lovforslag og udvides til at gælde alle virksomheder, omfattet af loven, herunder også Energinets El TSO og Gas TSO. Dette betyder, at § 51 d i elforsyningsloven og § 30 a, stk. 5 og 6 i gasforsyningsloven ophæves helt og erstattes af den foreslåede § 19 i denne lov, samt at de beløb, som opkræves for tilsyn med Energinet i elforsyningslovens § 51 b og gasforsyningslovens § 30 a, stk. 3, 1 pkt., justeres, så beløbene efter § 51 b og 30 a, reflekterer udgifterne til tilsyn med Energinet efter hhv. elforsyningsloven og gasforsyningsloven.

Justeringen af beløbet i elforsyningslovens § 51 b vil blive foretaget i lovforslag [om ændring af lov om elforsyning mm.], idet paragraffens indhold skal justeres af andre hensyn der.

Som beskrevet i afsnittet om gældende ret har virksomheder i dag mulighed for at få samordnet beredskab, hvor kun den udførende virksomhed opkræves betaling for tilsyn med beredskabsplanlægningen. Denne praksis har medført en uhensigtsmæssighed i nogle tilfælde, hvor en virksomhed varetager beredskabet for et stort antal anlæg, som regel vedvarende energi-anlæg, der hver for sig kun er klasse 3 eller 2 anlæg, men som tilsammen udgør en meget stor MW-andel af den danske elproduktion.

Det er Klima-, Energi- og Forsyningsministeriet vurdering, at når dette er tilfældet, bør virksomheden, der varetager det samordnede beredskab, modtage tilsyn, som var de niveau 5-virksomhed med et større antal klasse 4 el. 5 anlæg. Dette problem er løst i § 4, hvor virksomheder med samordnet beredskab, der tilsammen har så stor en energi- eller kundeportefølje at

de falder ind under et højere niveau, bliver indplaceret på dette niveau. Dette har samtidig den konsekvens, at virksomheden indplaceres i den tilsvarende gebyrkategori, og dermed er det Klima-, Energi- og Forsyningsministeriet vurdering, at der er den nødvendige finansiering af disse særtilfælde med store samordnede beredskaber.

3.5.2.2 Aktivitetsberegnet beløb til finansiering af ad-hoc tilsyn

I tillæg til de almindelige planlagte tilsyn med fast kadence kan der blive behov for ekstraordinære tilsyn i situationer, hvor klima-, energi- og forsyningsministeren bliver opmærksom på eller mistænker særligt grove overtrædelser af reglerne i loven eller fastsat i medfør af loven. Her kan tilsyn med virksomheden ikke vente til tidspunktet, hvor tilsynet i den normale tilsynskadence er planlagt til at blive afholdt.

Sådanne ekstraordinære tilsyn kan i dag ikke gebyrfinansieres, hvilket i sidste ende betyder, at andre opgaver må bortprioriteres af Klima-, Energi- og Forsyningsministeriet. For at bringe lighed mellem tilsynsopgaverne, uanset om der er tale om almindeligt planlagte tilsyn efter den normale tilsynskadence eller ekstraordinære tilsyn uden for kadencen, vurderer Klima-, Energi- og Forsyningsministeriet, at det er mest hensigtsmæssigt også at gebyrfinansiere ekstraordinære tilsyn. Det er Klima-, Energi- og Forsyningsministeriets vurdering, at det er mest gennemsigtigt at sådanne ekstraordinære tilsyn bliver afregnet som timeafregnede gebyrer, hvor virksomheden opkræves for det antal timer, der er medgået i udførelsen af det ekstraordinære tilsyn.

Et af de kriterier, der lægges til grund for vurderingen af behovet for gennemførelsen af et eller flere ekstraordinære tilsyn med en virksomhed, er, om overtrædelsen eller den mistænkte overtrædelse vurderes til konkret at kunne bringe leveringen af virksomhedens tjeneste i fare.

Da dette ekstraordinære tilsyn indledes på grund af en konkret begrundet mistanke om en virksomheds manglende overholdelse eller tilsidesættelse af reglerne på en sådan måde, at det har potentiale til at bringe virksomhedens levering af deres tjeneste i fare, findes det ikke rimeligt eller gennemsigtig blot at indregne udgifter til sådanne ekstraordinære tilsyn i de generelle grundbeløb, der finansierer de almindelige tilsyn. Hvis det var tilfældet, vil andre virksomheder, der overholder reglerne, reelt komme til at afholde en andel, om end det er en meget lille andel, af tilsynsudgiften for

andre virksomheder, fordi de andre virksomheder ikke overholder gældende ret. Dette findes urimeligt, hvorfor Klima-, Energi- og Forsyningsministeriet foreslår en separat gebyrfinansiering af sådanne tilsyn.

3.5.2.3 Beløb til finansiering af behandling virksomhedernes ansøgninger i egeninteresse

I dag modtager Energistyrelsen, til hvem klima-, energi- og forsyningsministeren har delegeret arbejdet med beredskabet i energisektoren, en række ansøgninger og dispensationsansøgninger efter reglerne i elberedskabs-, gasberedskabs- og it-beredskabsbekendtgørelserne. Der er tale om ansøgninger om samordnet beredskab mellem 2 eller flere virksomheder, dispensation fra overholdelse af alle eller dele af reglerne i de tre bekendtgørelser, dispensationer fra frister, dispensationer om personsammenfald (hvor den samme person i en virksomhed er både beredskabskoordinator og it-beredskabsansvarlig og/eller en del af ledelsen). Endeligt behandler Energistyrelsen et stadigt stigende antal ansøgninger om sikkerhedsgodkendelse af personer efter cirkulære CIR1H nr. 10338 af 17. december 2014.

Sagsbehandlingen af disse ansøgninger, dispensationsansøgninger og ansøgning om sikkerhedsgodkendelse er i dag ikke gebyrfinansieret.

Det er Klima-, Energi- og Forsyningsministeriets vurdering, at det fremover vil være hensigtsmæssigt at gebyrfinansiere sagsbehandlingen af de ovennævnte ansøgninger. Dette er, fordi klima-, energi- og forsyningsministeren må forventes at modtage væsentligt flere af disse ansøgninger, idet der fremover vil være mange flere virksomheder, der er omfattet reglerne om beredskab, ligesom der i den foreslåede §16 om sikkerhedsgodkendelser og baggrundskontrol åbnes op for, at endnu flere virksomheder vil blive pålagt krav om sikkerhedsgodkendelser og baggrundskontrol. Således vurderes udgiften til denne sagsbehandling at stige, hvorfor Klima-, Energi- og Forsyningsministeriet må sikre tilsvarende indtægt til afholdelsen af udgiften.

Ligeledes vil gebyrfinansieringen også være med til moderere antallet af ansøgninger, idet virksomhederne i så fald må forventes at overveje om udgiften til ansøgningen stemmer overens med den værdi, som virksomheden forventer at vinde ved en forhåbentlig godkendt ansøgning. Dette gør sig særligt gældende for sikkerhedsgodkendelserne og de udvidede baggrundskontroller, hvor der i dag observeres en tendens til et overforbrug af sikkerhedsgodkendelser.

Det må forventes, at virksomhederne, på samme måde som i dag, overvælter de øgede omkostninger, som gebyrerne medfører, på prisen for den tjeneste, som de leverer.

3.5.3. Den foreslåede ordning

Klima-, Energi- og Forsyningsministeriet foreslår med § 19, stk. 1, at de omfattede virksomheder halvårligt skal betale et beløb til Klima-, Energi- og Forsyningsministeriet til dækning af de omkostninger, der er til administration af ordningen og tilsyn med virksomhederne efter reglerne i denne lov og regler udstedt i medfør af denne lov. Den halvårlige betaling er en fortsættelse af den hidtidige frekvens for betaling for tilsyn med virksomhedernes beredskabsarbejde. Den halvårlige frekvens sikrer, at der ikke skal betales for store beløb ad gangen, samt at opkrævningen kan finde sted i samme frekvens som andre betalinger for myndighedsbehandling efter elforsyningsloven, gasforsyningsloven og olieberedskabsloven.

Desuden foreslår Klima, Energi- og Forsyningsministeriet i § 19, stk. 2, at de omfattede virksomheder halvårligt betaler et beløb til Klima-, Energi- og Forsyningsministeriet til dækning af omkostninger til ad-hoc tilsyn med virksomhederne efter reglerne i denne lov eller efter regler udstedt i medfør af regler i denne lov. Dette beløb skal dække tilsyn, der er blevet gennemført med virksomhederne uden for den almindelige kadence, som virksomhederne modtager tilsyn fx. årligt eller hvert tredje år. Det foreslås at beløbet virksomhederne skal betale efter § 19, stk. 2, afregnes på timebasis, i stedet for generelle grundbeløb som i stk. 1.

Det foreslås endvidere i § 19, stk. 3 at klima-, energi- og forsyningsministeren kan fastsætte nærmere regler om betaling og opkrævning af beløb til dækning af omkostningerne efter § 19, stk. 1 og stk. 2. Den foreslåede paragraf indebærer at størrelsen af gebyrerne for både stk. 1 og stk. 2 som hidtil fastsættes administrativt ved bekendtgørelse.

Det forventes, at klima-, energi- og forsyningsministeren vil bruge bemyndigelsen i § 19, stk. 3 til at gebyrerne efter § 19, stk. 1, som det er tilfældet i dag, fastsættes som generelle grundbeløb, der dækker de udgifter som Klima-, Energi- og Forsyningsministeriet har med tilsyn med virksomhederne og dækning af de omkostninger der er til administration af ordningen. Det forventes, at gebyrstørrelserne vil blive differentieret i minimum 6 gebyrkategorier, hvor gebyret vil være lavest for gebyrkategori 1 og højest for gebyrkategori 6, således at disse svarer til den niveauinddeling, der sker af

virksomhederne i reglerne udmøntet efter § 4 om kategorisering af virksomheder samt virksomhedernes systemer og anlæg, dog med indførelsen af en ekstra gebyrkategori (kategori 6).

Denne niveauinddeling er som beskrevet bestemmende for hvor stort et reguleringstryk virksomheden bliver underlagt efter disse regler, ligesom det også er bestemmende for hvor ofte og hvor mange timers tilsyn Klima-, Energi- og Forsyningsministeriet i gennemsnit forventer at bruge på virksomhederne på det givne niveau. Klima-, energi og forsyningsministeren forventes at bruge bemyndigelsen til at indføre en ekstra gebyrkategori 6, som skal bruges specifikt til Energinets EL TSO og GAS TSO, samt andre virksomheder der grundet deres helt særlige ansvar for funktionen af energisystemerne i Danmark, bør modtage et væsentligt mere grundigt og dybdegående tilsyn end alle andre virksomheder.

I tillæg hertil vil gebyrkategorierne, som det er tilfældet i dag, tage højde for antallet af anlæg som virksomhederne ejer. Virksomheder i niveau 5 med mange klasse 4 og 5 anlæg vil således blive indplaceret i en højere gebyrkategori, end virksomheder i niveau 5 med kun få klasse 4 og 5 anlæg.

Det forventes endvidere at klima-, energi- og forsyningsministeren vil bruge bemyndigelsen i § 19, stk. 3, til at fastsætte regler om at gebyrerne efter den forslåede § 19, stk. 2 vil blive afregnet på timebasis, således at virksomheden opkræves det antal timer, der er blevet brugt af klima-, energi- og forsyningsministeren til ad-hoc tilsyn, ganget med den budgetterede timepris i det pågældende år hvor tilsynet er blevet gennemført. Det forventes endvidere, at klima-, energi- og forsyningsministeren fastsætter, at hvis ad-hoc tilsynet strækker sig over 2 kalenderår, fx. fordi det er blevet indledt i slutningen af december, så benyttes den budgetterede timepris i det år, hvor ad-hoc tilsynet er blevet afsluttet.

Det forventes, at klima-, energi- og forsyningsministeren fastsætter, at den budgetterede timepris fastsættes på grundlag af gennemsnitlige lønudgifter tillagt en forholdsmæssig andel af generelle fællesomkostninger, relevante henførbare, indirekte omkostninger og direkte øvrige driftsomkostninger, der er forbundet med myndighedsbehandlingen i det pågældende regnskabsår. Energistyrelsens omkostningsfordeling følger Finansministeriets vejledninger herfor.

Det forventes desuden, at klima-, energi- og forsyningsministeren vil bruge bemyndigelsen i § 19 stk. 3 til at fastsætte, at gebyrerne efter stk. 1 og 2,

skal indbetales senest 30 dage efter fakturaens udstedelse, og der såfremt beløbet ikke betales rettidigt, betales renter af det opkrævede beløb i medfør af renteloven. Klima-, energi- og forsyningsministeren forventes også bruge bemyndigelsen til at fastsætte regler om efterregulering af eventuelle betalinger opkrævet i medfør af i § 19, stk. 2.

Endeligt foreslår Klima-, Energi- og Forsyningsministeriet i § 20, stk. 1, at virksomheder ved indgivelse af ansøgninger eller dispensationer halvårligt betaler et beløb for behandling af ansøgninger og dispensationer efter reglerne i denne lov eller efter regler udstedt i medfør af loven. Der forstås herved, at virksomhederne kun skal betale, såfremt de har de rent faktisk har indgivet en eller flere ansøgninger eller dispensationsansøgninger til behandling efter loven.

Det forventes endvidere, at klima-, energi- og forsyningsministeren vil bruge bemyndigelsen i § 20, stk. 2, til at fastsætte at gebyrerne efter den forslåede § 20, stk. 1 til at blive administrativt fastsatte gebyrer i en bekendtgørelse. Der er tale om et fast vederlag pr. ansøgning, hvor vederlaget vil være differentieret alt efter hvad det er, der ansøges om. Det forventes således, at ministeren vil fastsætte et vederlag for hhv. ansøgninger om samordnet beredskab, ansøgninger om personsammenfald, ansøgning om dispensation efter den generelle dispensationsregel, ansøgning om sikkerhedsgodkendelse af en medarbejder og ansøgning om baggrundskontrol af en medarbejder.

Det forventes, at vederlaget for de enkelte ansøgningstyper i første omgang vil blive fastsat på baggrund af klima-, energi- og forsyningsministerens initiale estimering af hvor mange timer det gennemsnitligt tager at behandle en sådanne ansøgning ganget med den budgetteret timepris. Efter der er opbygget et tilstrækkeligt datagrundlag gennem medarbejdernes tidsregistrering, vil de initiale estimering erstattes af det konkrete gennemsnitlige tidsforbrug pr. ansøgningstype, hvorfor de fastsatte vederlag vil op- eller nedjusteres på dette grundlag ligesom hvis den budgetterede timepris ændrer sig, idet gebyrordningen skal balancere over en 4-årig periode i overensstemmelse med Finansministeriets budgetvejledning.

Desuden forventes klima-, energi- og forsyningsministeren i medfør af den forslåede bemyndigelse i § 20, stk. 2 at fastsætte, at den budgetterede timepris fastsættes på grundlag af gennemsnitlige lønudgifter tillagt en forholdsmæssig andel af generelle fællesomkostninger, relevante henførbare, indirekte omkostninger og direkte øvrige driftsomkostninger, der er forbundet

med myndighedsbehandlingen i det pågældende regnskabsår. Klima-, Energi- og Forsyningsministeriets omkostningsfordeling vil følge Finansministeriets vejledninger herfor.

Endeligt forventes det, at klima-, energi- og forsyningsministeren vil bruge bemyndigelsen i § 20 stk. 2 til at fastsætte, at gebyrerne efter stk. 1, skal indbetales inden for et fast tidspunkt efter fakturaens udstedelse, og der såfremt beløbet ikke betales rettidigt, betales renter af det opkrævede beløb i medfør af renteloven, samt at vederlagene indkræves sammen med de vederlag, der opkræves efter § 19, stk. 1 og 2.

For nærmere beskrivelse, henvises til bemærkningerne til lovforslagets § 18 og 19.

3.6. Tilsyn

3.6.1. Gældende ret

Der føres med tilsyn med virksomheder i elsektoren som har en produktionsbevilling, en produktionstilladelse eller som har et balanceansvar for energisektoren. Desuden føres der tilsyn med distributions og transmissionsvirksomheder. Der føres tilsyn med virksomhedernes klassiske beredskab efter elforsyningslovens § 85 b og med virksomhedernes it-beredskab efter elforsyningslovens § 85 c. De nærmere regler om tilsyn fremgår af bekendtgørelse om beredskab for elsektoren og bekendtgørelse om it-beredskab for el- og naturgassektorerne.

I gassektoren føres der tilsyn med virksomheder der er bevillingspligtige efter gasforsyningsloven og Energinet samt Energinets helejede datterselskaber. Der føres tilsyn med virksomhedernes klassiske beredskab efter gasforsyningslovens § 15 a og med virksomhedernes it-beredskab efter gasforsyningslovens § 15 b. De nærmere regler om tilsyn fremgår af bekendtgørelse om beredskab for naturgassektoren og bekendtgørelse om it-beredskab for el- og naturgassektorerne.

For el- og gassektorerne inddeles virksomhederne i kategorier, der afgør frekvensen af tilsyn. Virksomhederne inddeles i 3 kategorier, hvor kategori 1 er de mindst kritiske virksomheder og kategori 3 er de mest kritiske virksomheder. Der føres tilsyn mindst hvert tredje år med virksomheder i kategori 2 og 3, men der hvert år føres tilsyn med virksomheder i kategori 1.

For oliesektoren føres der tilsyn med lagringspligtige virksomheder og den centrale lagerenhed. Tilsynet føres med hjemmel i olieberedskabslovens §

17 for både det klassiske beredskab og it-beredskabet. De nærmere regler for tilsyn fremgår af bekendtgørelse om beredskab for oliesektoren.

Ens for alle sektorer er, at der tilsynet sker proaktivt med mulighed for at foretage et reaktivt tilsyn.

3.6.2. Klima-, Energi- og Forsyningsministeriets overvejelser

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.

Direktivet skelner mellem væsentlige og vigtige enheder, til brug for tilsynsfrekvens og hvilke tiltag det er muligt for myndighederne at anvende ved tilsyn. Sondringen mellem enheder i direktivet, passer sammen med den måde de nuværende regler for tilsyn sondrer mellem virksomheder i energisektoren. Den nuværende ordning i for el- og gassektorerne med kategorisering af virksomheder bør derfor videreføres, da dette hjælper til at sikre en rimelig balance mellem forpligtelserne af virksomhederne og tilsynsenheden, og er foreneligt med den sondring som foreslås efter NIS 2-direktivet. Ordningen skal udvides til at omfatte de andre sektorer, som skal omfattes af loven. Fremadrettet forventes det, at virksomheder ikke bliver inddelt i kategorier, men derimod i niveauer. Desuden forventes det fremadrettet, jo højere et niveau en virksomhed inddeles på, jo mere kritisk er virksomhed for forsyningssikkerheden. Dermed vil niveau 1- virksomheder være de mindst kritiske, mens et højere niveau betyder at en virksomhed er mere kritiske og skal efterleve flere krav.

Virksomhederne i de forskellige sektorer er vigtige for den danske forsyning af energi, derfor forventes det at de nuværende regler om proaktive tilsyn videreføres for alle undtagen de mindst kritiske virksomheder.

Direktivet oplister herudover de tilsynsforanstaltninger, som minimum skal kunne anvendes ved tilsyn med virksomhederne. Der er navnlig tale om, at tilsynsmyndigheden 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.

Der skelnes i NIS 2-direktiver mellem vigtige og væsentlige enheder i forhold til, hvilke tilsynsforanstaltninger der skal kunne anvendes. Det er dog ministeriet vurdering, at alle tilsynsforanstaltninger som udgangspunkt skal kunne anvendes overfor alle virksomheder uagtet virksomhedens niveau, for at sikre en robust energisektor.

I dag føres der tilsyn, med henblik på at skabe værdi i sektoren, for at højne det fælles sikkerhedsniveau i energisektoren. Denne værdiskabende tilgang til tilsynet skal være grundstenen i den måde de forskellige tilsynsforanstaltninger skal anvendes.

3.6.3. Den foreslåede ordning

Det foreslås at klima-, energi- og forsyningsministeren fører tilsyn med virksomheder i energisektoren.

Det foreslås at Klima-, Energi- og Forsyningsministeriet for at opfylde deres tilsynsforpligtelser kan anvende en række tilsyns- og kontrolforanstaltninger, såsom at føre tilsyn og kontrol hos virksomhed, foretage regelmæssige tilsyns- og kontrolbesøg samt ad-hoc tilsyn. Desuden er der hjemmel til at få udleveret oplysninger og få adgang til relevante data og dokumenter.

Den foreslåede ordning vil medføre, at ministeren kan fastsætte nærmere regler om, at tilsynet kan ske ved et fysisk tilsyn med fremmøde hos virksomheden, eller om at tilsynet kan ske som et eksternt tilsyn. Ministeren vil også kunne fastsætte nærmere regler om hyppigheden af tilsyn.

Den foreslåede ordning vil derudover kunne anvendes til at fastsætte nærmere regler om, den geografiske og tidsmæssige udstrækning af tilsyn, så længe tilsynet er proportionelt med en virksomheds betydning for forsyningssikkerheden. Det foreslås desuden at ministeren kan fastsætte nærmere regler om tilsyn og kontrol af virksomhederne såsom metoder og varigheden, som fremtidssikrer loven, således at et tilpas grundigt tilsyn kan føres hos virksomhederne i energisektoren.

3.7. Håndhævelse og sanktion

3.7.1. Gældende ret

EPCIP-direktivet indeholder ikke bestemmelser om håndhævelse og sanktioner.

EPCIP-direktivet er blevet implementeret i energisektoren ved bekendtgørelse nr. 11 af 7. januar 2011 om identifikation og udpegning af europæisk kritisk infrastruktur på energiområdet og vurdering af behovet for bedre beskyttelse. Efter bekendtgørelsen kan virksomheder i forbindelse med tilsyn pålægges at udarbejde en sikkerhedsplan og ændre i virksomhedens beredskabsplaner.

Desuden kan virksomheder straffes med bøde, hvis de 1) ikke har udpeget en sikkerhedsofficer eller et kontaktpunkt for infrastruktur udpeget efter direktivets regler, ikke behandler materiale, der indeholder særligt følsomme oplysninger om infrastrukturen, fortroligt og opbevarer det sikkert eller undlader at oplyse Energistyrelsen om, at følsomme oplysninger er kompromitteret 2) ikke udarbejder eller reviderer planmateriale 3) afgiver urigtige eller vildledende oplysninger eller efter anmodning undlader at afgive oplysninger 4) ikke overholder pålæg meddelt efter denne bekendtgørelse eller 5) videregiver særligt følsomme oplysninger, til uvedkommende.

Efter NIS 1-direktivets artikel 21 skal medlemsstaterne fastsætte regler om sanktioner, der anvendes i tilfælde af overtrædelser af de nationale regler, der 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.

EPCIP-direktivet og NIS 1-direktivet indeholder ikke nærmere bestemmelser om ansvar for bestemte fysiske personer.

I energisektoren er virksomheders beredskab for forsyningssikkerheden af energi reguleret i delsektorerne el, gas og olie. Reguleringen omfatter både fysisk beredskab og it-beredskab.

På el- og gasområdet, er der beredskabsbestemmelser i forsyningslovene elforsyningsloven §§ 85 c og 85 c og gasforsyningsloven §§ 15 a og 15 b. Beredskabsbestemmelserne bemyndiger klima-, energi- og forsyningsministeren til at fastsætte nærmere regler om beredskab. De nærmere regler er udstedt i bekendtgørelse om beredskab for elsektoren, bekendtgørelsen for beredskab for naturgassektoren og bekendtgørelse om it-beredskab for el- og naturgassektorerne.

Der gælder beredskabskrav virksomheder i elsektoren, som er bevillingspligtige efter §§ 10 og 19 eller har tilladelse til elproduktion fra anlæg med en kapacitet på over 25 MW efter Elforsyningslovens § 11 eller § 29 i lov om fremme af vedvarende energi, Energinet og dennes helejede datterselskaber samt virksomheder, der yder produktionsbalance i elsystemet.

Der gælder beredskabskrav for virksomheder i gassektoren for selskaber, der er bevillingspligtige efter gasforsyningslovens § 10, samt Energinet og Energinets helejede datterselskaber, der varetager gasvirksomhed i medfør af § 2, stk. 2 og 3, i lov om Energinet. Virksomhederne skal foretage nødvendig planlægning og træffe de nødvendige foranstaltninger for at sikre gasforsyningen i beredskabssituationer og andre ekstraordinære situationer. Klima-, energi- og forsyningsministeren kan bestemme, at opstrømsanlæg og bygasnet tilsvarende skal foretage beredskabsplanlægning og træffe beredskabsforanstaltninger.

Efter elforsyningslovens § 85 d og gasforsyningslovens § 47 b, kan det påbydes, at forhold, der strider mod loven eller regler udstedt i medfør af loven, bringes i orden enten straks eller inden for en nærmere angivet frist. Virksomheder, der ikke overholder deres beredskabsforpligtelser, kan derfor gives påbud.

Klima-, energi- og forsyningsministeren kan midlertidigt inddrage en bevilling eller tilladelse, hvis en overtrædelse af bestemmelser, vilkår eller påbud efter elforsyningsloven eller lov om fremme af vedvarende energi eller regler udstedt i medfør af disse love indebærer tilsidesættelse af væsentlige hensyn til elforsyningssikkerheden. Dette gør sig ligeledes gældende, hvis en netvirksomhed gør sig skyldig i grove eller gentagne tilsidesættelse af vilkår stillet af Energinet i medfør af elforsyningslovens § 31, stk. 2, der berører virksomhedens bevillingspligtige aktivitet. Klima-, energi- og forsyningsministeren skal i forbindelse med afgørelsen vejlede den pågældende om prøvelsesadgangen

Klima-, energi- og forsyningsministeren kan inddrage en bevilling som er udstedt i medfør af gasforsyningslovens § 10, hvis virksomheden som har modtaget bevillingen, ikke efterkommer påbud meddelt jf. gasforsyningslovens § 33, stk. 1, nr. 1.

Virksomheder i el- og gassektorerne, som ikke efterlever påbud om manglende overholdelse af it-beredskab, kan påbydes at foretage en it-revision,

jf. bekendtgørelse om it-beredskab for el- og gassektorerne § 32, stk. 2 og § 33, stk. 2.

Efter elforsyningslovens § 88 og gasforsyningslovens § 50, kan der fastsættes regler om bødestraf for regler udsted i medfør af loven.

Virksomheder med beredskabsansvar i el- og gassektorerne kan straffes med bøde hvis virksomhederne, ikke udarbejder eller reviderer planmateriale, ikke fremsender planmateriale til godkendelse, afgiver urigtige eller vildledende oplysninger eller efter anmodning undlader at afgive oplysninger, ikke overholder pålæg meddelt efter denne bekendtgørelse eller videregiver følsomt materiale og oplysninger til uvedkommende, jf. bekendtgørelse om beredskab for elsektorens § 35 og bekendtgørelse om beredskab i naturgassektorens § 35.

Bekendtgørelse om it-beredskab for el- og naturgassektoren indeholder ikke en selvstændig strafbestemmelse.

Virksomheder i elsektoren som ikke efterlever påbud udstedt i medfør af elforsyningslovens § 85 d, straffes med bøde, jf. elforsyningslovens § 87, stk. 1, nr. 7. Virksomheder i gassektoren som ikke efterlever påbud udstedt i medfør af gasforsyningslovens § 47 b, straffes med bøde, jf. gasforsyningslovens § 49, stk. 1, nr. 6.

Efter olieberedskabslovens § 16, stk. 1, skal lagringspligtige olievirksomheder foretage den nødvendig planlægning og foretage de nødvendige foranstaltninger for at sikre forsyningen af råolie og olieprodukter i beredskabssituationer og andre ekstraordinære situationer. Klima- Energi- og Forsyningsministeren kan fastsætte nærmere regler om beredskabsarbejdet for virksomhederne efter olieberedskabslovens § 16, skt. 3.

Ifølge olieberedskabslovens § 18, kan klima- energi- og forsyningsministeren påbyde at forhold, der strider mod loven eller regler udstedt i henhold til loven, skal bringes i orden inden for en nærmere angivet frist. Klima-energi- og forsyningsministeren kan dermed på baggrund af manglende overholdelse af beredskabsregler påbyde lagringspligtige virksomheder, at forholdene skal bringes i orden.

Efter olieberedskabslovens § 23, stk. 1, nr. 5, straffes den, der undlader at efterkomme påbud efter olieberedskabslovens § 18, med bøde. Derudover kan der i regler, som udstedes i henhold til olieberedskabsloven, fastsættes bødestraf for overtrædelse af bestemmelserne i reglerne eller vilkår fastsat

i henhold til reglerne og for manglende overholdelse af påbud meddelt i henhold til reglerne. Der kan i henhold til olieberedskabslovens § 23, stk. 3, pålægges selskaber m.v. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.

Virksomheder med beredskabsansvar kan efter bekendtgørelse om beredskab i oliesektorens § 22, straffes med bøde, hvis virksomhederne 1) undlader at meddele Energistyrelsen om at være afhængige af et forsyningskritisk it-system og en hændelse i dette forsyningskritiske it-system vil få væsentlige forstyrrende virkninger for leveringen af råolie eller olieprodukter i en beredskabssituation eller anden ekstraordinær situation 2) undlader at underrette Energistyrelsen om hændelser, der i væsentlig grad reducerer funktionaliteten. 3) undlader at underrette Energistyrelsen eller Center for Cybersikkerhed om it-sikkerhedshændelser, der påvirker forsyningskritiske it-systemer, hvor underretningen som minimum indeholder en beskrivelse af hændelsen, hændelsens konsekvenser og hvorvidt hændelsen vurderes at have vidtrækkende konsekvenser for andre sektorer. 4) Undlader at udarbejde evalueringer efter hændelser eller at fremsende disse til Energistyrelsen.

Kompetencen til at føre beredskabstilsyn, udstede bøder og inddrage autorisation for virksomheder i el- og olie- gassektorerne er delegeret til Energistyrelsen, jf. bekendtgørelse om Energistyrelsens opgaver og beføjelser § 3, stk. 1, nr. 5 og nr. 6.

3.7.2. Klima-, Energi- og Forsyningsministeriets overvejelser

Med NIS 2-direktivet artikel 44 ophæves NIS 1-direktivet. Med CER-direktivets artikel 27 ophæves EPCIP-direktivet.

Der er i CER-direktivets artikel 21 og NIS 2-direktivets artikel 31-33 fastsat bestemmelser om håndhævelse. Medlemsstaterne forpligtes til at sikre, at deres kompetente myndigheder effektivt kan træffe de nødvendige håndhævelsesforanstaltninger for at bringe virksomhedernes beredskabsmæssige forhold i orden.

NIS 2-direktivet og CER-direktivet oplister de håndhævelsesforanstaltninger, der som minimum skal kunne anvendes over for virksomheder, som ikke opfylder deres beredskabsforpligtelser.

Efter direktiverne skal myndighederne kunne pålægge enhederne at afhjælpe konstaterede mangler eller på en nærmere angivet måde at overholde kravene til deres foranstaltninger til styring af fysisk sikring og cybersikkerhedsrisici eller at efterleve underretningsforpligtelserne.

Efter NIS 2-direktivet skal myndighederne desuden sikre sig ret til at kunne midlertidigt inddrage en autorisation, som fx. kan være en bevilling eller en tilladelse, samt retten til at forbyde enhver fysisk person med ledelsesansvar eller juridisk repræsentant at udøve ledelsesfunktioner.

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

NIS 2-direktivet foreskriver nærmere, hvilke hensyn, der skal indgå i en afgørelse om at træffe 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 den kompetente myndighed, d) hindringer for audits eller overvågningsaktiviteter beordret af den kompetente myndighed efter konstatering af en overtrædelse, e) afgivelse af urigtige eller klart unøjagtige oplysninger vedrørende cybersikkerhedsforanstaltninger eller rapporteringsforpligtelser, der er fastsat i direktivets artikel 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 gerningsmanden har begået overtrædelsen 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, samarbejder med den kompetente myndighed.

De hensyn som er oplistet i NIS 2-direktivet skal iagttages uagtet om der foretages håndhævelsesforanstaltninger på baggrund af bestemmelser der er en videreførelse af gældende ret eller implementering af NIS 2- og CER-direktiverne.

Det vurderes mest hensigtsmæssigt, at afgørelse om håndhævelsesforanstaltninger træffes af den myndighed der fører tilsyn efter loven. Det forventes at disse kompetencer delegeres til Energistyrelsen.

Håndhævelsesforanstaltninger som fratager en virksomhed deres autorisation eller forbyder et medlem af ledelsen at udføre ledelsesopgaver, er meget indgribende foranstaltninger. Foranstaltninger bør derfor ledsages af de fornødne retssikkerhedsmæssige garantier.

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 disse i sidste ende 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 Klima- Energi- og Forsyningsministeriets vurdering, at direktivets undtagelsesbestemmelse ift. administrative bøder finder anvendelse. Direktivets bestemmelser om administrative bøder vil således skulle fortolkes og implementeres 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.

Klima- energi- forsyningsministeren vil skulle påse, at denne lov og regler udstedt i medfør af loven efterleves, herunder undersøge mulige overtrædelser af lovgivningen. I den 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 Klima-Energi- og Forsyningsministeriets 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 anmeldes til politiet.

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

Klima-, Energi- og Forsyningsministeriet vurderer, at der bør kunne udmåles bøder til virksomhederne svarende til de i direktivet fastsatte maksimale bødeniveauer. Klima-, Energi-, og Forsyningsministeriet finder således ikke anledning til at fastsætte højere maksimumniveauer end de i direktivet foreskrevne.

Klima-, Energi- og Forsyningsministeriet lægger i øvrigt vægt på at foretage en implementering der i overensstemmelse med NIS 2- og CER-direktiverne fastsætter bestemmelser om sanktioner, som sikrer at disse er effektive, forholdsmæssige og har afskrækkende virkning.

3.7.2.1 Særligt om tvangsbøder

Det følger af NIS 2-direktivet, 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 udskrive tvangsbøder for at få nogen, herunder i givet fald virksomhederne som foreslås omfattet, til at opfylde en forpligtelse mod det offentlige, herunder de kompetente myndigheder.

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 – fx. 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, 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.

Klima-, Energi- og Forsyningsministeriet er på baggrund af ovenstående 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.

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

3.7.2.2 Særligt om fysiske personers strafansvar, herunder valg af ansvarssubjekt

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

Det følger dog af NIS 2-direktivets artikel 32, stk. 6, 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 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.

Det er i direktivets præambelbetragtning 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.

Det følger af Rigsadvokatmeddelelse CIR1H nr. 11550 af 17. april 2015 om strafansvar for juridiske personer, at udgangspunktet ved valg af ansvarssubjekt i særlovgivningen er, at tiltalen rejses mod den juridiske person.

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

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

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

Klima-, Energi- og Forsyningsministeriet 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 Klima-, Energi- og Forsyningsministeriet vurdering, 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 om mere end det, der allerede i dag følger af de almindelige 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.

3.7.2.3 Særligt om brud på persondatasikkerheden

NIS 2-direktivets artikel 35, stk. 2, 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 underretningsforpligtelser), der (også) kan medføre et brud på persondatasikkerheden i medfør af databeskyttelsesforordningen. I givet fald skal de kompetente myndigheder uden unødigt ophold underrette de relevante tilsynsmyndigheder, i dansk ret Datatilsynet, og der kan ikke straffes med (administrativ) bøde i medfør af NIS 2-direktivet, såfremt den samme adfærd straffes med (administrativ) bøde efter databeskyttelsesforordningen.

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

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

3.7.3. Den foreslåede ordning

Det forslås, at klima-, energi- og forsyningsministeren kan pålægge at forhold der ikke lever op til lovens krav bringes i orden. Påbud kan ske på baggrund af tilsyn eller, hvis ministeren på anden måde bliver bekendt med, at pligterne efter loven ikke efterleves. Ministeren kan blive bekendt med beredskabsforhold gennem anden kommunikation med den pågældende virksomhed, kommunikation om den pågældende virksomheder eller tilsyn, som føres efter anden regulering m.v.

Der kan være tilfælde, hvor Energistyrelsen ved tilsyn bliver opmærksom på væsentlige afvigelser i virksomhedernes risikostyring og sikkerhedsforanstaltninger. Dette kan bl.a. være i tilfælde af, at virksomheden ikke retter op på forhold, der har givet anledning til væsentlige påbud, eller hvor det vurderes, at en virksomheds risikovurderinger vedrørende risici for forsyningen er mangelfulde. Det foreslås derfor, at Energistyrelsen i særlige tilfælde kan pålægge virksomheden ekstern beredskabsrevision. I sådanne tilfælde foreslås det desuden, at Energistyrelsen er ansvarlig for at beskrive rammerne for revisionen samt vælge hvilke revisorselskaber, der kan benyttes.

Det foreslås, at den særlige ordning om at forbyde en fysisk person af ledelsen at udøve ledelsesfunktioner og midlertidig suspension af autorisation, som udgangspunkt bliver anvendt i de tilfælde, hvor allerede pålagte håndhævelsesforanstaltninger er utilstrækkelige. Efter den foreslåede ordning, fastsættes der en frist, inden for hvilken manglerne afhjælpes eller myndighedernes krav efterleves. Efter forslaget bliver udgangspunktet,

hvis de nødvendige tiltag ikke er foretaget inden for den fastsatte frist, at ministeren kan træffe afgørelse om:

1) Midlertidigt at suspendere en myndighedsudstedt 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 direktionsniveau eller juridisk repræsentant i enheden at udøve ledelsesfunktioner i den pågældende enhed.

Det vil i udgangspunktet være en forudsætning, at ordningen først anvendes, når det kan konstateres at mindre indgribende midler har vist sig utilstrækkelige.

Der foreslås endvidere, at muligheden for at anvende ordningen om suspension og forbud i helt særlige tilfælde kan anvendes uden forudgående påbud. Det skal være muligt i tilfælde, hvor ledelsen bevidst eller ved grov uagtsomhed har forsømt deres beredskabsmæssige forpligtelser i en sådan grad, at der er en overhængende fare for at virksomheden ved en væsentlig hændelse ikke ville kunne genoprette sine virksomhedsaktiviteter. Samme mulighed skal være til stede i de tilfælde, hvor ledelsen har nedprioriteret beredskabsniveauet i en sådan grad, at det kan have nationale forsyningsmæssige konsekvenser.

Det foreslås, at sådanne midlertidige suspensioner eller midlertidige forbud mod, at fysiske personer må udøve ledelsesfunktioner, kun kan anvendes, indtil virksomheden træffer de nødvendige foranstaltninger til at afhjælpe de mangler eller opfylde de krav, som gav anledning til, at foranstaltningerne blev anvendt.

Det foreslås at håndhævelsesforanstaltninger der fratager en virksomhed deres autorisation eller forbyder et medlem af ledelsen at udføre ledelsesopgaver, kan forlanges indbragt for domstolene. Desuden foreslås det, at domstolene kan bestemme at sagsanlæg har opsættende virkning.

Det foreslås, at der som led i implementeringen af CER og NIS 2-direktiverne indsættes sanktionsbestemmelser i loven med det formål, at alle materielle og processuelle krav i loven eller regler udstedt i medfør af loven, som ikke bliver overholdt kan medføre bødestraf.

Det foreslås således, at den, der 1) overtræder §§ 6-10, § 11, stk. 2, §§ 12 og 13, 2) undlader at efterkomme en afgørelse efter § § 23, stk. 1, nr. 1 eller 2, 3) undlader at efterkomme påbud efter § 21 og § 22, 4) undlader at efterkomme krav efter § 14, stk. 2 eller § 19, stk. 2, nr. 5-7, 5) hindrer myndighederne i at føre kontrol efter bestemmelserne i 19, stk. 2, nr. 1-4, 6) meddeler klima-, energi- og forsyningsministeren eller Energiklagenævnet urigtige eller vildledende oplysninger eller efter anmodning undlader at afgive oplysninger, kan 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, at bøder vil kunne pålægges fysiske personer og selskaber m.v. (juridiske personer), i det omfang de omfattes af lovens anvendelsesområde eller de allerede gældende bestemmelser i straffeloven.

NIS 2-direktivet indeholder ikke særlige forudsætninger for så vidt angår bødeniveauet for manglende efterlevelse af forpligtelser i direktivet ud over artikel 21 (foranstaltninger til styring af cybersikkerhedsrisici) og artikel 23 (rapporteringsforpligtelser). Der stilles ikke særlige krav til bødestørrelse efter CER-direktivet, men det foreslås at der i lovforslaget stilles bødekrav svarende til dem i NIS 2-direktivet til bestemmelserne som implementerer artikel 13 (kritiske enheder modstandsdygtighedsforanstaltninger) og artikel 15 (underretning om hændelser).

Det forudsættes i overensstemmelse med NIS 2-direktivets artikel 34, stk. 4 og 5, at bødens størrelse for så vidt angår overtrædelse af bestemmelserne i §§ 6-10, § 11, stk. 2, §§ 12 og 13, § 14, stk. 2, § 19, stk. 2, nr. 1-7, §§ 21, 22 og § 23, stk. 1, nr. 1 eller 2 samt reglerne udstedt i medfør af §§ 6-10, § 11, stk. 2, §§ 12 og 13, § 14, stk. 2, § 19, stk. 2, nr. 1-7, §§ 21 og 22 og § 23, stk. 1, nr. 1 eller 2 maksimalt vil udgøre et beløb svarende til 10.000.000 euro eller 2 pct. af virksomhedens samlede globale årsomsætning i det foregående regnskabsår, alt efter, hvad der er højest.

Der forudsættes i overensstemmelses med CER-direktivets artikel 22, at sanktionerne skal være effektive, stå i et rimeligt forhold til overtrædelsen og have afskrækkende virkning. Da fysisk sikkerhed og cybersikkerhed er tæt forbundet foreslås det at bødestørrelsen for overtrædelsen af bestemmelserne i §§ 6-10, § 11, stk. 2, §§ 12 og 13, § 14, stk. 2, § 19, stk. 2, nr. 1-7, §§ 21, 22 og § 23, stk. 1, nr. 1 eller 2 samt reglerne udstedt i medfør af §§ 6-10, § 11, stk. 2, §§ 12 og 13, § 14, stk. 2, § 19, stk. 2, nr. 1-7, §§ 21

og 22 og § 23, stk. 1, nr. 1 eller 2 skal følge samme bødestørrelse som den der er angivet efter NIS 2-direktivets artikel 34, stk. 4 og 5.

Der foreslås ikke i tilknytning til øvrige bestemmelser end de specifikt angivne ovenfor anlagt særlige forudsætninger for så vidt angår udmålingen af bødernes størrelse. Det samme gælder eventuel udmåling af bøder til fysiske personer, hvor det dog forudsættes, at der tages behørigt hensyn til direktivets forudsætninger om at lægge vægt på det generelle indkomstniveau og personens økonomiske stilling.

Bøderne vil kunne pålægges i tillæg til håndhævelsesforanstaltningerne i de foreslåede §§ 21-23.

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 i afsnit 3.7.2. beskrevne hensyn.

Det foreslås endvidere, i overensstemmelse med NIS 2-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.

3.8 Nødvendige omkostninger til beredskab efter lov om varmeforsyning

3.8.1. Gældende ret

Udgangspunktet for prisreguleringen følger af § 20, stk. 1, i lov om varmeforsyning. Prisreguleringen indebærer, at varmepriserne reguleres efter princippet om nødvendige omkostninger – også kaldet den omkostningsbestemte varmepris. Varmeforsyningsvirksomhederne kan alene indregne nødvendige omkostninger i varmeprisen. Derudover må prisen ikke være urimelig, jf. § 21, stk. 4, i lov om varmeforsyning.

Bestemmelsen i § 20, stk. 1, i varmeforsyningsloven, indeholder en ikke udtømmende opregning af de virksomheder, der er omfattet af prisbestemmelserne. Afgørende for at være omfattet er, at virksomheden leverer opvarmet vand, damp eller gas bortset fra naturgas til det indenlandske marked med det formål at levere energi til bygningers opvarmning og forsyning med varmt vand, dvs. til rumvarmeformål. Bestemmelsen finder tilsvarende anvendelse på levering af opvarmet vand til andre formål fra centrale kraftvarmeanlæg.

De omkostninger, der må indregnes i priserne, skal ud over at være nødvendige, også efter deres art være indregningsberettigede. Det drejer sig bl.a. om omkostninger som følge af pålagte offentlige forpligtelser, herunder omkostninger til energispareaktiviteter efter §§ 28 a, 28 b og 29.

Omkostninger til energispareaktiviteter efter §§ 28 a, 28 b og 29 er nærmere reguleret i kapitel 7 i lov om varmeforsyning om offentlige forpligtelser for varmeforsyningsanlæg. Ud over de disse bestemmelser er beredskab til bygas også reguleret, jf. § 29 a.

Virksomheder, som driver anlæg til produktion og fremføring af bygas, skal foretage nødvendig planlægning og træffe de nødvendige foranstaltninger for at sikre bygasforsyningen i beredskabssituationer og andre ekstraordinære situationer, jf. § 29 a, stk. 1, i lov om varmeforsyning. Klima-, energi- og forsyningsministeren kan fastsætte regler om varetagelse af de i stk. 1 nævnte opgaver samt om varetagelse af de overordnede, koordinerende planlægningsmæssige og operative opgaver vedrørende beredskabet, jf. § 29 a, stk. 2, i lov om varmeforsyning.

Bestemmelsen omfatter alene bygas. Anden energi er således ikke omfattet.

Det fremgår af de specielle bemærkninger til bestemmelsen i stk. 1, at det ikke blev fundet nødvendigt at etablere et beredskab for andre dele af varmeforsyningen, da brændstofforsyninger til varme- eller kraftvarmeværker påregnedes dækket af dels beredskabslagrene på olieområdet, dels beredskabet for naturgas. Derudover ville varmeproduktion og -distribution blive dækket af det almindelig driftsberedskab. Dertil kom, at varmeforsyning ikke blev anset for at være af afgørende betydning for opretholdelse af samfundets funktioner i en krisesituation.

Bygas blev foreslået omfattet af bestemmelserne, da bygas i vidt omfang er sidestillet med naturgas, og da bygas- og naturgasselskaberne gennem længere tid havde samarbejdet om beredskabsforhold.

Det fremgår af de specielle bemærkninger til bestemmelsen i stk. 2, at bestemmelsen endvidere skulle give hjemmel til at fastsætte regler for varetagelse af de overordnede, koordinerende planlægningsmæssige og operative opgaver vedrørende beredskabet; som hidtil varetaget i samarbejde med virksomheder inden for naturgassektoren. Bemyndigelsen er på nuværende tidspunkt ikke udnyttet.

Udover, at en omkostning skal være nødvendig, må den samlede pris ikke være urimelig, jf. § 21, stk. 4, i lov om varmeforsyning. Det er Forsyningstilsynet, der i konkrete sager afgør, hvilke udgifter og omkostninger, der må anses for nødvendige, og som derfor kan indregnes i priserne.

Finder Forsyningstilsynet, at tariffer (priser), omkostningsfordeling på anlæg med forenet produktion eller andre betingelser er urimelige eller i strid med nærmere fastlagte retsregler eller regler udstedt i henhold til loven, giver tilsynet, såfremt forholdet ikke gennem forhandling kan bringes til ophør, pålæg om ændring af tariffer, omkostningsfordeling på anlæg med forenet produktion eller betingelser, jf. § 21, stk. 4.

Det følger af Forsyningstilsynets praksis, at den samlede varmepris ikke må overstige den i administrativ praksis udviklede substitutionspris. Substitutionsprisprincippet er udviklet i den administrativ praksis. Substitutionsprisprincippet er derfor ikke fastsat ved lov. Substitutionsprisprincippet indebærer, at der for køb af varme ikke må indregnes en højere pris end den pris, som varmekøber selv ville kunne producere den omfattede varmemængde for eller købe den for fra tredjemand. Princippet kan efter praksis få virkning i alle led i værdikæden, dvs. for alle leverancer omfattet af § 20, stk. 1, i lov om varmeforsyning. I praksis fungerer substitutionsprisen således som et lokalt prisloft for varmeforsyningsvirksomhedernes køb af opvarmet vand m.v. En varmeforsyningsvirksomheds substitutionspris er dynamisk og kan ændre sig fra år til år. Det er Forsyningstilsynet, der af egen drift eller på baggrund af en henvendelse eller en klage, kan vurdere, om substitutionsprisprincippet finder anvendelse i et konkret leveringsforhold, herunder fastsætte substitutionsprisen. Princippet har dog ikke virkning for den del af værdikæden, der er mellem varmedistributionsvirksomhed og slutkunde.

De virksomheder, der er omfattet af prisreguleringen i lov om varmeforsyning, er derudover omfattet af en anmeldelsespligt af visse oplysninger til Forsyningstilsynet efter § 21, stk. 1, i lov om varmeforsyning. Anmeldelsespligten indebærer, at bl.a. priser for ydelser omfattet af § 20 i lov om varmeforsyning, skal anmeldes til Forsyningstilsynet med angivelse af grundlaget herfor efter nærmere regler fastsat af tilsynet. Forsyningstilsynet kan fastsætte regler om formen for anmeldelse og om, at anmeldelse skal foretages elektronisk. Forsyningstilsynet kan fastsætte regler om, at anmeldelse skal ledsages af en erklæring afgivet af en registreret revisor, statsautoriseret revisor eller kommunens revisor. Forsyningstilsynet kan give pålæg om anmeldelse. Anmeldelse er en gyldighedsbetingelse, jf. §

21, stk. 3, i lov om varmeforsyning, men indebærer ikke en godkendelse af det anmeldte fra Forsyningstilsynet.

3.8.2. Klima-, Energi- og Forsyningsministeriets overvejelser

Lovforslaget skal styrke energisektorens beredskabsniveau med henblik på at forebygge og modstå hændelser, som truer energiforsyningen. Der i dag et højt og markant trusselsniveau mod energisektoren i forhold til især cyberangreb og spionage, og lovforslaget skal sikre, at der er et tidsvarende, ambitiøst og robust beredskab i energisektoren. Der henvises til de almindelige bemærkninger i afsnittene 2 og 3.1.2 og 3.1.2. samt 3.2.2. og 3.2.3.

Fjernvarme er ikke i dag omfattet af beredskabsregulering, selvom denne delsektor har en væsentlig og stigende betydning for den danske energiforsyning.

Energisektorens beredskabsregulering har til formål at sikre, at sektoren er forberedt til at kunne opretholde og videreføre energiforsyningen i tilfælde af naturskabte, menneskeskabte og teknologiske risici.

Lovforslaget vil samle de beredskabsbestemmelser, der er i de respektive forsyningslove, herunder i lov om varmeforsyning, og placere dem i en samlet lov om beredskab for energisektoren.

3.8.3. Den foreslåede ordning

Det foreslås at ophæve bestemmelsen i § 29 a, i lov om varmeforsyning om beredskab for virksomheder, som driver anlæg til produktion og fremføring af bygas.

Med lovforslaget vil det endvidere skulle sikres, at varmeforsyningsvirksomhederne vil kunne indregne de nødvendige omkostninger, der er forbundet med det tilstrækkelige/nødvendige beredskab.

Det foreslås derfor videre at indføre i § 20, stk. 1, 1. pkt., at varmeforsyningsvirksomheder vil kunne til omkostninger til beredskab efter lov om styrket beredskab i energisektoren. Den foreslåede ændring, jf. lovforslagets § X, nr. 1, vil medføre, at varmeforsyningsvirksomheder omfattet af § 20, stk. 1, vil kunne indregne nødvendige omkostninger til beredskab efter lov om styrket beredskab i energisektoren. Forsyningstilsynet vil [fortsat] kunne vurdere, om en omkostning til beredskab er nødvendig, ligesom Forsyningstilsynets almindelige indgrebsbeføjelser vil finde anvendelse, jf. § 21, stk. 4, i lov om varmeforsyning,

4. Økonomiske konsekvenser og implementeringskonsekvenser for det offentlige

Lovforslaget vurderes at have økonomiske konsekvenser for staten, herunder implementeringskonsekvenser for statslige myndigheder.

De statsfinansielle meromkostninger forventes at være 3,0-4,0 mio. kr. årligt. Meromkostningerne kan henføres til opgaver, der følger af den nye regulering, herunder generel vejledning om lovgivningen eller koordinering med EU.

Ud over de statsfinansielle konsekvenser, skønnes det, at der vil være meromkostninger på 8,2 mio. kr., der forventes gebyrfinansieret.

Estimaterne dækker både monopolvirksomheder og konkurrenceudsatte virksomheder. Gebyret opkræves til at dække bl.a. sagsbehandling vedr. samordnet beredskab, dispensationer, administration ved gebyropkrævning, udarbejdelse af risiko- og sårbarhedsscenarier, forhåndstilsagn om klassificering af anlæg og sagsbehandling af risikovurderinger af projekter. Derudover indgår omkostninger ifm. afholdelse af tilsyn.

De forventede statslige meromkostninger skyldes bl.a., at lovforslaget udvider beredskabskravene og tilsynsforpligtelsen til at gælde nye sektorer. I dag omfatter tilsynsforpligtelsen store dele af el-, gas- og oliesektoren. Fremadrettet skal beredskabskravene, herunder tilsyn hermed ligeledes omfatte fjernvarme-, fjernkøling- og brintsektorerne. Samtidig udvides kredsen af virksomheder i gas-, el- og oliesektorerne, der omfattes af beredskabskrave efter direktiverne. Dermed udvides Energistyrelsens vejlednings- og tilsynsforpligtelse til at gælde nye sektorer.

Som følge af den udvidede kreds af omfattede virksomheder øges behovet for at kunne administrere dokumentationsmateriale ifm. tilsyn og anden kommunikation med virksomhederne. Der forventes derfor behov for at opdatere eksisterende onlineportal, som i dag benyttes. Der er bl.a. behov for at øge kapaciteten (dvs. storage) samt sikkerhedshærdning af portalen. Det forventes, at udgifterne hertil vil være meget begrænsede, idet onlineportalen allerede eksisterer, og der kun er tale om en opdatering.

Fsva. efterlevelse af krav i NIS2 og CER om indberetning af sikkerhedshændelser forventes fælles statslig løsning anvendt, hvilket følger princip nr. 6 anvendelse af offentlig infrastruktur fra principperne for digitaliseringsklar lovgivning. Der forventes således ikke behov for at udvikle egen digital løsning for hændelsesindberetning for energisektoren.

De syv principper for digitaliseringsklar lovgivning er iagttaget. Foruden ovenstående henvisning gælder det særligt ift. princip nr. 1 vedrørende *enkle og klare regler*, da loven samler hjemmelsbestemmelser og krav fra andre love i én lov, nr. 2 *digital kommunikation*, da loven indeholder regler, som understøtter digital kommunikation med borgere og virksomheder. Loven sikrer også, at fremtidige digitale platforme kan anvendes, da hjemlen til digital kommunikation er formuleret teknologineutralt. Derudover er der også fokus på princip nr. 5 om *tryg og sikker datahåndtering*, da loven understøtter digital kommunikation på en måde, hvorpå sikkerhed prioriteres hørt.

De øvrige principper for digitaliseringsklar lovgivning vurderes ikke relevante.

Lovforslaget vurderes at kunne have økonomiske konsekvenser for Klima-, Energi- og Forsyningsministeriet, som følge af forventet øget myndighedsbehandling i navnlig Energistyrelsen. Herudover kan Energiklagenævnet opleve flere klagesager.

Energiklagenævnet er i dag generel klageinstans for afgørelser truffet efter elforsyningsloven, gasforsyningsloven og olieberedskabsloven herunder i forhold til beredskab. Energiklagenævnets rolle som klageinstans foreslås overført til den nye lov om styrket beredskab i energisektoren. Lovforslagets udvidelse af omfattede virksomheder kan medføre en øget mængde klager over Energistyrelsens afgørelser efter loven eller regler fastsat i medfør af loven. For nuværende vurderes omkostningerne at være små, da der ikke forventes mange klagesager på baggrund af lovforslagets klageadgang. Vurderingen er foretages på baggrund af, at der ikke tidligere er indgivet klager til Energiklagenævnet på baggrund af Elforsyningslovens § 85 b og 85 c, Gasforsyningslovens § 15 a og 15 b eller olieberedskabsloven. Vurderingen er dog undergivet en vis usikkerhed, da lovforslaget vil omfatte nye typer af virksomheder og nye sektorer.

Da omkostninger til Energiklagenævnet ikke efter vanlig praksis gebyrfinansieres, foreslås det, at de potentielle meromkostninger, der vil følge af

nærværende lovforslag vil blive afregnet mellem Energistyrelsen og Nævnenes Hus kvartalsvis på medgåede timer. Finansieringen af potentielle meromkostninger til Energiklagenævnet tages op til revision, når markedet er modnet, og der er kommet indikationer på antallet af klagesager.

Lovforslaget forventes herudover ikke at medføre nogle implementeringskonsekvenser for det offentlige.

5. Økonomiske og administrative konsekvenser for erhvervslivet m.v.

Lovforslaget vurderes at have erhvervsøkonomiske konsekvenser, herunder både omstillingsomkostninger og løbende omkostninger samt administrative konsekvenser for erhvervslivet.

De forventede erhvervsøkonomiske konsekvenser vil i samarbejde med Erhvervsstyrelsens Område for Bedre Regulering (OBR) blive kvantificeret yderligere i forbindelse med høringen af bekendtgørelsen, der skal udmønte kravene i lov om styrket beredskab.

Lovforslaget vil indebære enkelte krav, som vil medføre administrative konsekvenser i form af omkostninger for erhvervslivet. Det forventes dog, at de økonomiske og administrative konsekvenser ved lovforslaget vil være under 4 mio. kr. De administrative konsekvenser består i, at myndighederne efter § 14, stk. 2 kan kræve, at virksomheder foretager en offentliggørelse af en hændelse. Dette kan fx indebære udarbejdelse og udsendelse af en pressemeddelelse. Hyppigheden forventes at være lav på samfundsniveau, da de fleste virksomheder formentligt selv vil offentliggøre hændelsen, hvis det er nødvendigt og under hensyntagen til hændelsens karakter og omfang. Desuden kan der være administrative konsekvenser efter § 21, hvor rådgivende missioner kan føre tilsyn med virksomheder, som er udpeget som enheder af særlig europæisk betydning. Da der sandsynligvis vil være få enheder af særlig europæisk betydning, vurderes de administrative konsekvenser at være begrænsede.

Med lovforslaget skønnes omkring 100-110 private virksomheder i energisektoren omfattet inden for el-, gas-, olie- og brintsektorerne. Derudover skønnes yderligere omkring 70-80 monopolvirksomheder omfattet inden for bl.a. eldistribution og fjernvarmesektoren. Monopolvirksomhederne er

iht. Erhvervsstyrelsens vejledning ikke medtaget i de erhvervsøkonomiske konsekvensberegninger.

De samlede omstillingsomkostninger for private virksomheder skønnes med betydelig usikkerhed at udgøre ca. 650 mio. kr. Såfremt tallene korrigeres for at mange virksomheder i forvejen forventes at afholde de udgifter, som reguleringen medfører (dvs. business-as-usual), skønnes omstillingsomkostningerne med betydelig usikkerhed at være ca. 250 mio. kr. Omstillingsomkostningerne skyldes primært, at virksomhederne som følge af de nye krav vil skulle foretage en række engangsinvesteringer vedr. forbedring af fysisk sikkerhed og cybersikkerhedstiltag.

De direkte løbende efterlevelsesomkostninger skønnes med betydelig usikkerhed i alt at udgøre ca. 100 mio. kr. årligt. Tages der højde for business-as-usual skønnes de løbende omkostninger med betydelig usikkerhed til at være ca. 30 mio. kr. Disse omkostninger kan henføres til bl.a. netværkssegmentering, fysisk sikring af anlæg og kritiske lokaler, omkostninger forbundet med leverandørstyring, logning og uddannelse af medarbejdere.

Både de løbende og omstillingsmeromkostningerne for virksomheder, som i dag er beredskabsreguleret, forventes at være relativt lavere end for nyregulerede virksomheder, da de allerede har beredskabspersonel ansat, og da direktiverne på flere områder overlapper med eksisterende krav. Den nuværende regulering sætter fx allerede krav til fysisk sikring af de mest forsyningskritiske anlæg, og derfor er det forventningen, at udgifterne for ikke-nyregulerede virksomheder vil være lavere. Desuden forventes omkostningerne at være størst for de virksomheder, der er mest kritiske for opretholdelse af forsyningen, da det vil være forbundet med større opgaver for disse virksomheder at efterleve kravene, da de fx har flere anlæg og større netværk. De administrative omstillingsomkostninger for erhvervslivet skønnes med betydelig usikkerhed at være ca. 25 mio. kr. Tages der højde for business-as-usual, skønnes de administrative omstillingsomkostninger til at være ca. 15 mio. kr.

De løbende administrative omkostninger skønnes med betydelig usikkerhed at være ca. 65 mio. kr. Tages højde for business-as-usual skønnes de at være ca. 30 mio. kr.

Omkostningerne kan henføres til bl.a. virksomheders udarbejdelse af beredskabsplaner, risiko- og sårbarhedsanalyser, risikovurderinger ifm. leverandørforhold og projekter og forberedelse og deltagelse i Energistyrelsens

beredskabstilsyn. Den administrative omstillingsomkostning forventes især at påhvile de virksomheder, der ikke er omfattet af beredskabsregulering i dag.

Det vurderes, at Innovations- og Iværksættertjekket ikke er relevant for lovforslaget, fordi forslaget ikke påvirker virksomheders eller iværksætteres muligheder for at teste, udvikle og anvende nye teknologier og innovation.

Det forventes desuden, at reguleringen er relevant for punkt 3, idet den vil fremme brugen af security-by-design. Dette skyldes bl.a., at det er hensigten at sikkerhedsfremmende teknologier eller metoder tænkes ind i projekt- eller anlægsfasen ifm. fx IT- eller anlægsprojekter, der har betydning for energiforsyningssikkerheden. Derudover stiller reguleringen krav om, at virksomheder skal sikre, at sikkerhed er integreret i udviklingsdesignet fra begyndelsen, samt at energivirksomhederne integrerer komponenter og systemer i net- og informationssystemer på en måde, der understøtter sikkerheden for leveringen af tjenesten. Dermed imødekommer reguleringen de sårbarheder, som digitaliseringen af energisektoren introducerer.

6. Administrative konsekvenser for borgerne

Det vurderes, at lovforslaget ikke har administrative konsekvenser for borgerne.

7. Klimamæssige konsekvenser

Lovforslagets formål er at styrke det eksisterende beredskab i energisektoren, herunder øge modstandsdygtigheden over for fysiske angreb og cybertrusler.

Lovforslaget forventes ikke at have klimamæssige konsekvenser. Lovforslaget kan dog have en klimaeffekt i det omfang, at tiltaget gør det relativt dyrere at producere el på fossile brændsler. Omvendt kan der være øgede udledninger, hvis forslaget gør det relativt dyrere at producere fx el på baggrund af VE-energikilder.

8. Miljø- og naturmæssige konsekvenser

Lovforslaget vurderes ikke at have nogen miljø- og naturmæssige konsekvenser.

9. Forholdet til EU-retten

Forslaget implementerer EU-regler i form 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)

- 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.

10. Forholdet til databeskyttelsesforordningen og databeskyttelsesloven

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).

Almindelige personoplysninger omfatter fx. væsentlige sociale oplysninger, andre private forhold, økonomi, skat, gæld, sygedage, tjenstlige forhold, familieforhold, bolig, bil, eksamen, ansøgning, CV, ansættelsesdato, stilling, arbejdsområde, arbejdstelefon, navn, adresse, fødselsdato m.v.

Følsomme personoplysninger omfatter fx. oplysninger om race og etnisk oprindelse, politisk overbevisning, religiøs og filosofisk overbevisning, fagforeningsmæssige tilhørsforhold, genetiske data, biometriske med henblik på entydig identifikation, helbredsoplysninger og seksuelle forhold eller seksuel orientering.

Efter databeskyttelsesforordningens artikel 10 gælder, at behandling af personoplysninger vedrørende straffedomme og lovovertrædelser eller tilknyttede sikkerhedsforanstaltninger på grundlag af forordningens artikel 6, stk.

1, kun må foretages under kontrol af en offentlig myndighed, eller hvis behandling har hjemmel i EU-retten eller medlemsstaternes nationale ret, som giver passende garantier for registreredes rettigheder og frihedsrettigheder.

Der anlægges en vid fortolkning af begrebet strafbare forhold. Ikke alene oplysninger om lovovertrædelser som har eller kan udløse strafansvar, men også andre sanktioner som fx. rettighedsfrakendelse er omfattet af begrebet. Det er imidlertid ikke alle oplysninger om et muligt strafbart forhold, herunder politianmeldelse, der er omfattet. Hertil kræves, at anmeldelsen i en eller anden form kan anses for underbygget.

Med lovforslaget gennemføres hhv. NIS 2-direktivet og CER-direktivet inden for klima-, energi og forsyningsministerens ressort.

Lovforslaget indebærer en række forpligtelser for omfattede virksomheder samt myndighedsopgaver for Energistyrelsen og enkelte andre myndigheder, der i et vist omfang vil indebære behandling af personoplysninger.

Der vil således kunne indgå almindelige personoplysninger som nævnt ovenfor i de oplysninger, som virksomheder efter lovforslaget skal indgive til Energistyrelsen i medfør af lovforslagets §§ 5 og 6, hvorefter Energistyrelsen kan kræve, at virksomheder fremlægger oplysninger og materiale, der er nødvendig for stillingtagen til, hvordan en virksomhed, dens anlæg og systemer skal kategoriseres samt om virksomheden ska udpeges som en enhed af særlig europæisk betydning.

Der kan videre indgå almindelige personoplysninger i de oplysninger, som virksomheder efter lovforslaget i medfør af lovforslagets § 6, stk. 2, nr. 3, skal indmelde om en udpeget kontaktperson til Energistyrelsen.

Derudover kan der indgå almindelige personoplysninger i en kritisk enheds underretning om hændelser efter lovforslagets §§ 13 og 14, hvorefter virksomheder skal underrette Energistyrelsen og andre myndighed om hændelser, der i betydelig grad forstyrrer eller har potentiale til at forstyrre leveringen af virksomhedens væsentlige tjenester. Af forarbejderne til §§ 13 og 14, fremgår, at underretninger skal indeholde alle tilgængelige oplysninger, der er nødvendige for, at Energistyrelsen og andre myndigheder kan forstå hændelsens art, årsag og mulige konsekvenser, herunder alle tilgængelige oplysninger der er nødvendige for at fastslå hændelsens eventuelle grænseoverskridende indvirkning. I en virksomheds underretning om en hændelse kan der således fx. indgå almindelige personoplysninger i forbindelse med en redegørelse for hændelsens faktiske forløb, eller ved at

der vedlægges e-mails eller andet materiale, der belyser hændelsens forløb, karakter eller håndtering.

Efter lovforslagets §§ 16 og 17 skal virksomheder have sikkerhedsgodkendt visse medarbejdere og andre medarbejdere skal opnå godkendt baggrundskontrol i overensstemmelse med nærmere regler fastsat efter forhandling med justitsministeren, der; 1) varetager følsomme funktioner i eller til fordel for en kritisk enhed, navnlig vedrørende den kritiske enheds modstandsdygtighed, 2) er bemyndiget til at få direkte adgang eller fjernadgang til en kritisk enheds lokaler, oplysninger eller kontrolsystemer, herunder i forbindelse med den kritiske enheds sikkerhed eller 3) overvejes ansat i stillinger, der indebærer opgavevaretagelse som nævnt ovenfor. Gennemførelse af sikkerhedsgodkendelse og baggrundskontrol sker således på baggrund af en anmodning fra en virksomhed og forudsætter at vedkommende virksomhed og dennes medarbejder eller potentielle medarbejder har meddelt samtykke dertil. Gennemførelse af baggrundskontrol og sikkerhedsgodkendelse vurderes at kunne medføre behandling af almindelige personoplysninger.

Der kan endvidere i forbindelse med anvendelsen af tilsyns- og håndhævelsesforanstaltninger i medfør af de foreslåede bestemmelser i §§ 21-27 blive behandlet almindelige personoplysninger. Det er Klima-, Energi- og Forsyningsministeriets vurdering, såvel som Forsvarsministeriets i forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau, at de oplysninger, der måtte blive behandlet i denne forbindelse, vil udgøre oplysninger om virksomhedens medarbejdere. Disse oplysninger vil primært udgøre kontaktoplysninger på virksomhedens 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 Klima-, Energi- og Forsyningsministeriets vurdering, såvel som Forsvarsministeriets i lovforslag [NIS 2] at behandling af almindelige personoplysninger i forbindelse med overholdelsen af underretningsforpligtelserne i §§ 13 og 14, 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 Klima-, Energi- og Forsyningsministeriets vurdering, såvel som Forsvarsministeriets i lovforslag [NIS 2], 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, jf. 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 den situation, hvor Energistyrelsen som kompetent myndighed efter NIS 2- og CER-direktiverne, videregiver oplysninger til Center for Cybersikkerhed som CSIRT og Beredskabsstyrelsen som national kontaktpunkt efter CER-direktivet, EU-Kommissionen eller dennes særlige rådgivningsmissioner efter § 6 om enheder af særlig europæisk betydning og lignende, 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 Energistyrelsens opgave som kompetent myndighed for energisektoren og Center for Cybersikkerheds opgave som CSIRT og centralt kontaktpunkt samt Beredskabsstyrelsen opgave som national kontaktpunkt, vurderer Klima-, Energi- og Forsyningsministeriet, såvel som Forsvarsministeriets i lovforslag [NIS 2], at videregivelse af almindelige personoplysninger til fx. Center for Cybersikkerhed er omfattet af forordningens artikel 6, stk. 1, litra e.

Det vurderes på den baggrund, at virksomheder samt andre kompetente myndigheder, Beredskabsstyrelsen og Center for Cybersikkerhed med hjemmel i databeskyttelsesforordningens artikel 6 kan videregive almindelige personoplysninger til Energistyrelsen og omvendt.

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. Klima-, Energi- og Forsyningsministeriet har ved vurderingen lagt vægt på, at Energistyrelsen som kompetent myndighed bl.a. vil få til opgave at analysere cybertrusler, sårbarheder og hændelser på nationalt plan, samt at reagere på hændelser.

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. Klima-, Energi- og Forsyningsministeriet 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 Energistyrelsen og andre myndigheders udførelse af opgaverne som hhv. kompetentmyndighed, CSIRT og centralt kontaktpunkt efter NIS 2- og CER-direktiverne.

Det er Klima-, Energi- og Forsyningsministeriets, såvel som Forsvarsministeriets vurdering, at for så vidt angår behandling af eventuelle oplysninger om strafbare forhold, jf. den foreslåede § 16 om sikkerhedsgodkendelse og baggrundskontrol, vil dette alene kunne ske på grundlag af samtykke fra den person, der er genstand for kontrollen, jf. databeskyttelsesforordningens artikel 6, stk. 1, litra a, hvoraf det følger, at behandling af personoplysninger er lovlig, hvis den registrerede har givet samtykke til behandling af sine personoplysninger til et eller flere specifikke formål. Den registreredes samtykke skal herudover opfylde betingelserne for samtykke i persondataforordningens artikel 7.

Det bemærkes herudover, at baggrundskontrol § 16 vil skulle ske inden for rammerne af CER-direktivets artikel 14, stk. 2, hvoraf det følger, at anmodninger om baggrundskontrol vurderes inden for en rimelig frist og behandles i overensstemmelse med national ret og nationale procedurer samt relevant og gældende EU-ret, herunder databeskyttelsesforordningen og Europa-Parlamentets og Rådets direktiv (EU) 2016/680 om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger og om ophævelse af Rådets rammeafgørelse 2008/977/RIA, samt at baggrundskontrol skal være forholdsmæssig og strengt begrænset til, hvad der er nødvendigt.

Det vurderes på den baggrund, at myndigheder og virksomheder med hjemmel i databeskyttelseslovens § 8 kan videregive oplysninger om strafbare forhold til Energistyrelsen og andre myndigheder efter lovens regler.

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 fx. 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- og CER-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.

11. Hørte myndigheder og organisationer m.v.

Et udkast til lovforslag har i perioden fra den … til den … (… dage) været sendt i høring hos følgende myndigheder og organisationer m.v.:

12. Sammenfattende skema

	Positive konsekvenser/mindreudgifter (hvis ja, angiv omfang/hvis nej, anfør »Ingen«)	Negative konsekvenser/merudgifter (hvis ja, angiv omfang/hvis nej, anfør »Ingen«)
Økonomiske konsekvenser for stat, kommuner og regioner	Ingen	3-4 mio. kr.
Implementeringskonsekvenser for stat, kommuner og regioner	Ingen	Ingen
Økonomiske konsekvenser	Ingen/kvantificeres yderligere ifm. udarbejdelse af bekendtgørelse.	650 mio.kr. i omstillingsomkostninger.

for erhvervslivet m.v.		100 mio.kr. i løbende omkostninger. Her er business-as-usual ikke iagttaget.
Administrative konsekvenser for erhvervslivet m.v.	Ingen/kvantificeres yderligere ifm. udarbejdelse af bekendtgørelse.	25 mio. kr. i omstillingsomkostninger. 65 mio. kr. i løbende omkostninger. Her er business-as-usual ikke iagttaget.
Administrative konsekvenser for borgerne	Ingen	Ingen
Klimamæssige konsekvenser	Ingen	Ingen
Miljø- og naturmæssige konsekvenser	Ingen	Ingen
Forholdet til EU-retten	Lovforslaget skal foruden at styrke beredskabsreguleringen i energisektoren implementere EU-direktiverne NIS2 og CER. Det er hensigten, at implementeringen af lovforslaget tager hensyn til, at danske virksomheder inden for energisektoren ikke stilles dårligere konkurrencemæssigt i international sammenhæng – samt udmøntningen af direktiverne ikke går videre end minimumskravene i direktiverne, medmindre at den eksisterende beredskabsregulering sætter større krav, end hvad direktiverne pålægger, eller såfremt sektorspecifikke hensyn, herunder trusselsbilledet tilsiger andet. Af hensyn til at sikre harmonisering af krav og definitioner på tværs af sektorer sker der tæt koordinering med FMN, der forestår overordnet implementering af NIS2 og CER på tværs af ministerområderne. Det skal sikre, at bl.a. multiforsyningsvirksomheder, som tilhører flere sektorer, samt multinationale virksomheder ikke pålægges uhensigtsmæssige forskellige krav. Lovforslaget tager højde for, at der ikke reguleres unødigt og uproportionalt, herunder:	

	1. at virksomhederne selv foretager risikovurderinger, således at sikkerhedsforanstaltningerne kan tilpasses de mange forskellige virksomhedstypers forretningsmodeller. 2. at der i videst muligt omfang ikke stilles krav om anvendelse af specifikke teknologier. I stedet stilles der krav om, at virksomhederne selv kortlægger deres netværk og kritiske systemer, og på den baggrund skal leve op til en række beredskabskrav. 3. at virksomhederne allerede er underlagt krav til beredskabsregulering. Lovforslaget tager hensyn til princippet om at træde i kraft senest muligt og under hensyntagen til de fælles ikrafttrædelsesdatoer.
Er i strid med de fem principper for implementering af erhvervsrettet EU-regulering (der i relevant omfang også gælder ved implementering af ikke-erhvervsrettet EU-regulering) (sæt X)	Ja [X] Nej [] [X] []

Bemærkninger til lovforslagets enkelte bestemmelser

Til § 1 [Kapitel 1]

Det foreslås med lovens *§ 1, stk. 1*, at loven har til formål at styrke virksomhederne i energisektorens modstandsdygtighed overfor naturskabte, menneskeskabte og teknologiske trusler. Dette skal ske ved at fastsætte regler om virksomhedernes organisatoriske beredskab, deres fysiske sikring og cybersikkerhed. Formålet med bestemmelsen er at fastsætte den overordnet ramme for loven og give kontekst til de resterende bestemmelser i loven.

Formålet i stk. 1 sigter på at klima-, energi- og forsyningsministeren løfter sit sektoransvar efter Beredskabslovens § 24, der bestemmer at hver minister indenfor sit område skal stå for planlægningen af det civile beredskab, altså opretholdelsen og videreførelsen af samfundets funktioner i tilfælde af større ulykker, katastrofer, antagonistiske handlinger og krig. Klima-, energi- og forsyningsministeren løfter således sit planlægningsmæssige sektoransvar ved udstedelse af denne lov og tilhørende bekendtgørelser, således virksomhederne er robuste og har et velforberedt beredskab, samt at virksomhedernes samarbejde med hinanden og med myndighederne er fastlagt på forhånd medhenblik på at virksomhederne, såvel som myndighederne kan handle hurtigt og effektivt for at imødegå en nærtstående hændelse i energisektoren eller minimere konsekvenserne af en allerede aktualiseret hændelse og sikre hurtig genopretning af forsyningen.

Samtidig må gøres klart, at der som led i dette formål ikke vil blive stillet krav til virksomhederne om, at de aktivt skal kunne beskytte sig mod terrorangreb el. angreb af en militaristisk natur. Det er således i udgangspunktet kun den civile sektors ansvar at have passive beskyttelsesforanstaltninger kunne beskytte sig mod kriminelle, idet staten har til opgave beskytte Danmark igennem suverænitetshævelse, overvågning af danske farvande og luftrum og opretholde sikkerhed, fred og orden ved at føre kontrol med, at lovene overholdes, og at skride ind over for lovovertrædelser ved efterforskning og forfølgning.

Ovenstående er gældende både i den fysiske og logiske verden. Eksempelvis betyder det at en virksomhed ikke vil skulle kunne forhindre en terrorist der har intention om at detonere en bombe på en transformerstation. Men virksomheden skal kunne opdage når uautoriserede personer forsøger

på eller er kommet ind på lokation som indeholder kritisk energiinfrastruktur, at forsinke deres indtrængen igennem passive installationer som hegn, låse og barrikader og virksomheden skal have procedurer på plads der gør at politiet eller andre myndigheder underrettes hurtigt, ligesom der skal kunne indsamles overvågningsmateriale, der kan hjælpe myndighederne i deres opklaringsarbejde.

Det samme er gældende for den digitale verden, hvor virksomhederne igennem tekniske og organisatoriske foranstaltninger, skal kunne beskytte sig mod hackerangreb, ved i at videst muligt omfang at forhindre uautoriserede personer i at tilgår deres netværk, forsinke deres videre færd igennem deres netværk og systemer, når de er kommet ind i et system. Dette kan opnås f.eks. ved segmentering af systemer både logisk og fysisk. Ligeledes skal virksomhederne kunne detektere når de bliver kompromitteret eller forsøgt kompromitteret, have procedurer på plads til at foretage mitigerende foranstaltninger og underrette de relevante myndigheder og samarbejdspartnere, samt indsamle bevismaterialer såsom logs og adgangsregistre der kan hjælpe myndigheder i deres opklaringsarbejde.

Det følger af det foreslåede stk. 2, at loven endvidere har til formål at sikre, at der føres et grundigt og faglig funderet myndighedstilsyn med overholdelsen af disse regler, samt sikre et stærkt samarbejde mellem virksomhederne, organisationer og myndigheder der varetager roller i planlægningen af beredskabet og håndteringen af beredskabshændelser i energisektoren.

Det sekundære formål med loven jf. det foreslåede § 1, stk. 2 er todelt. Det første del af formålet er at sikre at der føres et grundigt og faglig funderet myndighedstilsyn med overholdelsen af disse regler. Således har Energistyrelsen der i dag varetager tilsynet med beredskabet i energisektoren på vegne af klima-, energi- og forsyningsministeren oparbejdet et tilsyn der er forankret i en stærk beredskabs- og cybersikkerhedsfaglighed der ligger vægt på at være værdiskabende for virksomhederne, således at udgangspunktet tilsynet er at gøre den enkelte virksomheds beredskab og cybersikkerhed bedre efter fuldendt tilsyn.

For at kunne opnå dette formål, er det en fundamental forudsætning, at tilsynet med virksomhedernes almene beredskab og it-beredskabet ligger hos den samme myndighed, af hensyn til synergien mellem disse opgaver og for at sikre en holistisk sikring af virksomhederne. Det har således også hi-

storisk været tilfældet, idet tilsynet med el- og naturgassektorerne har ligget hos Energinet fra 2005 til 2019, hvorefter Energistyrelsen har varetaget tilsynsopgaven.

Det andet delformål er at tilsikre et stærkt samarbejde mellem virksomhederne, organisationer og myndigheder, der direkte eller indirekte varetager en rolle i planlægningen af beredskabet og håndteringen af beredskabshændelser i energisektoren. Her tænkes der særligt på, at der et stor behov der er for informationsudveksling i forbindelse med planlægningen af beredskabet, men også under en hændelse og efter en hændelse. Her skal lovens forskellige paragraffer være med til at skabe tillid imellem de nævnte aktører således der kan ske effektiv planlægning, udførsel og evaluering af beredskabet, uden at beskyttelsesværdige informationer kommer uvedkommende i hænde. Ligeledes skal det tilsikres at mødefora, vejledningsmateriale og systemer oprettes og vedligeholdes til at understøtte den førnævnte informationsudveksling.

Til § 2 [Kapitel 1]

Den nuværende beredskabsregulering i energisektoren omfatter krav til hhv. alment beredskab og it-beredskab.

Beredskabet i el- og gassektoren er reguleret i elforsyningsloven og gasforsyningsloven samt tilhørende bekendtgørelser. Beredskabet i oliesektoren er reguleret i olieberedskabsloven og dertil hørende bekendtgørelse om beredskab i oliesektoren, samt i undergrundsloven, hvis bemyndigelsesparagraf ikke er udmøntet i en bekendtgørelse. Endvidere er der i lov om varmeforsyning krav om beredskabsplanlægning om end bemyndigelsen til at fastsætte nærmere regler heller ikke her er blevet udmøntet ved bekendtgørelse.

Beredskabsreguleringen for elsektoren omfatter virksomheder som er bevillingspligtige efter §§ 10 og 19 i elforsyningsloven eller har tilladelse til elproduktion fra anlæg med en kapacitet på over 25 MW efter § 29 i lov om fremme af vedvarende energi eller § 11, elforsyningsvirksomhed, der varetages af Energinet eller denne virksomheds helejede datterselskaber i medfør af § 2, stk. 2 og 3, i lov om Energinet, samt virksomheder, der yder balancering af elsystemet.

Beredskabsreguleringen for gassektoren omfatter selskaber, der er bevillingspligtige efter § 10, samt Energinet og dennes helejede datterselskaber,

der varetager gasforsyningsvirksomhed i henhold til § 2, stk. 2 og 3, i lov om Energinet.

Beredskabet for oliesektoren omhandler primært lagerberedskab af olieprodukter. Olieberedskabsbekendtgørelsen har ophæng i olieberedskabsloven, som fastsætter regler om beredskab for virksomheder, der er kritiske for forsyning af råolie og olieprodukter i Danmark i en beredskabssituation og andre ekstraordinære situationer. Bekendtgørelsen finder anvendelse på virksomheder med positiv lagringspligt samt den centrale lagerenhed FDO (Danske Olieberedskabslagre). Virksomhederne og FDO skal foretage beredskabsplanlægning, der sikrer forsyningen af olie fra egne lagre i en beredskabssituation.

Derudover regulerer undergrundsloven forsyningsberedskabet for virksomheder, som driver offshore olie- og gasplatforme og rørledninger i Nordsøen i forbindelse med udvindingen af olie og gas. Loven indeholder en generel forpligtigelse til virksomheder om beredskabsplanlægning mm. for at kunne opretholde og videreføre forsyningen af kulbrinter til samfundet i krisesituationer. Loven giver ministeren mulighed for at fastsætte nærmere regler herom, men denne hjemmel har ikke hidtil været benyttet.

I varmeforsyningsloven er der ligeledes en generel forpligtigelse til at virksomheder der driver anlæg til produktion og fremføring af bygas, skal foretage nødvendig planlægning og træffe de nødvendige foranstaltninger for at sikre bygasforsyningen i beredskabssituationer og andre ekstraordinære situationer. Loven giver ministeren mulighed for at fastsætte nærmere regler herom, men denne hjemmel har ikke hidtil været benyttet, ligesom ved undergrundsloven.

Efter gældende ret er det altså kun nogle begrænset typer virksomheder og virksomheder af en vis størrelse i de forskellige delsektorer, der omfattet af beredskabskravene. Således er lang række af virksomheder i energisektoren ikke omfattet af gældende ret, f.eks. fjernvarmevirksomheder, fjernkølingsvirksomheder, brintvirksomheder, biogasvirksomheder, virksomheder der udfører forskellige opgaver i el- og gasmarkedet og kommercielle virksomheder i downstream oliesektoren hvis disse ikke har pligt til at holde olieberedskabslagre.

Da indeværende lovforslag bl.a. skal gennemføre NIS 2- og CER-direktiverne for klima-, energi- og forsyningsministerens ressort, er det foreslåede anvendelsesområde for loven i høj grad dikteret af disse direktivers anvendelsesområder.

Det følger derfor af den foreslåede § 2, *stk. 1,* at loven i udgangspunktet finder anvendelse på følgende virksomheder når disse leverer deres tjenester eller udfører deres aktivitet inden for Danmark jf. dog stk. 2-4; 1) Elektricitetsvirksomheder, 2) Distributionssystemoperatører, 3) Transmissionssystemoperatører, 4) Elproducenter, 5) Udpegede elektricitetsmarkedsoperatører, 6) Markedsdeltagere der leverer tjenester, der vedrører aggregering, fleksibelt elforbrug eller energilagring, 7) 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, 8) Operatører af fjernvarme eller fjernkøling, 9) Olierørledningsoperatører, 10) Operatører af olieproduktionsanlæg, -raffinaderier og -behandlingsanlæg, olielagre og olietransmission, 11) Centrale lagerenheder, 12) Gasforsyningsvirksomheder, 13) Lagersystemoperatører,14) LNG-systemoperatører, 15) Naturgasvirksomheder, 16) Operatører af naturgasraffinaderier og –behandlingsanlæg ,17) Operatører inden for brintproduktion, -lagring og –transmission, 18) Operatører af tankstationer, der er ansvarlige for forvaltningen og driften af en tankstation.

De ovennævnte typer af virksomheder modsvarer de virksomheder der er nævnt i bilag I i NIS 2- og CER-direktivet for energisektoren, dog med undtagelse af nr. 18) Operatører af tankstationer, der er ansvarlige for forvaltningen og driften af en tankstation, denne tilføjelse er efter nationalt ønske om også lade tankstationer omfatte af reglerne.

Det følger af foreslåede § 2, *stk. 2,* at udgangspunktet for anvendelsesområdet for loven modificeres for de virksomheder der er nævnt i nr. 1-8, 10, 12 og 18, således at disse typer af virksomheder kun er omfattet såfremt de overskrider de minimumskriterier der oplistes i stk. 2, nr. 1-5. Det følger således at loven kun gælder for disse virksomheder såfremt virksomheden; 1) årligt producerer, forbruger eller kontrollerer mere end 25 MW elektricitet, 2) i 2 ud af 3 sidste år har solgt mere end 13,9 GWh eller produceret over 181 Gwh fjernvarme, 3) årligt producerer/injicerer mere end 26 mio. Nm^3 gas i et gasnet, 4) Olieterminaler og lagre med kapacitet på 100.000 m^3 eller derover, 5) opererer en eller flere tankstationer med et årligt salg af olieprodukter på 600.000 m^3 eller derover.

De foreslåede nedre grænse for visse typer af virksomheder er udtryk for en fastholdelse af den eksisterende afgrænsning af virksomheder, som i høj grad er baseret på forsyningsstørrelse og kritikalitet. Den foreslåede afgrænsning i stk. 2, nr. 1, på 25 MW følger således den afgrænsning der gælder i dag for elproduktionsvirksomheder, hvor kun virksomheder med elproduktionsbevilling efter elforsyningsloven og virksomheder med tilladelse til elproduktion fra anlæg med en kapacitet på over 25 MW efter § 29 i lov om fremme af vedvarende energi er omfattet.

Den foreslåede bestemmelse i § 2 stk. 2, *nr. 2,* medfører at virksomheder omfattes af loven, såfremt de i 2 ud af de sidste 3 år har solgt mere end 13,9 GWh eller produceret over 181 GWh fjernvarme. Grænserne i bestemmelsen er en konvertering af 25 MW grænsen til fjernvarmesektoren. Grunden til at det er solgt eller produceret i 2 af de 3 sidste år, er fordi fjernvarmevirksomhederne kan opleve udsving i salg/produktionen alt efter vejret og priserne på elmarkedet.

Den foreslåede bestemmelse i § 2, stk. 2, *nr. 3,* medfører at virksomheder omfattes af loven, såfremt de årligt producerer eller injicerer mere end 26 mio. Nm^3 gas i et gasnet. Den foreslåede grænse er blevet fastsat efter diskussion med blandet andet biogasbranchen, hvorefter at man får frasorteret de mindste og derfor ikke kritiske biogasproducenter.

Den foreslåede bestemmelse i § 2, stk. 2, *nr. 4,* medfører at virksomheder omfattes af loven, såfremt de operer olieterminaler og lagre med kapacitet på 100.000 m^3 eller derover. Den foreslåede grænse er blevet fastsat hensyn til at frasortere de mindste olielagre og terminaler, således operatører af mindre og ikke kritiske olieterminaler og lagre ikke er omfattet.

Den foreslåede bestemmelse i § 2, stk. 2, *nr. 5,* medfører at virksomheder omfattes af loven, såfremt de opererer en eller flere tankstationer med et årligt salg af olieprodukter på 600.000 m^3 eller derover. Den foreslåede grænser er fastsat ud fra det hensyn at beskytte forsyningen af benzin og diesel til vejtransport. Grænsen er fastsat således at kun de største tankstationsoperatører vil blive omfattet, og skal forstås som en operatørs samlede årlige salg af olieprodukter på tværs af alle de tankstationer som operatøren operer. Det således Klima-, Energi- og Forsyningsministeriets forståelse at et helt netværk af tankstationer kan kompromitteres igennem de net- og informationssystemer der bruges til at overvåge beholdninger af olieprodukter på stationerne. Men idet at Danmark er et af de lande med den største kon-

centration af tankstationer pr. indbygger har Klima-, Energi- og Forsyningsministeriet valgt at foreslå at kun de største operatører skal omfattes således der altid være et minimum af forsyning af olieprodukter til understøttelse af vejtransporten.

I dag er 84 virksomheder inden for el-, gas- og oliesektoren omfattet af bered-skabsbekendtgørelserne. Direktivernes tilføjelse af nye delsektorer samt en fastholdelse af eksisterende afgrænsningsmodel baseret på forsyningsstørrelse og kritikalitet indebærer, at antallet af virksomheder, som omfattes af beredskabskrav og fast tilsyn estimeres at øges til ca. 180 virksomheder. I tillæg til de ca. 180 virksomheder estimeres det at yderligere ca. 200 energivirksomheder med lille forsyning omfattes af nye krav om en beredskabsplan og et kontaktpunkt.

Det følger af den foreslåede § 2, *stk. 3,* at Loven gælder uanset stk. 2, for virksomheder; 1) der har en positiv lagringsforpligtelse efter Olieberedskabsloven, 2) nævnt i stk. 1, men som falder under grænserne i stk. 2, såfremt virksomheden beskæftiger minimum 50 ansatte eller har en årlig omsætning på minimum 10 mio. EUR og en årlig samlet balance på minimum 10 mio. EUR.

Det foreslåede § 2, stk. 3, *nr. 1,* er en regel der fungerer som sikkerhedsventil ift. de nedre grænser foreslåede i stk. 2. Således er det med den foreslåede stk. 3, nr. 1, sikret at virksomheder med positiv lagringsforpligtigelse efter Olieberedskabsloven altid er omfattet den foreslåede lov også selvom de ikke selv ejer lagret eller terminalen som beredskabsolien befinder sig i eller hvis de har en kapacitet på mindre end 100.000 m^3. Det er essentielt at de virksomheder med positiv lagringsforpligtigelse efter olieberedskabsloven er omfattet denne lov, idet tilgængeligheden af beredskabslagrene disse virksomheder holder, er et grundlæggende krav for at kunne have et velfungerende og brugbart olielagerberedskab.

Den foreslåede § 2, stk. 3, *nr. 2,* er for sikre at der uagtet de nedre grænser i stk. 2, forsat kan ske EU konform implementering af NIS 2 direktivet. NIS 2-direktivets art. 2, stk. 1 forskriver således at direktivet skal finde anvendelse 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.

Det følger af det foreslåede *§ 2, stk. 4*, at kapitel 5 om sikkerhedsgodkendelser og baggrundkontrol samt § 18 om gebyrbetaling for anmodning om sikkerhedsgodkendelse og baggrundskontrol finder anvendelse på alle virksomheder, organisation, fonde og erhvervsdrivende fonde, der varetager opgaver som direkte led eller i forbindelse med leveringen af de i stk. 1, nævnte tjenester.

Den foreslåede bestemmelse udvider anvendelsesområdet for, hvilke aktører der kan anmode Klima-, Energi- og Forsyningsministeriet om at få foretaget undersøgelse og afgørelse om sikkerhedsgodkendelse og baggrundskontrol af deres ansatte. Således vil organisationer, fonde og erhvervsdrivende fonde samt flere virksomheder end de i § 2, stk. 1-3 nævnte kunne anmode herom, såfremt den pågældende ansatte varetager opgaver som et direkte led eller i forbindelse med leveringen af de tjenester, der er nævnt i § 2, stk. 1. Endvidere indebærer bestemmelsen, at virksomheder, organisationer, fonde og erhvervsdrivende er omfattet af kravet om at skulle betale for deres ansøgninger om baggrundskontrol og sikkerhedsgodkendelse hos Klima-, Energi- og Forsyningsministeriet på vegne af virksomheden, organisationen, fonden eller den erhvervsdrivende fond.

Den foreslåede bestemmelse tager hensyn til, at energisektoren omfatter mange aktører, der ikke nødvendigvis har en direkte forbindelse til leveringen af tjenesterne nævnt i § 2, stk. 1, men som leverer andre tjenester, services eller indsigt, der bidrager til at skabe en mere robust og sikker energisektor. Flere fora, der diskuterer resiliens og sikkerhed i energisektoren, anvender sikkerhedsgodkendelser som et krav for at kunne deltage. Det vil eksempelvis være fora, hvor emner omhandlende kritisk infrastruktur og kortlægning heraf drøftes. Derfor foreslås det, at der sikres en hjemmel til at sikkerhedsgodkende af disse aktører. Endvidere vil eksempelvis virksomheder, som indsamler data om cybertrusler og -angreb om energisektoren, ikke være omfattet af lovens almene anvendelsesområde, men vil være omfattet af det udvidede anvendelsesområde for sikkerhedsgodkendelser og baggrundskontrol i lovens kapitel 5.

Der henvises i øvrigt til afsnit 3.4 om sikkerhedsgodkendelser og baggrundskontrol i lovforslagets almindelige bemærkninger.

Det følger af den foreslåede § 2, *stk. 5*, at loven gælder på land- og søterritoriet, den eksklusive økonomiske zone samt kontinentalsokkelen.

Den foreslåede bestemmelse er en forsættelse af de paragraffer der findes i en række af de forsyningslove som beredskabet tidligere har været forankret i og cementerer at loven og regler udstedt i medfør af loven gælder på land- og søterritoriet, den eksklusive økonomiske zone samt kontinentalsokkelen.

Til § 3 [Kapitel 1]

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

Definitionerne bygger på de relevante tilsvarende definitioner i artikel 6 i NIS 2-direktivet. Definitionerne bygger endvidere også på de relevante tilsvarende definitioner i artikel 2 i CER-direktivet. Endvidere gengives definitionerne fra de to direktivers bilag I fsva. energisektorens enhedskategorier, og såfremt der her er henvist til artikler i andre direktiver og forordninger er disse medtaget i indeværende lovforslags definitioner for at hjælpe regelanvenderne, således at der ikke er behov for at slå op i to eller flere EU-retsakter for at forstå definitionen.

Definitionerne i den foreslåede § 3 svarer således indholdsmæssigt til de relevante dele af NIS 2-direktivets artikel 6 og CER-direktivets artikel 2, og skal i udgangspunktet forstås og anvendes i overensstemmelse med direktivernes forudsætninger. Der er dog enkelte tilfælde, hvor definitioner er blevet lagt sammen eller udvidet, idet indeværende lovforslag implementerer både NIS 2- og CER-direktivet, og begge direktiver taler om tilnærmelsesvis samme begreber flere steder. Således er en »hændelse« efter denne lov både en hændelse som defineret i NIS 2- og CER-direktivet, mens en »cyberhændelse« er en cyberhændelse som defineret i NIS 2-direktivet. Det vil fremgå for hver definition nedenfor.

Det foreslås i § 3, stk. 1, *nr. 1*, at »aggregering« defineres som funktion, der varetages af en fysisk eller juridisk person, der samler flere kunders forbrug eller producerede elektricitet til salg, køb eller auktion på et elektricitetsmarked. Aggregering er ikke levering af elektricitet.

Det foreslås i § 3, stk. 1, *nr. 2*, at »centrale lagerenheder « defineres som et organ eller tjeneste, som er tildelet beføjelser til at handle med henblik på at erhverve, holde eller sælge olielagre, herunder beredskabslager og specifikke lagre.

Det foreslås i § 3, stk. 1, *nr. 3*, at »cyberhændelse« 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 NIS 2-direktivets definition.

Det foreslås i § 3, stk. 1, *nr. 4*, 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 § 3, stk. 1, *nr. 5*, 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 § 3, stk. 1, *nr. 6*, at »distributionssystemoperatører« defineres som en fysisk eller juridisk person, der er ansvarlig for driften, vedligeholdelsen og om nødvendigt udbygningen af distributionssystemet i et givet

område samt i givet fald dets sammenkoblinger med andre systemer og for at sikre, at systemet på lang sigt kan tilfredsstille en rimelig efterspørgsel efter distribution af elektricitet eller gas.

Det foreslås i § 3, stk. 1, *nr. 7,* at » elektricitetsvirksomheder« defineres som en fysisk eller juridisk person, der driver mindst en af følgende former for virksomhed: produktion, transmission, distribution, aggregering, fleksibelt elforbrug, energilag-ring, levering eller køb af elektricitet, og som er ansvarlig for de kommercielle, tekniske eller vedligeholdelsesmæssige opgaver i forbindelse med disse aktiviteter, men som ikke er slutkunde der varetager salg, herunder videresalg, af elektricitet til kunder.

Det foreslås i § 3, stk. 1, *nr. 8,* at »elproducenter« defineres som en fysisk eller juridisk person, der fremstiller elektricitet.

Det foreslås i § 3, stk. 1, *nr. 9,* at »energilagring« defineres som i elektricitetssystemet, udsættelse af den endelige anvendelse af elektricitet til et senere tidspunkt end det, hvor den blev produceret, eller konvertering af elektrisk energi til en energiform, der kan lagres, lagringen af sådan energi og den efterfølgende rekonvertering af sådan energi til elektrisk energi eller anvendelse som anden energibærer.

Det foreslås i § 3, stk. 1, *nr. 10,* at »fleksibelt elforbrug« defineres som ændringer i en slutkundes elforbrug i forhold til det normale eller aktuelle forbrugsmønster som reaktion på markedssignaler, herunder som reaktion på tidspunktafhængige elpriser eller finansielle incitamenter, eller som reaktion på accept af slutkundens bud om at sælge en forbrugsreduktion eller -forøgelse til en bestemt pris på et organiseret marked, hvad enten dette sker alene eller gennem aggregering.

Det foreslås i § 3, stk. 1, *nr. 11,* at »gasforsyningsvirksomheder« defineres som Enhver fysisk eller juridisk person, der varetager forsyningsopgaven.

Det foreslås i § 3, stk. 1, *nr. 12,* at »hændelse« defineres som en begivenhed, herunder en cyberhændelse, der har potentiale til i betydelig grad at forstyrre, eller som forstyrrer, leveringen af en væsentlig tjeneste, herunder når den påvirker de nationale systemer, der sikrer retsstatsprincippet, samt cyberhændelser.

Bestemmelsen bygger på CER-direktivets artikel 2, nr. 3, hvorefter der ved »hændelse« forstås en begivenhed, der har potentiale til i betydelig grad at forstyrre, eller som forstyrrer, leveringen af en væsentlig tjeneste, herunder

når den påvirker de nationale systemer, der sikrer retsstatsprincippet. Dog er der tilføjet "herunder en cyberhændelse", medhenblik på at gøre det klart at hændelsesbegrebet i denne lov omfatter alle hændelser.

Det foreslås i § 3, 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 NIS 2-direktivets definition. Men i modsætning til NIS 2-direktivets artikel vil den blive anvendt og skal forstås i kontekst både af den fysiske og den logiske verden.

Det foreslås i § 3, 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 § 3, stk. 1, *nr. 15,* at »IKT-produkt«: 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 § 3, stk. 1, *nr. 16,* at »IKT-tjeneste«: 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 § 3, stk. 1, *nr. 17,* at »lagersystemoperatører« defineres som enhver fysisk eller juridisk person, der foretager oplagring af gas og er ansvarlig for driften af en gaslagerfacilitet.

Det foreslås i § 3, stk. 1, *nr. 18,* at »LNG-systemoperatører« defineres som enhver fysisk eller juridisk person, der foretager flydendegørelse af naturgas eller import, losning og forgasning af LNG og er ansvarlig for driften af en LNG-facilitet.

Det foreslås i § 3, stk. 1, *nr. 19,* at »markedsdeltagere der leverer tjenester, der vedrører aggregering, fleksibelt elforbrug eller energilagring« defineres som en fysisk eller juridisk person, der køber, sælger eller producerer elektricitet, der udfører aggregering, eller der er en operatør af tjenester vedrørende fleksibelt elforbrug eller energilagringstjenester, herunder ved afgivelse af handelsordrer, på et eller flere elektricitetsmarkeder, herunder på balanceringsenergimarkeder.

Det foreslås i § 3, stk. 1, *nr. 20,* at »modstandsdygtighed« defineres som en enhed evne til at forebygge, beskytte mod, reagere på, modstå, afbøde, absorbere, tilpasse sig og komme på fode igen efter en hændelse.

Bestemmelsen bygger på CER-direktivets artikel 2, nr. 2, hvorefter der ved »modstandsdygtighed« forstås en kritisk enheds evne til at forebygge, beskytte mod, reagere på, modstå, afbøde, absorbere, tilpasse sig og komme på fode igen efter en hændelse.

Det foreslås i § 3, stk. 1, *nr. 21,* at »naturgasvirksomheder« defineres som enhver fysisk eller juridisk person, der driver mindst en af følgende former

for virksomhed: produktion, transmission, distribution, forsyning, køb eller oplagring af naturgas, herunder LNG, og som er ansvarlig for de kommercielle, tekniske og/eller vedligeholdelsesmæssige opgaver i forbindelse med disse aktiviteter, men som ikke er endelig kunde.

Det foreslås i § 3, stk. 1, *nr. 22,* at »net- og informationssystem « defineres som; a) et elektronisk kommunikationsnet, hvorved forstås transmissionssyste-mer, uanset om de bygger på en permanent infrastruktur eller centraliseret administrationskapacitet, og, hvor det er relevant, koblings- og dirigerings-udstyr og andre ressourcer, herunder netelementer, der ikke er aktive, som gør det muligt at overføre signaler ved hjælp af trådforbindelse, radiobøl-ger, lyslederteknik eller andre elektromagnetiske midler, herunder satellit-net, jordbaserede fastnet (kredsløbs og pakkekoblede, herunder i internet-tet) og mobilnet, elkabelsystemer, i det omfang de anvendes til transmissi-on 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 NIS 2-direktivets definition.

Det foreslås i § 3, stk. 1, *nr. 23,* at »nærvedhændelse« defineres som en begivenhed, der kunne have bragt tilgængeligheden, autenticiteten, integriteten eller fortroligheden af lagrede, overførte eller behandlede data eller af de tjenester, der tilbydes af eller er tilgængelige via net- og informationssystemer, i fare, men som det lykkedes at forhindre, eller som ikke materialiserede sig.

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

Det foreslås i § 3, stk. 1, *nr. 24,* at »operatører af fjernvarme eller fjernkøling« defineres som operatører af distribution af termisk energi i form af

damp, varmt vand eller afkølede væsker fra centrale eller decentrale produktionssteder gennem et net til flere bygninger eller anlæg til anvendelse ved rum- eller procesopvarmning eller –køling.

Det foreslås i § 3, stk. 1, *nr. 25,* at »organiseret marked« defineres som; a) Et multilateralt system, der samler eller faciliterer samlingen af flere tredjeparters købs- og salgsinteresser i engrosenergiprodukter på en måde, der fører til indgåelse af en kontrakt, b) Ethvert andet system eller enhver anden facilitet, hvor flere købs- og salgsinteresser i engrosenergiprodukter tilhørende tredjeparter kan interagere på en måde, der fører til indgåelse af en kontrakt. Dette omfatter elektricitets- og gasbørser, mæglere og andre personer, der erhvervsmæssigt arrangerer transaktioner, og markedspladser, herunder ethvert reguleret marked, en MHF eller en OHF.

Det foreslås i § 3, stk. 1, *nr. 26,* at »risiko« defineres som potentialet for tab eller forstyrrelse som følge af en hændelse, udtrykt som en kombination af størrelsen af et sådant tab eller en sådan forstyrrelse og sandsynligheden for, at hændelsen indtræffer.

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

Det foreslås i § 3, stk. 1, *nr. 27,* at »risikovurdering« defineres som den samlede proces med henblik på at bestemme arten og omfanget af en risiko ved at identificere og analysere potentielle relevante trusler, sårbarheder og farer, der kunne føre til en hændelse, og ved at evaluere det potentielle tab eller den potentielle forstyrrelse af leveringen af en væsentlig tjeneste forårsaget af denne hændelse.

Den foreslåede bestemmelse svarer til definitionen i CER-direktivets artikel 2, nr. 7. Det forudsættes, at bestemmelsen fortolkes i overensstemmelse med CER-direktivets definition.

Det foreslås i § 3, stk. 1, *nr. 28,* at »transmissionssystemoperatører « defineres som en fysisk eller juridisk person, der er ansvarlig for driften, vedligeholdelsen og om nødvendigt udbygningen af transmissionssystemet i et givet område samt i givet fald dets sammenkoblinger med andre systemer og for at sikre, at systemet på lang sigt kan tilfredsstille en rimelig efterspørgsel efter transmission af elektricitet eller gas.

Det foreslås i § 3, stk. 1, *nr. 29*, at »udpegede elektricitetsmarkedsoperatører« defineres som en markedsoperatør, der af den kompetente myndighed er blevet udpeget til at udføre opgaver i forbindelse med den fælles day-ahead- eller intraday-kobling.

Det foreslås i § 3, stk. 1, *nr. 30*, at »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.

Det foreslås i § 3, stk. 1, nr. 31, at »væsentlig tjeneste« defineres som en tjeneste, der er afgørende for opretholdelsen af vitale samfundsmæssige funktioner, økonomiske aktiviteter, folkesundhed og offentlig sikkerhed eller miljøet.

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

Det bemærkes, at Kommissionens delegerede forordning (EU) 2023/2450 af 25. juli 2023, til supplering af Europa-Parlamentets og Rådets direktiv (EU) 2022/2557 ved opstilling af en liste over væsentlige tjenester, opstiller en ikke udtømmende lister over væsentlige tjenester i artikel 2.

Til § 4 [Kapitel 2]

Rådets direktiv (EU) 2008/114 af 8. december 2008 om indkredsning og udpegning af europæisk kritisk infrastruktur og vurdering af behovet for at beskytte den bedre (EPCIP-direktivet) finder anvendelse for energi- og transportsektorerne.

I energisektoren er EPCIP-direktivet implementeret ved bekendtgørelse om identifikation og udpegning af europæisk kritisk infrastruktur på energiområdet og vurdering af behovet for bedre beskyttelse. Efter § 3, stk. 1, foretager Energistyrelsen identifikation af europæisk kritisk infrastruktur. Metoden for udpegelse fremgår af bekendtgørelsens § 4, stk. 1.

Ifølge bekendtgørelse om beredskab om elsektoren § 11, stk. 1 og bekendtgørelse om beredskab for gassektorens § 11, stk. 1, skal Energistyrelsen

foretage en klassificering af anlæg i el og gassektoren. Det følger af bekendtgørelse om it-beredskab for el- og naturgassektoren, at Energistyrelsen skal foretage kategorisering af virksomheder.

Ifølge bekendtgørelse om beredskab i elsektoren § 11, stk. 1 og bekendtgørelse i beredskab for gassektorens § 11, stk. 1, skal Energistyrelsen foretage en klassificering af anlæg i el og gassektoren. Kategorisering og klassificering afhænger af anlæggets eller virksomhedens betydning for energiforsyningen og er afgørende for, hvilke beredskabskrav der stilles til virksomhederne.

For oliesektoren er der ikke indført en kategorisering af virksomheder, som fastsætter, hvilke beredskabskrav de skal overholde.

Det følger af den foreslåede § 4, *stk. 1*, at klima-, energi- og forsyningsministeren identificerer kritiske virksomheder samt kritiske systemer og anlæg i energisektoren, der anvendes til at levere virksomhedens tjenester.

Den foreslåede bestemmelse gennemfører artikel 6, stk. 1, i CER-direktivet, hvoraf det fremgår, at hver medlemsstat senest den 17. juli 2026 skal have identificeret de kritiske enheder for de sektorer og delsektorer, der er anført i bilaget til CER-direktivet. Med bestemmelsen har klima-, energi- og forsyningsministeren hjemmel til at foretage identificeringen.

Om baggrunden for artikel 6, stk. 1, beskrives det i CER-direktivets præambelbetragtning nr. 8, at medlemsstaterne, for at opnå en høj grad af modstandsdygtighed, bør identificere kritiske enheder, som vil være underlagt specifikke krav og specifikke tilsyn, og som vil ydes særlig støtte og vejledning over for alle relevante risici. Den særlige støtte og vejledning vil eksempelvis komme til udtryk i nationale strategier eller risiko- og sårbarhedsscenarier.

Bestemmelsen vil desuden gennemføre NIS 2-direktivets artikel 3, stk. 3, hvoraf det fremgår, at medlemsstater 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.

Den foreslåede bestemmelse skal ses i sammenhæng med den foreslåede § 35, stk. 2, om indmeldingspligt for virksomheder, som skal sikre informationsgrundlaget for at foretage identifikation af virksomheder.

Identificering vil være en afgørelse i forvaltningsretlig forstand. Afgørelsen vil derfor skulle overholde de almindelige forvaltningsretlige regler og principper. Det medfører også, at en virksomhed vil kunne påklage en afgørelse om kategorisering til en højere administrativ myndighed efter de almindelige forvaltningsretlige principper om administrativ rekurs.

Efter den foreslåede § 4, *stk. 2,* fastsætter klima-, energi- og forsyningsministeren nærmere regler om identifikation og kategorisering af virksomheder og af virksomheders systemer og anlæg som anvendes til levering af virksomhedens tjenester.

Det følger af den foreslåede bestemmelse, at klima-, energi- og forsyningsministeren kan fastsætte nærmere regler om kategorisering i energisektoren. Det forudsættes med bestemmelsen, at der med kategoriseringen derigennem sker en identifikation af virksomheder samt kritiske systemer og anlæg som opfylder kravene for kritiske enheder efter CER-direktivets artikel 6, stk. 2.

Kategoriseringen forventes at blive udformet, således at virksomheder inddeles i niveauer på baggrund af kritikalitet. Virksomheder, som er mindst kritiske, indplaceres på niveau 1. Kategoriseringen af net- og informationssystemer og anlæg, vil ske ved at inddele disse i forskellige klasser. Ved klassificeringen vil de mindst kritiske net- og informationssystemer og anlæg indplaceres i klasse 1.

Efter den foreslåede bestemmelse, kan klima-, energi- og forsyningsministeren fastsætte regler om identificering og kategorisering af ikke kritiske virksomheder og af virksomheder systemer og anlæg som anvendes til virksomhedens tjenester.

Det forventes, at der vil ske kategorisering af net- og informationssystemer og anlæg, som falder uden for anvendelsesområdet af NIS 2- og CER-direktivet. Dette vil være virksomheder i de laveste niveauer og net- og informationssystemer i de laveste klasser. Dette sikrer, at der kan fastsættes regler om, at visse virksomheder skal efterleve simplere beredskabs krav, end hvad der fremgår af direktiverne.

Det bemærkes, at virksomheder som placeres i de lave kategorier ikke vil skulle indmeldes til kommissionen efter NIS 2-direktiets artikel 3, stk. 4 og CER-direktivets artikel 6, stk. 3.

Virksomheder, der er omfattet af loven, anses som kritiske enheder efter CER-direktivets artikel 6, stk. 2 og væsentlige og vigtige enheder efter NIS 2-direktivets artikel 3, stk. 3. Dog ikke virksomheder i de lave kategorier.

Det forudsættes, at de nærmere regler om identificering og kategorisering inddrager følgende hensyn; 1) den nationale strategi for styrkelse af modstandsdygtighed, 2) den nationale risikovurdering med henblik på kategorisering, 3) om enheden leverer en eller flere væsentlige tjenester, 4) om enheden opererer og har sin kritiske infrastruktur beliggende på dansk territorium og 5) om en hændelse vil have virkning på forsyningssikkerheden eller på leveringen af andre væsentlige tjenester i sektorer i bilag 1 af 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), som er afhængige af denne eller disse væsentlige tjenester.

De ovenfor anførte hensyn fremgår af CER-direktivets artikel 6, stk. 2, hvoraf det fremgår, at når en medlemsstat identificerer kritiske enheder, tager den hensyn til resultaterne af dens medlemsstatsrisikovurdering og dens strategi, og anvender alle følgende kriterier; a) enheden leverer en eller flere væsentlige tjenester, b) enheden opererer og dens kritiske infrastruktur er beliggende på denne medlemsstats område, og c) en hændelse vil have betydelige forstyrrende virkninger som fastslået i overensstemmelse med CER-direktivets artikel 7, stk. 1, (om betydelige forstyrrende virkninger) på enhedens levering af en eller flere væsentlige tjenester eller på leveringen af andre væsentlige tjenester i sektorerne anført i direktivets bilag, som er afhængige af denne eller disse væsentlige tjenester.

Bestemmelsen vil således gennemføre CER-direktivets artikel 6, stk. 2.

Det bemærkes i den forbindelse, at den danske sprogversions gengivelse af direktivets kriterier for identificering af kritiske enheder omtaler, hvorvidt »enheden opererer og dens kritiske infrastruktur er beliggende på denne medlemsstats område«. Den engelske sprogversion anvender derimod »territory«. Det samme gør sig gældende i direktivets præambelbetragtning nr. 16, hvorefter en enhed vil skulle anses for at operere på en medlemsstats område – i den engelske sprogversion »the territory« – hvor den udfører de aktiviteter, der er nødvendige for den eller de pågældende væsentlige tjenester, og hvor enhedens kritiske infrastruktur, som anvendes til at levere den eller de pågældende tjenester, er beliggende. Hvis der ikke er nogen

enhed, der opfylder disse kriterier i en medlemsstat, bør den pågældende medlemsstat ikke være forpligtet til at identificere en kritisk enhed i den tilsvarende sektor eller delsektor.

Energisektoren anvender i stort omfang det vindenergipotentiale som er i den eksklusive økonomiske zone ved opstilling af vindmøller. Disse vindmøller placeres således uden for dansk territorie. Desuden udnyttes der gas- og oliefelter som er placeret uden for dansk territorie. Energisektoren har derved flere former for virksomheder med tilhørende infrastruktur som er placeret inden for dansk område, men uden for dansk territorie.

Henset til, at der vurderes at være en indholdsmæssig forskel på »område« og »territory« og de særlige forhold der gør sig gældende for infrastruktur i energisektoren, foreslår klima-, energi og forsyningsministeriet, at nærværende lovforslag lægger sig op ad den danske sprogversion. Det indebærer, at der ved identificering af kritiske enheder bl.a. vil skulle lægges vægt på, om virksomheden opererer i og har sin kritiske infrastruktur beliggende »på dansk område«, hvor område også vurderes at omfatte den danske eksklusive økonomiske zone.

De nærmere regler om identificering kategorisering skal desuden tage hensyn til følgende kriterier; 1) antal brugere, der er afhængige af den væsentlige tjeneste, som udbydes af den berørte virksomhed, 2) omfanget af andre i bilaget anførte sektorers og delsektorers afhængighed af den pågældende væsentlige tjeneste, 3) den indvirkning som hændelser kunne have med hensyn til omfang og varighed på økonomiske og samfundsmæssige aktiviteter, miljøet, den offentlige sikkerhed eller befolkningens sundhed, 4) virksomhedens markedsandel på markedet for den berørte væsentlige tjeneste eller de berørte væsentlige tjenester, 5) det geografiske område, der kunne blive berørt af en hændelse, herunder eventuel grænseoverskridende indvirkning, under hensyntagen til den sårbarhed, som er forbundet med den grad af afsondrethed, der kendetegner visse typer af geografiske områder, såsom ø-regioner, afsidesliggende regioner eller bjergområder, og 6) virksomhedens betydning med hensyn til at opretholde et tilstrækkeligt niveau for den væsentlige tjeneste under hensyntagen til tilgængelighed af alternative måder at levere denne væsentlige tjeneste på. Den foreslåede bestemmelse gennemfører således CER-direktivets artikel 7, stk. 1, som opstiller samme kriterier.

Baggrunden for artikel 7, stk. 1, beskrives i CER-direktivets præambelbetragtning nr. 18, hvoraf det bl.a. fremgår, at der bør fastlægges kriterier for

bestemmelse af betydningen af en forstyrrende virkning som følge af en hændelse, og at disse kriterier bør være baseret på kriterierne 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). Det fremgår videre, at større kriser, såsom covid-19-pandemien, har vist, hvor vigtigt det er at sørge for forsyningskædesikkerhed, og hvordan forstyrrelse heraf kan have negativ økonomisk og samfundsmæssig indvirkning inden for en lang række sektorer og på tværs af grænserne. Medlemsstaterne bør derfor også i det omfang, det er muligt, overveje virkningerne på forsyningskæden, når de fastslår i hvilket omfang andre sektorer og delsektorer afhænger af de væsentlige tjenester, der udbydes af en kritisk enhed.

Bestemmelsen vil kunne anvendes til at fastsætte nærmere de nærmere kriterier for identificering af kritiske virksomheder, systemer og anlæg. De nærmere regler for identificering kan ændres over tid i forbindelse med den dynamiske udvikling af energisystemers opbygning og den gensidige afhængighed, der er mellem forskellige energiformer.

Det forventes, at kategoriseringen af virksomheder sker ved at inddele virksomhederne i niveauer. Med niveauinddeling kan der fastsættes differentierede krav om foranstaltninger og tilsyn, som tager hensyn til virksomhedernes kritikalitet for forsyningen. Det forventes, at virksomhederne vil blive inddelt i fem niveauer. De mindst kritiske virksomheder vil være niveau 1, mens de mest kritiske vil være niveau 5. Reglerne forventes udformet, således at antallet af niveauer kan udvides, i det omfang udviklingen af energisektoren kræver det.

Det forventes, at niveauinddelingen af virksomheder vil tage udgangspunkt i, hvilken delsektor virksomheden operer inden for, og den tjeneste, som virksomheden leverer. Hvis en virksomhed leverer tjenester i flere delsektorer, f.eks. hvis den leverer både el og varme, vil virksomheden kun blive inddelt på ét niveau. Det forventes, at virksomheden vil blive inddelt i niveauet for den forsyningsart, hvor tjenesten vil være mest kritisk.

Det forventes også, at virksomhedens samlede betydning for forsyningssikkerheden vil have betydning for, hvilket niveau virksomheden vil blive inddelt på. Ligeledes vil det have en betydning, om virksomheden leverer en tjeneste, som påvirker eller kan påvirke andre kritiske sektorer.

Virksomhedernes niveauinddeling vil blive foretaget ud fra en konkret vurdering med udgangspunkt i den samlede energimængde, virksomheden kontrollerer, virksomhedens betydning for energiforsyningen, om virksomheden leverer tjenester til andre kritiske sektorer eller varetager samfundskritiske opgaver.

Det forventes, at kategoriseringen af anlæg og systemer sker ved at inddele disse i klasser. Det forventes, at der ved klassificeringen vil blive taget udgangspunkt i den tjeneste, som anlægget eller systemer vedrører, mængden af energi, som de er med til at understøtte, og deres betydning for forsyningssikkerheden.

Det bemærkes at niveau inddeling og klassificering vurderes at være omfattet af begrebet kategorisering.

Klima-, energi- og forsyningsministeren kan fastsætte nærmere regler for, frekvensen af identificering og kategorisering.

Den foreslåede bestemmelse, vil dermed gennemføre CER-direktivets artikel 6, stk. 5, 1. pkt., hvoraf det fremgår, at medlemsstaterne gennemgår, hvor det er nødvendigt og under alle omstændigheder mindst hvert fjerde år, listen over identificerede kritiske enheder.

Det bemærkes, at identificering og kategorisering, foretaget på baggrund af regler udstedt i medfør af bestemmelsen, vil være en afgørelse i forvaltningsretlig forstand. Afgørelsen vil derfor skulle overholde de almindelige forvaltningsretlige regler og principper. Det medfører også, at en virksomhed vil kunne påklage en afgørelse om kategorisering til en højere administrativ myndighed efter de almindelige forvaltningsretlige principper om administrativ rekurs.

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

Til § 5 [Kapitel 2]

EPCIP-direktivet fastsætter en procedure og nærmere kriterier for indkredsning af potentiel europæisk kritisk infrastruktur og eventuel efterfølgende udpegning af den europæiske kritiske infrastruktur som sådan.

Det følger af artikel 3, stk. 1, i EPCIP-direktivet, at hver medlemsstat indkredser den potentielle europæiske kritiske infrastruktur, som opfylder

nærmere fastsatte tværgående og sektorbaserede kriterier og er i overensstemmelse med definitionerne for »kritisk infrastruktur« og »europæisk kritisk infrastruktur« i EPCIP-direktivets artikel 2, litra a og b. I direktivets bilag III er fastsat en nærmere procedure for medlemsstaternes indkredsning af europæisk kritisk infrastruktur.

Det følger af EPCIP-direktivets artikel 2, litra b, at der ved »europæisk kritisk infrastruktur« forstås kritisk infrastruktur, der befinder sig i medlemsstaterne, og hvis afbrydelse eller ødelæggelse ville få betydelige konsekvenser for to eller flere medlemsstater.

EPCIP-direktivet fastsætter herefter en høringsmekanisme, hvorefter medlemsstaterne efter indkredsning af potentiel europæisk kritisk infrastruktur underretter og indleder drøftelser med de øvrige medlemsstater, som kan blive berørt i betydelig grad af en potentiel europæisk kritisk infrastruktur. På baggrund af drøftelsen og nærmere aftale herom, kan den medlemsstat, på hvis område en potentiel europæisk kritisk infrastruktur er beliggende, derefter udpege den som europæisk kritisk infrastruktur. Medlemsstaten skal herefter underrette ejeren/operatøren af infrastrukturen om dens udpegning som europæisk kritisk infrastruktur.

Det følger af den foreslåede § 5, *stk. 1,* at virksomheder betragtes som kritiske enheder af særlig europæisk betydning, når virksomheden opfylder alle af følgende betingelser; 1) Er blevet identificeret som kritisk efter § 4, stk. 1., 2) Leverer de samme eller lignende væsentlige tjenester til eller i seks eller flere medlemsstater, 3) Er blevet underrettet om, at virksomheden betragtes som en kritisk enhed af særlig europæisk betydning i overensstemmelse med EU-regler.

Den foreslåede bestemmelse er med til at gennemføre artikel 17, stk. 1, i 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), hvorefter en enhed betragtes som en kritisk enhed af særlig europæisk betydning, hvor den a) er blevet identificeret som en kritisk enhed i henhold til direktivets artikel 6, stk. 1, b) leverer de samme eller lignende væsentlige tjenester til eller i seks eller flere medlemsstater, og c) er blevet underrettet i henhold til direktivets artikel 17, stk. 3.

Udpegelsen som kritisk enhed af særlig europæisk betydning, kan således alene ske, såfremt de tre betingelser som er oplistet i direktivet af opfyldt.

Den første betingelse om at enheden skal være identificeret som kritisk, vil ske i overensstemmelse med lovens foreslåede § 4, hvor der ved kategoriseringen af virksomheder og anlæg deri også vil ske en identifikation af virksomheder som opfylder eller ejer anlæg der opfylder kriterierne for kritiske enheder.

Det er således en forudsætning efter den foreslåede bestemmelse, at der leveres de samme eller lignende væsentlige tjenester til eller i seks eller flere EU-medlemsstater.

For at fastslå om der sker levering af væsentlige tjenester i fornødent omfang, vil den konsultationsprocedure, som reguleres i CER-direktivets artikel 17, stk. 2, og 3, skulle følges. Konsultationsproceduren indebærer overordnet, at Europa-Kommissionen konsulterer de kritiske enheder og de kompetente myndigheder i de medlemsstater, hvor de pågældende enheder har oplyst at levere væsentlige tjenester, med henblik på at undersøge, om enheden leverer de samme eller lignende væsentlige tjenester i eller til seks eller flere EU-medlemsstater. Europa-Kommissionen vil på den baggrund konstatere, om den pågældende kritiske enhed er at betragte som en kritisk enhed af væsentlig europæisk betydning. Klima-, energi- og forsyningsministeren kan således først udpege en kritisk enhed af særlig europæisk betydning, når Europa-kommissionen har konstateret at betingelserne herfor er opfyldt.

Efter den foreslåede § 5, *stk. 2*, underretter klima-, energi- og forsyningsministeren virksomheder, at de betragtes som kritiske enheder af særlig europæisk betydning i energisektoren i overensstemmelse med EU-regler.

Det følger af bestemmelsen, at klima-, energi- og forsyningsministeren underretter virksomheder, at de betragtes som kritiske enheder af særlig europæisk betydning. Ministeren vil skulle foretage underretningen, når kommissionen giver besked om at en virksomhed betragtes som en kritisk enhed af særlig europæisk betydning.

Efter bestemmelsen skal underretningen ske i overensstemmelse med gældende EU-regler. Denne del af bestemmelsen, sikrer at en fremtidig ændring hos Kommissionen, om hvornår en kritisk enhed betragtes som en kritisk enhed af særlig europæisk betydning, vil være i overensstemmelse med den foreslåede bestemmelse.

Efter den foreslåede § 5, *stk. 3*, fastsætter klima-, energi- og forsyningsministeren nærmere regler til brug for udpegelsen af kritiske enheder af særlig europæisk betydning.

Det forventes at der på baggrund af bestemmelsen, at der eksempelvis vil blive fastsat nærmere regler om, at relevante virksomheder skal underrette Klima-, Energi-, og Forsyningsministeriet, såfremt de eller anlæg de ejer leverer væsentlige tjenester til eller i seks eller flere EU-medlemsstater. I den forbindelse forventes, det at der fastsættes regler om, at der ved underretning skal ske oplysning om, hvilke væsentlige tjenester der leveres, og til hvilke EU-medlemsstater der leveres til eller i.

På baggrund af de regler, der forventes at blive fastsat, vil det i første omgang være op til de virksomheder, som opfylder kravene for kritiske enheder, at vurdere, om de leverer væsentlige tjenester til eller i seks eller flere EU-medlemsstater og derfor er omfattet af underretningspligten. En væsentlig tjeneste er defineret i den foreslåede § 3, stk. 1, nr. 29, som en tjeneste, der er afgørende for opretholdelsen af vitale samfundsmæssige funktioner, økonomiske aktiviteter, folkesundhed og offentlig sikkerhed eller miljøet.

Der kan ligeledes fastsættes nærmere regler om, hvad der er en væsentlig tjeneste inden for energisektoren da dette har betydning for udpegningen af kritiske enheder af særlig europæisk betydning. Såfremt en virksomhed er i tvivl om, hvorvidt de måtte levere væsentlige tjenester til eller i seks eller flere EU-medlemsstater, vil de kunne søge rådgivning hos den relevante kompetente myndighed.

Bestemmelsen gennemfører CER-direktivets artikel 17, stk. 2, 1. led, hvorefter medlemsstaterne sikrer, at en kritisk enhed efter den i direktivets artikel 6, stk. 3, omhandlede underretning oplyser sin kompetente myndighed, hvis den leverer væsentlige tjenester til eller i seks eller flere medlemsstater. I så fald sikrer medlemsstaterne, at den kritiske enhed oplyser sin kompetente myndighed om de væsentlige tjenester, den leverer til eller i disse medlemsstater, og om de medlemsstater, hvortil eller hvori den leverer sådanne væsentlige tjenester. Medlemsstaterne underretter uden unødigt ophold Kommissionen om identiteten af sådanne kritiske enheder samt om de oplysninger, de leverer i henhold til nærværende stykke.

Efter den foreslåede § 5, *stk. 4*, kan klima-, energi- og forsyningsministeren fastsætte nærmere regler om særlige forpligtelser for virksomheder, der er eller ejer kritiske enheder af særlig europæisk betydning.

Det forventes eksempelvis, at klima-, energi- og forsyningsministeren vil fastsætte regler om, at kritiske enheder af særlig europæisk betydning skal modtage rådgivende missioner. Det følger af CER-direktivets art. 18, stk. 5, at hver rådgivende mission består af eksperter fra den medlemsstat, hvor den kritiske enhed af særlig europæisk betydning er beliggende, eksperter fra de medlemsstater, hvortil eller hvori den væsentlige tjeneste leveres, og repræsentanter for Kommissionen. Disse medlemsstater kan foreslå kandidater til at deltage i en rådgivende mission. Kommissionen udvælger og udnævner efter en konsultation med den medlemsstat, som har identificeret en kritisk enhed af særlig europæisk betydning som en kritisk enhed i henhold til artikel 6, stk. 1, medlemmerne af hver rådgivende mission i overensstemmelse med deres faglige kapacitet og sikrer, hvor det er muligt, en geografisk afbalanceret repræsentation fra alle disse medlemsstater. Når det er nødvendigt, skal medlemmerne af den rådgivende mission have gyldig og passende sikkerhedsgodkendelse. Kommissionen afholder omkostningerne i forbindelse med deltagelse i rådgivende missioner.

Det forventes desuden, at der vil blive fastsat regler, om hvornår en kritisk enhed skal efterleve de særlige krav.

Bestemmelsen gennemfører CER-direktivets artikel 17, stk. 3, om at hvis Kommissionen på grundlag af de i direktivets artikel 17, stk. 2, omhandlede konsultationer konstaterer, at den pågældende kritiske enhed leverer væsentlige tjenester til eller i seks eller flere medlemsstater, så underretter Kommissionen gennem den kompetente myndighed den pågældende kritiske enhed om, at den anses for at være en kritisk enhed af særlig europæisk betydning, og oplyser den kritiske enhed om dens forpligtelser i henhold til direktivets kapitel om kritiske enheder af særlig europæisk betydning og om, fra hvilken dato disse forpligtelser finder anvendelse på den. Når Kommissionen således har oplyst den kompetente myndighed om sin beslutning om at betragte en kritisk enhed som en kritisk enhed af særlig europæisk betydning, videresender den kompetente myndighed uden unødigt ophold denne underretning til den pågældende kritiske enhed.

Bestemmelsen skal fortolkes i overensstemmelse af CER-direktivet og 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). Desuden skal bestemmelsen fortolkes i overensstemmelse med udviklingen på beredskabsområdet generelt, den geopolitiske udvikling og det dertilhørende trusselsbillede.

Bemyndigelsesbestemmelsen vil også sikre, at der ved større afhængighed mellem de forskellige systemer på tværs af EU kan stilles tidssvarende krav til kritiske enheder af særlig europæisk betydning.

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

Til § 6 [Kapitel 3]

Det følger af elforsyningslovens § 85 b og § 85 c, at visse virksomheder med bevilling eller tilladelse til produktion af el skal have et klassisk beredskab og et it-beredskab. Det samme gælder for Energinet og dennes helejede datterselskaber, samt virksomheder, der yder balancering af elsystemet.

Efter elforsyningslovens § 85 b, stk. 4, kan klima-, energi- og forsyningsministeren fastsætte regler om udførelse af tilsyn med virksomhedernes beredskabsarbejde, herunder om virksomhedernes fremsendelse af materiale som grundlag for tilsynet, om tilsynets beføjelser i forhold til virksomhederne og om klageadgang.

Elforsyningslovens § 85 c, stk. 5, indeholder en bemyndigelsesbestemmelse om at klima-, energi- og forsyningsministeren kan fastsætte nærmere regler om it-beredskabet, herunder regler om; 1) organisering af virksomhedens it-beredskab og evne til at modtage advarsler om trusler mod it-sikkerheden, 2) planlægning og beredskabsarbejde, som virksomhederne skal udføre for at modvirke trusler mod it-sikkerheden, herunder virksomhedernes pligt til at videregive oplysninger til Energinet og relevante myndigheder, 3) virksomhedernes risikostyring, herunder inddragelse af andre virksomheder i risikovurderinger, 4) tilmelding til en it-sikkerhedstjeneste, der yder varsler og informationer om it-sikkerhedstrusler og 5) Energinets varetagelse af overordnede, koordinerende planlægningsmæssige og operative opgaver vedrørende it-beredskab, jf. stk. 1.

Det følger af gasforsyningslovens § 15 a og § 15 b, at virksomheder som er bevillingspligtige efter gasforsyningslovens § 10, samt Energinet og

dennes helejede datterselskaber, som foretager gasforsyningsvirksomhed skal have et klassisk beredskab og et it-beredskab.

Efter gasforsyningslovens § 15, a, stk. 4, kan klima-, energi- og forsyningsministeren fastsætte regler om udførelse af tilsyn med virksomhedernes beredskabsarbejde, herunder om virksomhedernes fremsendelse af materiale som grundlag for tilsynet, om tilsynets beføjelser i forhold til virksomhederne og om klageadgang.

Gasforsyningslovens § 15 b, stk. 5, indeholder en bemyndigelsesbestemmelse om, at klima-, energi- og forsyningsministeren kan fastsætte nærmere regler om it-beredskabet, herunder regler om; 1) organisering af virksomhedens it-beredskab og evne til at modtage advarsler om trusler mod it-sikkerheden, 2) planlægning og beredskabsarbejde, som virksomhederne skal udføre for at modvirke trusler mod it-sikkerheden, herunder virksomhedernes pligt til at videregive oplysninger til Energinet og til klima-, energi- og forsyningsministeren, 3) virksomhedernes risikostyring, herunder inddragelse af andre virksomheder i risikovurderinger, 4) tilmelding til en tjeneste, der yder varsler og informationer om it-sikkerhedstrusler og 5) Energinets varetagelse af overordnede, koordinerende planlægningsmæssige og operative opgaver vedrørende it-beredskabet, jf. stk. 1.

For el- og gassektorerne er de nærmere regler for organisatorisk beredskab gennemført i bekendtgørelse om beredskab for elsektoren, bekendtgørelse om beredskab for naturgassektoren og bekendtgørelse om it-beredskab for el- og naturgassektorerne.

Ifølge § 5, stk. 1, 1. pkt., i bekendtgørelse om beredskab for elsektoren og bekendtgørelse om beredskab i naturgassektoren, skal virksomhederne udpege en beredskabskoordinator og et kontaktpunkt i krisesituationer (operationel kontakt). Virksomhederne skal desuden efter bekendtgørelsernes § 5, stk. 4, meddele kontaktoplysningerne på medarbejderne til Energinet, Energistyrelsen og det lokale politi. Virksomheder med klasse 1- og 2 anlæg, skal desuden have en sikringsansvarlig medarbejder, jf. § 5, stk. 1, 2. pkt.

Ifølge bekendtgørelse om it-beredskab i el- og naturgassektorerne § 6, stk. 1, skal virksomhederne have en it-beredskabsansvarlig. Virksomheder skal efter § 6, stk. 3, sikre at der sker koordination mellem det almene beredskab og it-beredskabet mindst fire gange årligt. Efter bekendtgørelsens § 7,

skal virksomhederne organiseres sådan, at det sikres de kan modtage it-sikkerhedsvarsler.

Virksomheder i el- og naturgassektoren skal udarbejde risiko- og sårbarhedsvurderinger inden for både klassisk og it-beredskab, jf. bekendtgørelse om beredskab i elsektoren § 6, skt. 1, bekendtgørelse om beredskab i naturgassektoren § 6, stk. 1 og bekendtgørelse om it-beredskab for el- og naturgassektoren § 10, stk. 1. Risiko- og sårbarhedsvurderinger skal indeholde alle relevante forhold, herunder virksomheders egne erfaringer fra øvelser og hændelser. Dertil indeholder bekendtgørelser formkrav til udarbejdelse af vurderingerne.

Virksomheder i el- og naturgassektoren skal udarbejde beredskabsplaner for både klassisk og it-beredskabet, jf. bekendtgørelse om beredskab i elsektoren § 7, skt. 1, bekendtgørelse om beredskab i naturgassektoren § 7, stk. 1 og bekendtgørelse om it-beredskab for el- og naturgassektoren § 14, stk. 1. Beredskabsplanerne skal baseres på virksomhedernes sårbarhedsvurderinger.

Beredskabsplanerne for det klassiske beredskab, skal indeholde følgende elementer; 1) aktivering, etablering og drift af krisehåndteringsorganisationen, 2) indhentning, behandling og fordeling af relevante informationer, 3) koordinering af aktørernes handlinger og ressourceanvendelse, 4) udsendelse af relevant, opdateret og samordnet ekstern information og 5) ydelse af en forsvarlig operativ indsats. Desuden skal planerne angive følgende konkrete forhold; 1) virksomhedens modtagelse af oplysninger om situationen, 2) virksomhedens kompetence- og beslutningsforhold af relevans for krisehåndteringen, 3) virksomhedens information af relevante myndigheder, samarbejdsparter m.fl. om situationen og krisehåndteringen, 4) virksomhedens muligheder for at indsætte yderligere ressourcer i krisehåndteringen i form af personale, materiel, støtte fra andre virksomheder i henhold til aftale og lign. herom og 5) virksomhedens planer for fremskaffelse af kritiske reservedele fra eget lager eller fra leverandører, jf. bekendtgørelse om beredskab for elsektorens § 7, stk. 2 og 3 og bekendtgørelse om beredskab for naturgassektorens § 7, stk. 2 og 3.

It-beredskabsplaner for virksomheder i el- og naturgassektorens, skal efter bekendtgørelse om it-beredskabs for el- og naturgassektorens § 14, stk. 2, indeholde følgende; 1) En identificering af forsyningskritiske it-systemer og afhængighed af andre systemer, 2) Beskrivelse af forebyggende foranstaltninger til at imødegå utilsigtede it-hændelser, herunder muligheder for

segmentering af it-infrastruktur og alternative driftsformer. Anvendes fjernadgang til forsyningskritisk it-systemer, skal beredskabsplanen indeholde en plan for, hvordan angreb på disse systemer opdages og håndteres, 3) Beskrivelse af intern ansvars- og rollefordeling under krisestyring, 4) Beskrivelse af intern ansvarsplacering af systemansvar for forsyningskritiske it-systemer, 5) Beskrivelse af kommunikation med Energinet eller Energistyrelsen og virksomhedens tilknyttede it-sikkerhedstjeneste, 6) Beskrivelse af procedurer for etablering af alternativ drift ved nedbrud på forsyningskritiske it-systemer, 7) Plan for genoprettelse af forsyningskritiske it-systemer, 8) Plan for dokumentation og opfølgning på hændelser, 9) Beskrivelse af den operative ansvarsfordeling mellem virksomheden og dennes samarbejdsparter.

Det følger af bekendtgørelse om beredskab i elsektoren §§ 20 og 21, stk. 1, bekendtgørelse om beredskab i naturgassektoren §§ 20 og 21, stk. 1, samt bekendtgørelse om it-beredskab for el- og naturgassektoren §§ 18 og § 19, stk. 1, at virksomhederne i el- og gassektoren løbende skal sikre at medarbejdere modtager den fornødne instruktion og uddannelse i klassisk beredskab samt it-beredskab. Det følger desuden af bestemmelserne, at virksomhederne skal afholde øvelser, med udgangspunkt i egene beredskabsplaner.

Bekendtgørelse om it-beredskab i el- og naturgassektoren § 24, stk. 2, tilsiger at virksomheder og skal etablere procedurer for leverandørers adgang til forsyningskritisk infrastruktur. Dette omfatter også fjernadgang, hvor procedurerne for fjernadgang til beskrives i kontrakter med leverandører.

Det følger af olieberedskabslovens § 16, stk. 1, at lagringspligtige virksomheder skal foretage nødvendig planlægning og træffe nødvendige foranstaltninger for, at sikre olieforsyningen i beredskabssituationer og andre ekstraordinære situationer. Efter § 16, stk. 3, kan klima-, energi- og forsyningsministeren fastsætte nærmere regler, om beredskabsplanlægningen efter stk. 1. De nærmere regler er gennemført i bekendtgørelse om beredskab for oliesektoren.

Ifølge bekendtgørelse om beredskab for oliesektorens § 5, skal beredskabsarbejdet baseres på alle risici, sådan ledelsen har et samlet risikobillede. Det følger desuden af § 6, i bekendtgørelsen, at organisationen skal indrettes, således det sikres, at der kan modtages varsler af teknisk karakter. Efter § 6, stk. 1, skal organisationen sikre, at der i akutte situationer kan kommunikeres med relevante samarbejdsparter, for at genoprette forsyningen.

Virksomheder og den centrale lagerenhed i oliesektoren skal udarbejde en vurdering af alle de risici og sårbarheder, der kan påvirke virksomhedens forsyning fra egne beredskabslagre i en beredskabssituation eller anden ekstraordinær situation, jf. bekendtgørelse om beredskab for oliesektorens § 8, stk. 1. Vurderinger skal indeholde alle relevante forhold, herunder egene erfaringer fra øvelser og hændelser, jf. § 8, stk. 2.

Virksomheder og den centrale lagenhed i oliesektoren skal udarbejde beredskabsplaner, som skal baseres på deres risiko- og sårbarhedsvurderinger, jf. bekendtgørelse om beredskab for oliesektorens § 11, stk. 1. Beredskabsplanerne skal indeholder; 1) En identificering af forsyningskritiske anlæg og processer, samt afhængighed af andre systemer uden for virksomheden, 2) Beskrivelse af forebyggende foranstaltninger til mulig iværksættelse under en beredskabssituation, herunder muligheder for alternative driftsformer, 3) Beskrivelse af intern ansvars- og rollefordeling under krisestyring, 4) Overordnet beskrivelse af intern beredskabsorganisering, der kan iværksættes for at håndtere en beredskabssituation, som f. eks. en krisestab eller skærpet driftsbemanding, 5) Beskrivelse af kommunikation med andre virksomheder, den centrale lagerenhed, Energistyrelsen og andre myndigheder i en akut krisesituation, 6) Beskrivelse af procedurer for etablering af alternativ drift ved nedbrud på forsyningskritiske anlæg og processer, 7) Plan for genoprettelse af forsyningskritisk infrastruktur og processer, 8) Plan for dokumentation og opfølgning på hændelser, 9) Beskrivelse af den operative ansvarsfordeling mellem virksomheden og dennes samarbejdsparter, jf. § 11, stk. 2.

Virksomheder og den centrale lagerenhed i oliesektoren skal sikre, at beredskabsmedarbejdere løbende modtager den fornødne instruktion, uddannelse og træning, jf. bekendtgørelse om beredskab i oliesektorens § 12.

Efter bekendtgørelse om beredskab for oliesektorens § 13, stk. 1, skal virksomheder og den centrale lagerenhed afholde beredskabsøvelser med udgangspunkt i egne beredskabsplaner. Der skal desuden udarbejdes en øvelsesplan for en treårig periode, jf. § 13, skt. 2.

Bekendtgørelse om beredskab for oliesektorens § 17, stk. 2, tilsiger at virksomheder og den centrale lagerenhed skal etablere procedurer for leverandørers adgang til forsyningskritisk infrastruktur. Dette omfatter også fjernadgang, hvor procedurerne for fjernadgang til beskrives i kontrakter med leverandører.

Det foreslås i *§ 6, stk. 1*, at virksomheder, skal foretage nødvendig beredskabsplanlægning og gennemføre passende organisatoriske foranstaltninger for at beskytte leveringen af deres tjenester og sikre effektiv genoprettelse af deres tjenester.

Med de foreslåede § 6, stk. 1 rammesættes de overordnede krav til virksomhedens modstandsdygtighed og etableringen af et organisatorisk beredskab. De nærmere krav detaljeres i det foreslåede § 6, stk. 2, hvorefter klima-, energi- og forsyningsministeren fastsætter nærmere regler om det organisatoriske beredskab. Der vil således i bekendtgørelsesform blive stillet konkretiserede krav til den planlægning og de foranstaltninger, som virksomheder skal træffe i medfør af den foreslåede bestemmelse i stk. 1. Der henvises til bemærkningerne til stk. 2.

De foreslåede bestemmelser viderefører i vidt omfang de gældende bestemmelser om organisatorisk beredskab i den gældende elforsyningslov §§ 85b, stk.1 og 85, stk. c, stk. 1 samt i den gældende gasforsyningslov §§ 15 a og b, som udmøntet i gældende beredskabsregulering for el og gassektoren, dog skærpes kravene på en række områder.

Det foreslås i § 6, *stk. 2*, at indføre hjemmel til at klima-, energi- og forsyningsministeren fastsætter efter forhandling med forsvarsministeren nærmere regler om organisatorisk beredskab. Bemyndigelsen forventes udmøntet i en bekendtgørelse, der blandt andet fastsætter nærmere regler for de i nr. 1 – 12 nævnte elementer af organisatorisk beredskab, som beskrevet nedenfor. Ved at bemyndige klima-, energi- og forsyningsministeren til at fastsætte sådanne regler, vil nye trusler kunne imødegås og relevante tidsvarende nye rammer for de organisatoriske kunne indarbejdes i kravene til virksomhedernes organisatoriske beredskabsarbejde smidigt, hvis reglerne udstedes i bekendtgørelse.

Det foreslås i § 6, stk. 2, *nr. 1*, at klima-, energi- og forsyningsministeren fastsætter nærmere regler om ledelsesansvar, herunder krav om godkendelse af virksomhedens risiko- og sårbarhedsvurdering samt beredskabsplaner, tilsynsrapporter og leverandørkontrakter.

Ved de nærmere regler om ledelsesansvar, forventes det, at vil der blive stillet krav til, at ledelsen aktivt forholder sig i virksomhedens beredskab og niveau af modstandsdygtighed. På baggrund af bestemmelsen, forventes der fastsat nærmere regler om, at den enkelte virksomheds ledelse kon-

tinuerligt godkender virksomhedens beredskabsplaner og risiko- og sårbarhedsvurderinger, herunder bl.a. godkender foranstaltninger for styring af cybersikkerhedsrisici. Den foreslåede ordning vil medføre, at virksomhedens ledelse har et samlet og ajourført billede af beredskabet samt kendte og mulige risici mod produktion, forsyning eller levering af virksomhedens tjenester.

Den foreslåede bestemmelse gennemfører NIS 2-direktivets artikel 20, stk. 1, hvorefter medlemsstater sikrer, at de væsentlige og vigtige enheders ledelsesorganer godkender de foranstaltninger til styring af cybersikkerhedsrisici, som disse enheder har truffet og fører tilsyn med gennemførelsen.

I den foreslåede bestemmelse lægges der op til, at ledelsen både gøres ansvarlig for foranstaltninger til styring af organisatorisk sikkerhed, fysisk sikring og cybersikkerhed. Dette er en udvidelse af NIS 2-direktivets artikel 20, idet denne udelukkende omhandler styring i forhold til cybersikkerhedsrisici. Denne udvidelse i forhold til, hvad der er indeholdt i NIS 2-direktivet foreslås ud fra en betragtning om, at konsekvensen ved afbrud i leveringen af virksomhedens tjeneste og omkostninger ved genopretning er lige kritiske, uagtet om dette skyldes organisatoriske forhold, manglende fysisk sikring eller cybersikkerhed. Endvidere er der indbyrdes forbindelser mellem organisatorisk beredskab, fysisk sikring og cybersikkerhed, og det kan i praksis være svært at adskille risici inden for disse områder.

Klima-, Energi- og Forsyningsministeren forventes endvidere på baggrund af bestemmelsen, at fastsætte nærmere regler, der præciserer, at ledelsen har ansvar for at inddrage sikkerhedshensyn i forbindelse med beslutninger der vedrører leverandørkontrakter. Ved leverandørkontrakter forstås i denne sammenhæng nye projekter og leverandør- samt serviceaftaler.

Med den foreslåede ordning vil det sikres, at virksomheder vil skulle forholde sig til trusler og sårbarheder i forbindelse med f.eks. anlægsprojekter eller systemerhvervelser, som har mulighed for at påvirke leveringen af virksomhedens tjenester. Det forventes desuden, at der fastsættes nærmere regler om, at ledelsen skal tage stilling til passende foranstaltninger, der skal mitigere identificerede risici forbundet med de konkrete projekt eller erhvervelse.

Det følger af den foreslåede § 6, stk. 2, *nr. 2*, at klima-, energi- og forsyningsministeren fastsætter nærmere regler om, at ledelsesorganer tilegner

sig viden og kundskaber inden for risiko- og sårbarhedsstyring. Det forventes på baggrund af den foreslåede bestemmelse, at der vil blive fastsat nærmere regler om, at ledelsen opbygger viden og kompetencer til at træffe kvalificerede beslutninger vedrørende cybersikkerhed og beredskab. Den foreslåede ordning vil medføre, at det vil være ledelsens ansvar at etablere en sikkerhedskultur og sikre uddannelse i hele organisationen.

Den foreslåede bestemmelse gennemfører dele af NIS 2-direktivets artikel 20, stk. 2, hvorefter medlemmerne af væsentlige og vigtige enheders ledelsesorganer er forpligtet til at følge kurser, der gør ledelsen i stand til at identificere risici og vurdere metoderne til styring af cybersikkerhedsrisici. Den foreslåede bestemmelse lægges der dog op til, at ledelsen både skal kunne gøres i stand til at identificere risici forbundet med organisatorisk sikkerhed, fysisk sikring og cybersikkerhed. Dette er en udvidelse af NIS 2-direktivets artikel 20, idet denne udelukkende omhandler uddannelse og kurser vedrørende styring i forhold til cybersikkerhedsrisici.

Det følger af den foreslåede § 6, stk. 2, *nr. 3*, at klima-, energi- og forsyningsministeren fastsætter nærmere regler om identifikations- og adgangskontrolpolitikker for beskyttelse mod uautoriseret adgang.

Den foreslåede bestemmelse gennemfører dele af CER-direktivets artikel 13, stk. 1, litra b, hvorefter kritiske enheder skal sikre tilstrækkelig fysisk beskyttelse af deres lokaler og kritiske infrastruktur under hensyntagen til f.eks. adgangskontrol. Derudover gennemfører bestemmelsen artikel 13, stk. 1, litra e, hvorefter kritiske enheder skal sikre passende medarbejdersikkerhedsstyring såsom fastlæggelse af adgangsrettigheder til lokaler, kritisk infrastruktur og følsomme oplysninger. Desuden gennemfører den foreslåede bestemmelse NIS 2-direktivets artikel 21, stk. 2, litra i, hvorefter vigtige og væsentlige enheder skal træffe foranstaltninger om bl.a. personalesikkerhed og adgangskontrolpolitikker.

Det forventes på baggrund af den foreslåede bestemmelse, at der fastsættes nærmere regler om, at virksomhederne skal have politikker og procedurer for identifikation af personel med adgang til virksomhedens anlæg. Det forventes også, at der fastsættes regler for virksomheden skal have politikker og procedurer for at identificere fysiske områder og inddele adgang til disse områder i zoner, som del af en samlet tilgang til fysisk sikring med henblik på at kunne identificere og verificere hvilke personer, der må opholde sig i og omkring virksomhedens anlæg.

Ministeren forventes på endvidere baggrund af bestemmelsen, at fastsætte nærmere regler om, at virksomheden skal kunne etablere adgangsstyring baseret på roller og arbejdsbetinget behov med henblik på at sikre klart definerede regler for, hvilke medarbejdere eller medarbejdergrupper, der kan tilgå forskellige dele af et anlæg eller net- og informationssystemer. På den baggrund forventes, der eksempelvis fastsat nærmere regler om, at virksomhederne skal have procedurer for hvordan adgange til kritiske anlæg og net- og informationssystemer tildeles, ændres og lukkes for både virksomhedens egne medarbejdere såvel som for gæster, konsulenter, eksterne samarbejdspartnere og leverandører.

Det følger af den foreslåede § 6 stk. 2, *nr. 4*, at klima-, energi- og forsyningsministeren fastsætter nærmere regler om udpegelse af personer til at varetage specifikke beredskabsroller.

Den foreslåede bestemmelse gennemfører CER-direktivets artikel 13, stk. 3, hvorefter medlemsstaterne sikrer, at hver kritisk enhed udpeger en forbindelsesofficer eller tilsvarende som kontaktpunkt for de kompetente myndigheder.

Som en udvidelse af CER-direktivets krav foreslås det med dette lovforslag, at der også kan fastsættes regler om roller vedrørende cyberberedskabet.

Den nødvendige beredskabsplanlægning kræver, at der er klart definerede roller og ansvar for de involverede. Det forventes, at gældende ret for udpegelsen af beredskabsroller videreføres i vidt omfang. Dog ændres betegnelsen it-beredskabsansvarlig til cyberberedskabskoordinator, som er et kontaktpunkt for kommunikation med myndigheder. Dette er ikke den samme rolle som det operationelle kontaktpunkt, som forventes at være døgnbemandet. På baggrund af bestemmelsen forventes det således, at virksomhederne bl.a. ville skulle udpege en beredskabskoordinator, en cyberberedskabskoordinator, et operationelt kontaktpunkt og en eller flere sikringsansvarlige medarbejdere.

Det følger af den foreslåede § 6, stk. 2, *nr. 5*, at klima-, energi- og forsyningsministeren fastsætter nærmere regler om politikker for informationssystemsikkerhed.

Den foreslåede bestemmelse gennemfører dele af NIS 2-direktivets artikel 21, stk. 2, litra a, hvorefter vigtige og væsentlige enheder skal have politikker for informationssystemsikkerhed.

Det forventes på baggrund af den foreslåede bestemmelse, at der fastsættes nærmere regler om at virksomheden som del af organisatorisk modstandsdygtighed skal udarbejde en informationssystemsikkerhedspolitik, der sætter en overordnet ramme for beskyttelse af virksomhedens informationer, herunder at virksomheden selv har forhold sig til relevante aktiviteter for beskyttelse af anvendte net- og informationssystemer.

Det foreslås, at der differentieres i hvilke virksomheder, der skal efterleve den foreslåede § 6, stk. 2, nr. 5, således at de mere forsyningskritiske virksomheder skal følge flere elementer af kravene. Dette er ud fra en betragtning om, at en forstyrrelse af disse virksomheders tjenester vil have større betydning for samfundet samt ud fra en betragtning om, at der bør være proportionalitet mellem sikkerhedseffekten og omkostningen ved kravene.

Det følger af den foreslåede § 6, stk. 2, *nr. 6*, at klima-, energi- og forsyningsministeren fastsætter nærmere regler om politikker for og udarbejdelse af risiko- og sårbarhedsvurderinger, som omfatter nyindkøb, projekter og etablering af net- og informationssystemer og anlæg

Den foreslåede bestemmelse gennemfører dele af NIS 2-direktivets artikel 21, stk. 2, litra a, hvorefter vigtige og væsentlige enheder skal have politikker for politikker for risikoanalyse. Desuden gennemfører den foreslåede bestemmelse CER-direktivets artikel 12, stk. 1-2, hvorefter kritiske enheder foretager en risikovurdering for at vurdere alle relevante risici, der kunne forstyrre leveringen af deres væsentlige tjenester.

Som en udvidelse af NIS 2-direktivets krav foreslås det med dette lovforslag, at der også fastsættes regler om, at virksomheder også skal foretage risiko- og sårbarhedsvurderinger under hele aktivets livscyklus såsom i forbindelse med indkøb, projekter og nyetableringer.

Ministeren forventes på endvidere baggrund af bestemmelsen, at fastsætte nærmere regler om, at virksomheden skal udarbejde risiko- og sårbarhedsvurderinger, som identificerer og vurderer risici og sårbarheder i forhold til virksomhedens kontinuitet.

Det forventes endvidere, at der fastsættes nærmere regler om, at risiko- og sårbarhedsvurderingerne og handlingsplanerne skal gennemgås med fast interval eller når nye risici, trusler eller sårbarheder erkendes samt ved væsentlige ændringer af virksomhedens organisation, kritiske systemer eller infrastruktur eller ved ændringer i trusselsbilledet. Det foreslås samtidig, at vurderingen af cybersikkerhedsrisici, organisatoriske risici og fysiske risici

kobles sammen, ved at virksomhedernes opdateringer af deres risiko- og sårbarhedsvurderinger af henholdsvis virksomhedens cybersikkerhed og fysiske sikring følger samme kadence for udarbejdelse og indsendelse til Energistyrelsen.

De foreslåede bestemmelser viderefører i vidt omfang de gældende ret for udarbejdelse af risiko- og sårbarhedsvurdering. Det forventes således, at der fastsættes nærmere regler om, at virksomhederne skal udarbejde en vurdering af virksomhedens risici og sårbarheder på baggrund af risiko- og sårbarhedsscenarier, som Energistyrelsen udarbejder.

Som noget nyt forventes der fastsat nærmere regler om at som led i udarbejdelsen af risiko- og sårbarhedsvurderinger, at virksomhederne skal udarbejde en politik og have en proces for risikostyring, der skal identificere og vurdere de væsentligste risici for virksomhedens organisation, kritiske net- og informationssystemer og infrastruktur med henblik på opretholdelsen af leveringen af deres tjeneste.

På baggrund af bestemmelsen forventes der udstedt nærmere regler om, at virksomhedernes processer for risikostyring skal forholde sig til de væsentligste trusler og sårbarheder og forankres i organisationen således at virksomhedsledelsen forholder sig til både processerne for risikostyring, de identificerede risici, samt de foranstaltninger til styring af risici, som virksomheden iværksætter på baggrund heraf.

Det foreslås, at der differentieres i hvilke virksomheder, der skal efterleve den foreslåede § 6, stk. 2, nr. 6, således at de mere forsyningskritiske virksomheder skal følge flere elementer af kravene.

Dette er ud fra en betragtning om, at en forstyrrelse af disse virksomheders tjenester vil have større betydning for samfundet samt ud fra en betragtning om, at der bør være proportionalitet mellem sikkerhedseffekten og omkostningen ved kravene.

Det følger af den foreslåede § 6, stk. 2, *nr. 7* at klima-, energi- og forsyningsministeren fastsætter nærmere regler om forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem virksomheden og dens direkte leverandører eller tjenesteudbydere.

Den foreslåede bestemmelse gennemfører NIS 2-direktivets artikel 21, stk. 2, litra d, hvorefter væsentlige og vigtige enheder træffer foranstaltninger

for forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem den enkelte enhed og dens direkte leverandører eller tjenesteudbydere. Den foreslåede bestemmelse gennemfører desuden NIS 2-direktivets artikel 21, stk. 2, hvorefter væsentlige og vigtige enheder tager hensyn til de sårbarheder, der er specifikke for hver direkte leverandør og tjenesteudbyder.

På baggrund af den foreslåede bestemmelse fastsætter ministeren nærmere regler om, at virksomhederne skal etablere den nødvendige leverandørstyring, herunder at virksomhederne skal iværksætte sikkerhedsrelaterede foranstaltninger til styring af risici i virksomhedens leverandørkæder.

Den foreslåede bestemmelse vil indebære, at virksomhederne skal sikre, at leverandører, der varetager opgaver i relation til anlæg, komponenter og net- og informationssystemer med betydning for leveringen af tjenesten, overholder samme krav for opretholdelse af virksomhedens modstandsdygtighed, som virksomheden er underlagt efter den foreslåede lov. Det følger heraf, at virksomhederne skal have politikker og procedurer for kontrol af, at leverandørerne efterlever kravene og opretholder det nødvendige sikkerhedsniveau i forbindelse med udførelsen af opgaven.

Som følge af bestemmelsen fastsætter ministeren nærmere regler om, at virksomhederne skal vurdere og håndtere de risici, der er forbundet med indgåelse af leverandøraftaler. Dette vil blandt andet indebære, at virksomhederne inden indgåelse af en aftale samt løbende skal tage stilling til sikkerhedsrisici forbundet med kritikaliteten af opgaven eller leverancen, hvorvidt der sker væsentlige forandringer hos leverandøren der kan påvirke leverancen, leverandørernes villighed til at efterleve kravene i den foreslåede lov og det aktuelle trusselsbillede.

Det foreslås derudover, at ministeren kan fastsætte nærmere regler om, at leverandører, som varetager opgaver i relation til anlæg, komponenter og net- og informationssystemer eller leverandører af net- og informationssystemer med betydning for leveringen af tjenesten, deltager i relevante dele af virksomhedens beredskabsplanlægning. Dette indebærer bl.a., at ministeren kan fastsætte nærmere regler om, at leverandørerne deltager i virksomhedens arbejde med risiko- og sårbarhedsvurderinger samt øvelser, der træner de dele af beredskabet, hvor leverandørerne har betydning for opretholdelse af leveringen af virksomhedens tjenester.

Det følger af den foreslåede § 6, stk. 2, *nr. 8*, at klima-, energi- og forsyningsministeren fastsætter nærmere regler om beredskabsplaner og beredskabsplanlægning for håndtering af hændelser.

Den foreslåede bestemmelse gennemfører CER-direktivets artikel 13, stk. 2, hvorefter medlemsstaterne sikrer, at kritiske enheder har indført og anvender en plan for modstandsdygtighed eller et eller flere tilsvarende dokumenter. Derudover gennemfører den foreslåede bestemmelse elementer af NIS 2-direktivets artikel 21, stk. 2, litra b og c, hvorefter vigtige og væsentlige enheder skal træffe foranstaltninger, der omfatter håndtering af hændelser, driftskontinuitet og krisestyring.

Det foreslås, at gældende ret for udarbejdelse og indhold af beredskabsplaner i vidt omfang videreføres. Det forventes at der fastættes nærmere regler om, at beredskabsplanerne bl.a. skal beskrive virksomhedens krisehåndtering, hvordan virksomhedens krisehåndteringsorganisation aktiveres, etableres og driftes, og hvordan der koordineres og udsendes information internt og eksternt i virksomheden. Desuden foreslås det, at virksomhederne skal have metoder til at sikre, at virksomhederne overholder deres underretnings- og rapporteringsforpligtelser i forbindelse med en hændelse. Beredskabsplanen skal kunne bruges som en operativ vejledning, når en hændelse bliver varslet eller opstår.

Det foreslås *i* § 6 stk. 2, *nr. 9*, at klima-, energi- og forsyningsministeren fastsætter nærmere regler om øvelsesplanlægning, herunder afholdelse af øvelser og træning af beredskabsforanstaltninger.

Den foreslåede bestemmelse gennemfører CER-direktivets artikel 13, stk. 1, litra f, hvorefter medlemsstaterne sikrer, at kritiske enheder øger bevidstheden blandt det relevante personale under hensyntagen til øvelser.

NIS 2-direktivet stiller ikke krav om, at vigtige og væsentlige enheder afholder øvelser. Den foreslåede bestemmelse går dermed videre end NIS 2-direktivet, idet det foreslås, at der også fastsættes regler om, at virksomheder også skal afholde øvelser, der træner cyberberedskabet.

Ministeren forventes på endvidere baggrund af bestemmelsen, at fastsætte nærmere regler om, at det at virksomhederne skal udarbejde en øvelsesplan og afholde øvelser efter nærmere fastsatte kadencer, med udgangspunkt i virksomhedens beredskabsplaner. Det forventes endvidere, at der

fastsættes nærmere regler om revidering af øvelsesplanen, eksempelvis mindst en gang om året og i forbindelse med særlige sårbarheder eller væsentlige ændringer i virksomhedens beredskab. Der forventes også fastsat nærmere regler om, at en evaluering af en hændelse kan godkendes som en øvelse på øvelsesplanen, hvis hændelsen har afprøvet konkrete forhold i virksomhedens beredskab og vurderes at have samme værdi, som en øvelse.

Det forventes endelig, at der fastsættes nærmere regler om at virksomheden løbende skal sikre at medarbejdere modtager den fornødne instruktion og uddannelse i beredskab, herunder cybersikkerhed samt, at der stilles krav om at virksomheden gennemføre awareness-tiltag om cybersikkerhed efter en nærmere fastsat kadence.

Den foreslåede bestemmelse viderefører i vidt omfang de gældende ret for øvelsesplanlægning, herunder afholdelse af øvelser og træning af beredskabsforanstaltninger, dog forventes det som noget nyt, at der vil bliver fastsat nærmere regler om indholdet i øvelsesplanerne, herunder elementer i beredskabet, som skal øves, eksempelvis krisestyring, mobilisering af ekstra ressourcer og materialer, henholdsvis intern og ekstern kommunikation, genopretning af forsyning eller sikring af fortsat drift og iværksættelse af foranstaltninger i henhold til nyt sektorberedskabsniveau.

Det følger af den foreslåede § 6, stk. 2, *nr. 10*, at klima-, energi- og forsyningsministeren fastsætter nærmere regler om beredskabstræning, cybersikkerhedsadfærd- og sikkerhedsuddannelse af ansatte i virksomheden.

Den foreslåede bestemmelse gennemfører CER-direktivets artikel 13, stk. 1, litra f, hvorefter medlemsstaterne sikrer, at kritiske enheder øger bevidstheden blandt det relevante personale under hensyntagen til bl.a. uddannelseskurser og informationsmateriale.

Desuden gennemfører den foreslåede bestemmelse NIS 2-direktivets artikel 20, stk. 2, hvorefter ledelsen i vigtige og væsentlige enheder skal tilskynde deres ansatte at følge kurser, således at de opnår tilstrækkelige kundskaber og færdigheder til at kunne identificere risici og vurdere metoderne til styring af cybersikkerhedsrisici. Bestemmelsen gennemfører også NIS 2-direktivets artikel 21, stk. 2, litra g, hvorefter vigtige og væsentlige enheder træffer foranstaltninger om grundlæggende cyberhygiejnepraksisser og cybersikkerhedsuddannelse. Det foreslås, at virksomhederne stilles

krav om at øge sikkerhedsbevidstheden hos medarbejderne. Den foreslåede bestemmelse vil medføre, at de medarbejdere, der deltager i virksomhedens arbejde med beredskabsplanlægning, fysisk sikring og sikkerheden i net- og informationssystemer, skal have tilstrækkelige færdigheder samt viden til at kunne varetage deres opgaver.

Det forventes, at der vil blive fastsat nærmere regler om,at medarbejdere har kompetence til at agere sikkerhedsmæssigt forsvarligt i de opgaver, der skal udføres jf. § 6, stk. 2, nr. 1. Den gældende regulering af el- og gassektorerne, som stiller krav om at virksomhederne gennemfører awareness-tiltag om it-sikkerhed, forventes udvidet med krav om at disse tiltag kan omfatte både cybersikkerhed fx sikker konfigurering af- og test af it-udstyr, netværk og infrastruktur, cloud-løsninger eller identitets- og adgangsstyring, såvel som årvågenhed i forhold til fx spionage, uautoriseret adgang, utilsigtet informationsdeling og andre forhold, der kan kompromittere forsyningssikkerheden. De pågældende tiltag skal baseres på medarbejderens funktion i virksomheden. Den foreslåede ordning vil sikre, at også medarbejdere med adgang til og på kritiske anlæg og lokationer, herunder daglig stationsadgang, sikres tilstrækkelig viden og sikkerhedsbevidsthed.

Ifølge den foreslåede bestemmelse kan dette indebære, at disse medarbejdere i relevant omfang skal følge uddannelsesforløb. Den foreslåede bestemmelse vil derudover medføre, at virksomheden skal gennemføre awareness-tiltag om fysisk sikring, cybersikkerhed og beredskab, der øger den organisatoriske modstandsdygtighed på tværs af virksomheden.

Det følger af den foreslåede § 6, stk. 2, *nr. 11*, at klima-, energi- og forsyningsministeren fastsætter nærmere regler om kapacitet til at modtage og videreformidle advarsler om trusler.

Den foreslåede bestemmelse gennemfører elementer af NIS 2-direktivets artikel 21, stk. 2, litra e, hvorefter væsentlige og vigtige enheder træffer foranstaltninger til håndtering og offentliggørelse af sårbarheder.

På den baggrund forventes der eksempelvis fastsat nærmere regler om, at virksomheden skal indrette cyberberedskabet på en måde, der sikrer operationel koordinering af varsler og alarmer på tværs af virksomhedens forretningsområder og aktiver. Det forventes blandt andet at indbefatte krav om, at virksomheden skal have metoder til at identificere sårbarheder og skal

organisere et beredskab med evne til at modtage og videreformidle advarsler om trusler og sårbarheder, der potentielt kan påvirke virksomhedens evne til at levere deres tjeneste.

Med den foreslåede ordning sikres det, at virksomheden både vil kunne modtage varsler fra samarbejdspartnere, operatører eller øvrige aktører og videreformidle sådanne data og information, som en mitigerende foranstaltning for tjenesten, samt videregive oplysninger til klima-, energi- og forsyningsministeren, andre myndigheder og relevante samarbejdspartnere, såsom leverandører og kunder uden unødig forsinkelse.

Det følger af den foreslåede § 6, stk. 2, *nr. 12*, at klima-, energi- og forsyningsministeren fastsætter nærmere regler om tilmelding til en it-sikkerhedstjeneste.

Den foreslåede bestemmelse gennemfører elementer af NIS 2-direktivets artikel 21, stk. 2, litra e, hvorefter væsentlige og vigtige enheder træffer foranstaltninger til sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer, herunder foranstaltninger til håndtering og offentliggørelse af sårbarheder. Desuden gennemfører den foreslåede bestemmelse NIS 2-direktivets artikel 21, stk. 2, litra c, hvorefter væsentlige og vigtige enheder træffer foranstaltninger til bl.a. reetablering og krisestyring. Den foreslåede bestemmelse går videre end NIS 2-direktivet, idet der direkte stilles krav om, at virksomhederne skal tilmeldes en it-sikkerhedstjeneste.

Det forventes på baggrund af den foreslåede bestemmelse, at fastsætte nærmere regler om at virksomheder i energisektoren indgår aftale om at være tilmeldt en it-sikkerhedstjeneste. Virksomheden skal sikre sig at være tilmeldt en it-sikkerhedstjeneste, der yder vejledning om vurdering og mitigering af sårbarheder. Den it-sikkerhedstjeneste skal endvidere give informationer og varsle om relevante it-sikkerhedstrusler. Supplerende til eksisterende krav foreslås det at virksomhedens proaktive indsats skal omfatte viden om trusler baseret på globale informationer fra anerkendte kilder, såsom abonnementer på cyber-trusselsfeed, der er leveret af globale aktører inden for cybersikkerhed. Den foreslåede bemyndigelsesbestemmelse vil også medføre, at der kan fastsættes regler om, at virksomheden skal være tilmeldt en reaktiv it-sikkerhedstjeneste, der bistår virksomheden ved nedbrud eller angreb på it-systemer, herunder assistance til akut skadesbegrænsning, bevisindsamling og reetablering i akutte sikkerhedsmæs-

sige situationer. Information fra it-sikkerhedstjenesten skal kunne videreformidles til andre virksomheder i energisektoren uden forsinkelse, såfremt disse oplysninger vurderes at have betydning for leveringen af andre virksomheders tjenester.

Til § 7 [Kapitel 3]

Det følger af elforsyningslovens § 85 b, at visse virksomheder med bevilling eller tilladelse til produktion eller distribution af elektricitet skal have et klassisk beredskab. Det samme gælder for Energinet og dennes helejede datterselskaber.

Efter elforsyningslovens § 85 b, stk. 4, kan klima-, energi- og forsyningsministeren fastsætte regler om udførelse af tilsyn med virksomhedernes beredskabsarbejde, herunder om virksomhedernes fremsendelse af materiale som grundlag for tilsynet, om tilsynets beføjelser i forhold til virksomhederne og om klageadgang. De nærmere regler er gennemført i bekendtgørelse om beredskab for elsektoren.

Det følger af gasforsyningslovens § 15 a, at virksomheder som er bevillingspligtige efter gasforsyningslovens § 10, samt Energinet og dennes helejede datterselskaber, som foretager gasforsyningsvirksomhed skal have et klassisk beredskab.

Efter gasforsyningslovens § 15, a, stk. 4, kan klima-, energi- og forsyningsministeren fastsætte regler om udførelse af tilsyn med virksomhedernes beredskabsarbejde, herunder om virksomhedernes fremsendelse af materiale som grundlag for tilsynet, om tilsynets beføjelser i forhold til virksomhederne og om klageadgang. De nærmere regler er gennemført i bekendtgørelse om beredskab for naturgassektoren.

Efter bekendtgørelse om beredskab for elsektoren og bekendtgørelse for beredskab for naturgassektorens § 12, stk. 1, skal virksomhederne udarbejde sikringsplaner, som omfatter kortmateriale, oversigt over anlægs sårbarheder, m.v. Virksomhederne skal desuden efter bekendtgørelsernes § 13, stk. 1, sikre 1) at anlæg har lav sårbarhed over for funktionssvigt af offentligt udbudte net og tjenester for elektronisk kommunikation, 2) at anlæg har lav sårbarhed over for funktionssvigt af væsentlige it-systemer, og

3) at anlæg har nødstrømsforsyning, som i tilfælde af strømafbrydelse sikrer anlæggets funktionalitet i perioden frem til strømforsyningens reetablering.

Det gælder desuden at ubemandede anlæg i klasse 1, skal sikres mod uautoriseret adgang gennem etablering af mekaniske og elektroniske sikrings- og overvågningsforanstaltninger, jf. bekendtgørelsernes § 13, stk. 2. Virksomheder skal desuden etablere et system for styret adgangskontrol til klasse anlæg, jf. bekendtgørelsernes § 13, stk. 3. Der skal regelmæssigt og mindst hver måned, føres kontrol med at den fysiske sikring af klasse 1 anlæg, hvilket virksomhederne skal føre en log over, jf. bekendtgørelsernes § 13, stk. 4.

Det følger af olieberedskabslovens § 16, stk. 1, at lagringspligtige virksomheder skal foretage nødvendig planlægning og træffe nødvendige foranstaltninger for, at sikre olieforsyningen i beredskabssituationer og andre ekstraordinære situationer. Efter § 16, stk. 3, kan klima-, energi- og forsyningsministeren fastsætte nærmere regler, om beredskabsplanlægningen efter stk. 1.

Ifølge bekendtgørelse om beredskab for oliesektorens § 16, stk. 1, skal virksomhederne og den centrale lagerenhed sikre, at forsyningskritiske anlæg beskyttes i forhold til deres kritikalitet. Virksomhederne skal desuden, sikre forsyningskritiske anlæg mod uautoriseret adgang, jf. § 16, stk. 2.

Det følger af den foreslåede § 7, *stk. 1*, at virksomhederne skal sikre, at der implementeres passende foranstaltninger, der opretholder nødvendig fysisk sikring af lokationer og anlæg, der bruges til at levere virksomhedens tjenester, eller hvorfra drift af net- og informationssystemer finder sted. Dette vil indebære, at virksomhederne etablerer den nødvendige fysiske sikring af net- og informationssystemer, som bruges til eller understøtter leveringen af tjenesten. Efter den foreslåede bestemmelse, skal virksomhederne beskytte anlæg, lokationer og net- og informationssystemer i forhold til både tilsigtede og utilsigtede hændelser.

Det foreslås i § 7, *stk. 2*, at indføre hjemmel til at klima-, energi- og forsyningsministeren fastsætter nærmere regler om fysisk sikring. Bemyndigelsen forventes udmøntet i en bekendtgørelse, der blandt andet fastsætter nærmere regler for de i nr. 1 – 5 nævnte elementer af fysisk sikring, som beskrevet nedenfor. Ved at bemyndige klima-, energi- og forsyningsministeren til at fastsætte sådanne regler, vil nye trusler kumme imødegås og

relevante tidsvarende nye rammer for fysisk sikring kunne indarbejdes i kravene til virksomhedernes beredskabsarbejde med fysisk sikring hurtigere, hvis reglerne udstedes i bekendtgørelsesform end hvis de fastsættes ved lov.

Det foreslås *i* § 7 stk. 2, *nr. 1*, at klima-, energi- og forsyningsministeren kan fastsætte nærmere regler om, at virksomhederne skal forhindre hændelser i at indtræffe under behørig hensyntagen til katastroferisikoreduktions- og klimatilpasningsforanstaltninger.

Den foreslåede bestemmelse gennemfører CER-direktivets artikel 13, stk. 1, litra a, hvorefter medlemsstaterne sikrer, at kritiske enheder forhindrer hændelser i at indtræffe under behørig hensyntagen til katastroferisikoreduktions- og klimatilpasningsforanstaltninger.

Denne bestemmelse forventes at medføre, at virksomhederne skal identificere deres kritiske anlæg og net- og informationssystemer. Desuden skal virksomhederne have overblik over sårbarheder i forhold til naturkatastrofer og ekstreme vejrforhold, herunder at virksomhederne løbende forholder sig til risici, der er forbundet med at intensiteten og hyppigheden af ekstreme vejrforhold stiger i takt med klimaforandringerne. Det foreslås desuden, at virksomhederne skal iværksætte foranstaltninger, der tager højde for vurderingen af de risici, der er forbundet med naturkatastrofer og ekstreme vejrforhold, og som minimerer risikoen for, at disse hændelser kan forstyrre leveringen af tjenesten. Den foreslåede bestemmelse indebærer også, at virksomhederne skal tage højde for klimatilpasningsforanstaltninger i beslutninger vedrørende hvor og hvordan anlæg og net- og informationssystemer etableres og driftes. Ligeledes foreslås det med den nævnte bestemmelse, at beredskabsplanlægningen i relevant omfang skal vurdere muligheder for genopretning af leveringen af tjenesten i tilfælde af større katastrofer og ekstreme vejrforhold.

Ifølge den foreslåede § 7, stk. 2, *nr. 2*, kan klima-, energi- og forsyningsministeren fastsætte nærmere regler om, at virksomhederne skal etablere foranstaltninger til overvågning, detektion og reaktion i forbindelse med uautoriseret adgang til og på anlæg og lokationer.

Den foreslåede bestemmelse vil gennemføre dele CER-direktivets artikel 13, stk. 1, litra b, hvorefter kritiske enheder træffer foranstaltninger til fysisk beskyttelse af deres lokaler og kritiske infrastruktur under hensyntagen til værktøjer og rutiner til overvågning af perimetre, detektionsudstyr

og adgangskontrol. Den foreslåede bestemmelse går videre end CER-direktivet, idet der stilles krav om, at virksomhederne desuden skal etablere overvågning, der kan opdage uautoriseret adgang til net- og informationssystemer med betydning for leveringen af tjenesten.

Det foreslås på baggrund af bestemmelsen, at der fastsættes nærmere regler om, at virksomheden skal træffe passende tekniske foranstaltninger og konfigurationer, der sikrer monitorering og detektion af uautoriseret adgang til net- og informationssystemer. Det forventes på baggrund af bestemmelsen, at der vil blive fastsat nærmere regler om, at virksomheden skal sikre koordination af sikkerhedsniveauet for tekniske og elektroniske foranstaltninger med fysiske og organisatoriske sikringsforanstaltninger. Det forventes, at ministeren kan fastsætte nærmere regler om brug af videoovervågning, herunder om elektronisk og fysisk sikring af net- og informationssystemer, der benyttes til videoovervågning, der har betydning for leveringen af tjenesten.

Ligeledes foreslås det, at virksomhedernes skal være i stand til at detektere, verificere og alarmere i tilfælde af utilsigtede hændelser såsom brand, naturkatastrofer og ekstreme vejrforhold.

Bestemmelsen skal derudover sikre, at uautoriseret adgang kan opdages i realtid og at virksomhederne skal have fastlagt procedurer for, hvordan der reageres på forsøg på uautoriseret adgang til og på lokationer og anlæg med betydning for leveringen af tjenesten. I denne sammenhæng kan den nødvendige overvågning og detektion fx omfatte en kombinationen af kamera, sensorer, alarmer, hegn, vagtordninger eller lignende foranstaltninger. Det foreslås, at bestemmelsen giver klima-, energi- og forsyningsministeren mulighed for at fastsætte regler om reaktionstid.

Det foreslås på baggrund af bestemmelsen, at der fastsættes nærmere regler om, at virksomheden skal træffe passende tekniske foranstaltninger og konfigurationer, der sikrer monitorering og detektion af uautoriseret adgang til net- og informationssystemer. Den foreslåede bestemmelse vil indebære, at uautoriseret adgang til anlæg eller komponenter med netværksadgang skal kunne opdages i realtid. Det forventes på baggrund af bestemmelsen, at der vil blive fastsat nærmere regler om, at virksomheden skal sikre koordination af sikkerhedsniveauet for tekniske og elektroniske foranstaltninger med fysiske og organisatoriske sikringsforanstaltninger. Det foreslås desuden, at ministeren kan fastsætte nærmere regler om brug af fx videoovervågning, herunder om elektronisk og fysisk sikring af net-

og informationssystemer, der benyttes til videoovervågning, der har betydning for leveringen af tjenesten.

Det foreslås i § 7, stk. 2, *nr. 3,* at virksomhederne skal sikre tilstrækkelig fysisk sikring af virksomhedens anlæg og lokationer, herunder kontrolrum og kontrolrummets arbejdsstationer.

Den foreslåede bestemmelse vil gennemføre dele af CER-direktivets artikel 13, stk. 1, litra b, hvorefter kritiske enheder sikrer tilstrækkelig fysisk beskyttelse af deres lokaler og kritiske infrastruktur under behørig hensyntagen til f.eks. hegn, barrierer, værktøjer og rutiner til overvågning af perimetre.

Bestemmelsen vil medføre, at den fysiske sikring skal etableres uanset, om der er tale om anlæg, der allerede er i drift eller anlæg, som er projekterede eller under etablering. Her forstås fysisk sikring som perimeter-, skal- og cellesikring. Det vil sige, at der skal være sikring af den ydre grænse rundt om anlægget, sikring af anlægget, herunder anlæggets bygninger og ydre mure og sikring af udvalgte rum eller komponenter. Med den foreslåede ordning, sikres der sammenhæng mellem virksomhedernes fysiske sikring af anlæg og lokationer og de overvågnings- og detektionsforanstaltninger, der er foreslået i § 7 stk. 2, nr. 3.

Efter bestemmelsen, kan klima-, energi- og forsyningsministeren endvidere fastsætte nærmere regler om, at anlæg og komponenter med netværksadgang til net- og informationssystemer, der har betydning for leveringen af tjenesten, skal have tilstrækkelig fysisk sikring. Ifølge den foreslåede bestemmelse skal virksomhederne derudover sikre, at der er tilstrækkelig afskærmning af anlæg, lokationer og komponenter for visuel eksponering, således at uvedkommende ikke kan få adgang til eller indblik i informationer, der har betydning for leveringen af virksomhedens tjenester.

Den foreslåede bestemmelse gælder anlæg, lokationer og komponenter, der er i drift såvel som anlæg, lokationer og komponenter der er projekterede, herunder er under etablering. Bestemmelsen vil således medføre, at virksomhederne skal sikre, at deres anlæg og net- og informationssystemer ikke kompromitteres inden de er idriftsat og dermed har indbyggede sårbarheder. Således foreslås det, at der stilles krav om virksomhederne allerede under projekteringen skal forholde sig til fysiske sikkerhedsrisici og

cybersikkerhedsrisici og mitigere disse i relevant omfang. Med bestemmelsen foreslås det derudover, at klima-, energi- og forsyningsministeren kan fastsætte nærmere regler om, at virksomhederne skal have tilstrækkelig fysisk sikring samt overvågnings- og detektionsforanstaltninger ved og omkring de anlæg og lokationer, der benyttes ved en relokering af kontrolrum eller serverrum.

Det foreslås i § 7, stk. 2, *nr. 4*, at klima-, energi- og forsyningsministeren fastsætter nærmere regler om, at virksomheder skal have planer for håndtering af hændelser og genopretning efter hændelser.

Den foreslåede bestemmelse gennemfører CER-direktivets artikel 13, stk. 1, litra c, hvorefter kritiske enheder skal være i stand til at reagere på, modstå og afbøde følgerne af hændelser under behørig hensyntagen til gennemførelsen af risiko- og krisestyringsprocedurer og -protokoller samt varslingsrutiner. Desuden gennemfører bestemmelsen CER-direktivets artikel 13, stk. 1, litra d, hvorefter kritiske enheder skal træffe foranstaltninger, der sikrer genopretning efter hændelser under behørig hensyntagen til forretningskontinuitetsforanstaltninger og identifikation af alternative forsyningskæder.

Med den foreslåede bestemmelse skal virksomhedernes hændelseshåndtering indebære planer og procedurer for, hvordan virksomhederne håndterer en hændelse. Dette vil indebære, at virksomhederne skal have planer for, hvordan de forebygger hændelser, hvordan de opdager, analyserer og varsler hændelser, og hvordan de inddæmmer eller reagerer på og reetablerer sig efter en hændelse. Ifølge den foreslåede bestemmelse skal virksomhederne således have procedurer, der sikrer integriteten og den fysiske beskyttelse af virksomhedens anlæg i tilfælde af både tilsigtede og utilsigtede hændelser med henblik på, at leveringen af tjenesten videreføres.

Med den foreslåede bestemmelse skal virksomhederne have etableret procedurer og foranstaltninger, der sikrer at virksomhederne hurtigst muligt kan genoprette leveringen af tjenesten i tilfælde af, at en hændelse har haft forstyrrende indvirkning. Det foreslås i bestemmelsen, at virksomhedernes procedurer for genopretning skal bygge på virksomhedernes egen identifikation af kritiske anlæg og komponenter og deres fysiske sårbarheder. Det foreslås således, at virksomhederne skal have overblik over tilgængeligheden af reservedele og identificere alternative forsyningskæder, der kan sikre, at leveringen af tjenesten genoprettes.

Det foreslås i § 7 stk. 2, *nr. 5*, at klima-, energi- og forsyningsministeren fastsætter nærmere regler om medarbejdersikkerhedsstyring.

Den foreslåede bestemmelse gennemfører CER-direktivets artikel 13, stk. 1, litra sikre passende medarbejdersikkerhedsstyring under behørig hensyntagen til foranstaltninger såsom fastsættelse af kategorier af personale, der udøver kritiske funktioner, fastlæggelse af adgangsrettigheder til lokaler, kritisk infrastruktur og følsomme oplysninger, fastsættelse af procedurer for baggrundskontrol.

Herved foreslås det, at virksomhederne skal have politikker og systemer for styret adgangskontrol, således at der tages stilling til hvilke medarbejdere, herunder eksterne, der har adgang til hvilke dele af anlægget samt hvilke medarbejdere, herunder eksterne, der har fysisk adgang til net- og informationssystemer. Dette vil desuden indebære, at der føres log over denne adgang, og at der vil føres løbende kontrol med, at adgangskontrollen virker efter hensigten. Det følger derudover af den foreslåede bestemmelse, at der skal sikres sammenhæng med bestemmelsen om autentificering og adgangsbeskyttelse af net- og informationssystemer, jf. den foreslåede § 8 stk. 2, nr. 9.

Til § 8 [Kapitel 3]

Det følger af elforsyningslovens § 85 c, at visse virksomheder med bevilling eller tilladelse til produktion af el skal have et it-beredskab. Det samme gælder for Energinet og dennes helejede datterselskaber, samt virksomheder der yder balancering af elsystemet.

Elforsyningslovens § 85 c, stk. 5, indeholder en bemyndigelsesbestemmelse om at klima-, energi- og forsyningsministeren kan fastsætte nærmere regler om it-beredskabet, herunder regler om; 1) organisering af virksomhedens it-beredskab og evne til at modtage advarsler om trusler mod it-sikkerheden, 2) planlægning og beredskabsarbejde, som virksomhederne skal udføre for at modvirke trusler mod it-sikkerheden, herunder virksomhedernes pligt til at videregive oplysninger til Energinet og relevante myndigheder, 3) virksomhedernes risikostyring, herunder inddragelse af andre virksomheder i risikovurderinger, 4) tilmelding til en it-sikkerhedstjeneste, der yder varsler og informationer om it-sikkerhedstrusler og 5) Energinets varetagelse af overordnede, koordinerende planlægningsmæssige og operative opgaver vedrørende it-beredskab, jf. stk. 1. De nærmere regler om

it-beredskab er gennemført i bekendtgørelse om it-beredskab i el- og naturgassektorerne.

Det følger af gasforsyningslovens § 15 b, at virksomheder som er bevillingspligtige efter gasforsyningslovens § 10, samt Energinet og dennes helejede datterselskaber, som foretager gasforsyningsvirksomhed skal have et it-beredskab.

Gasforsyningslovens § 15 b, stk. 5, indeholder en bemyndigelsesbestemmelse om, at klima-, energi- og forsyningsministeren kan fastsætte nærmere regler om it-beredskabet, herunder regler om; 1) organisering af virksomhedens it-beredskab og evne til at modtage advarsler om trusler mod it-sikkerheden, 2) planlægning og beredskabsarbejde, som virksomhederne skal udføre for at modvirke trusler mod it-sikkerheden, herunder virksomhedernes pligt til at videregive oplysninger til Energinet og til klima-, energi- og forsyningsministeren, 3) virksomhedernes risikostyring, herunder inddragelse af andre virksomheder i risikovurderinger, 4) tilmelding til en tjeneste, der yder varsler og informationer om it-sikkerhedstrusler og 5) Energinets varetagelse af overordnede, koordinerende planlægningsmæssige og operative opgaver vedrørende it-beredskabet, jf. stk. 1. De nærmere regler for it-beredskab er gennemført i bekendtgørelse om it-beredskab i el- og naturgassektorerne.

Ifølge bekendtgørelse om it-beredskab for el- og naturgassektorernes § 23, stk. 1, skal virksomhederne sikre, at den fysiske opbevaring af forsyningskritiske it-systemer beskyttes i forhold til deres kritikalitet for forsyningen på nationalalt, regionalt eller lokalt niveau. Virksomhederne skal desuden sikre forsyningskritiske systemer mod uautoriseret adgang, jf. § 23, skt. 1.

Det følger af olieberedskabslovens § 16, stk. 1, at lagringspligtige virksomheder skal foretage nødvendig planlægning og træffe nødvendige foranstaltninger for, at sikre olieforsyningen i beredskabssituationer og andre ekstraordinære situationer. Efter § 16, stk. 3, kan klima-, energi- og forsyningsministeren fastsætte nærmere regler, om beredskabsplanlægningen efter stk. 1.

Ifølge bekendtgørelse om beredskab for oliesektorens § 16, stk. 1, skal virksomhederne og den centrale lagerenhed sikre, at forsyningskritiske it-systemer beskyttes i forhold til deres kritikalitet. Virksomhederne skal desuden, sikre forsyningskritiske it-systemer mod uautoriseret adgang, jf. § 16, skt. 2.

Det følger af den foreslåede § 8, *stk. 1*, at virksomheder skal træffe passende cybersikkerhedsforanstaltninger for at sikre beskyttelsen af net- og informationssystemer, der bruges til at levere virksomhedens tjenester.

Med den foreslåede bestemmelse rammesættes de overordnede krav til virksomhedens cybersikkerhed herunder cyberberedskabsforanstaltninger. De nærmere krav detaljeres i det foreslåede § 8, stk. 2, hvorefter klima-, energi- og forsyningsministeren fastsætter nærmere regler. Der vil således i bekendtgørelsesform blive stillet konkretiserede krav til de foranstaltninger, som virksomheder skal træffe i medfør af den foreslåede bestemmelse i stk. 1. Der henvises til bemærkningerne til stk. 2.

Dette vil medføre at, virksomheder skal etablere passende cybersikkerhedsforanstaltninger til at opretholde driften og sikre modstandsdygtighed over for trusler, der påvirker eller potentielt kan påvirke virksomheders levering af tjenesten.

Det foreslås samtidig, at virksomhederne skal etablere den nødvendige sikkerhed af de identificerede aktiver og at ministeren kan fastsætte nærmere regler om, at sikkerhedsniveaet opretholdes i hele aktivets levetid fra erhvervelse til dekommissionering gennem blandt andet risikobaseret styring af opdateringer af software.

Det foreslås i § 8, *stk. 2*, at indføre hjemmel til at klima-, energi- og forsyningsministeren efter forhandling med forsvarsministeren fastsætter nærmere regler om cybersikkerhedsforanstaltninger. Bemyndigelsen forventes udmøntet i en bekendtgørelse, der blandt andet fastsætter nærmere regler for de i nr. 1 – 11 nævnte elementer af cybersikkerhed og cyberberedskab, som beskrevet nedenfor. Ved at bemyndige klima-, energi- og forsyningsministeren til at fastsætte sådanne regler, vil nye trusler kunne imødegås og relevante og tidssvarende nye rammer for de cybersikkerheden i energisektoren kunne indarbejdes hurtigere, hvis reglerne udstedes i bekendtgørelsesform end hvis de fastsættes ved lov.

Det foreslås i § 8, stk. 2, *nr. 1*, at klima-, energi- og forsyningsministeren fastsætter nærmere regler om forvaltning af net- og informationssystemer og passende teknisk sikkerhed til beskyttelse af enheder med adgang til virksomhedens netværk.

Bestemmelsen gennemfører dele af NIS 2-direktivets artikel 21, stk. 2, litra i, hvorefter vigtige og væsentlige enheder skal træffe passende foranstaltninger til forvaltning af aktiver.

Det foreslås på baggrund af bestemmelsen, at der fastsættes nærmere regler om, at virksomheder skal etablere og ajourføre et samlet overblik over deres aktiver. Det anses derfor nødvendigt at virksomheder etablerer et samlet og opdateret overblik over blandt andet deres net- og informationssystemer, anlæg, tilhørende komponenter samt kritiske afhængigheder mellem disse og eventuelle samarbejdspartnere.

Det foreslås samtidig, at virksomhederne skal etablere den nødvendige sikkerhed af de identificerede aktiver og at ministeren kan fastsætte nærmere regler om, at sikkerhedsniveaet opretholdes i hele aktivets levetid fra erhvervelse til dekommissionering gennem blandt andet risikobaseret styring af opdateringer af software.

Dertil skal virksomheder have et ajourført overblik over virksomhedens internetvendte enheder og brugerkonti med privilegerede rettigheder, informationsstrømme som understøtter virksomhedernes levering af deres tjenester.

Det foreslås i § 8, stk. 2, *nr. 2*, at klima-, energi- og forsyningsministeren fastsætter nærmere regler om etablering af netværks- og infrastruktursikkerhed, herunder principper for netværksarkitektur og -topologi med henblik på at minimere risici for virksomhedens net- og informationssystemer.

Bestemmelsen gennemfører NIS 2-direktivets artikel 21, stk. 2, litra c, hvorefter vigtige og væsentlige enheder træffer passende foranstaltninger for driftskontinuitet. Desuden gennemfører bestemmelsen artikel 21, stk. 2, litra g, som vedrører grundlæggende cyberhygiejnepraksisser. Den foreslåede bestemmelse går videre end NIS 2-direktivet, idet der direkte stilles krav til, at virksomheder skal etablere bl.a. netværkssegmentering.

Det foreslås på baggrund af bestemmelsen, at der fastsættes nærmere regler om, at virksomhederne skal have procedurer for opbygning af deres netværksinfrastruktur, der muliggør det nødvendige sikkerhedsniveau i forhold til netværkets kritikalitet for leveringen af tjenesten. Det foreslås desuden, at netværksinfrastrukturen skal muliggøre effektiv monitorering.

Efter bestemmelsen forventes det endvidere, der vil blive fastsat regler om, at virksomheder skal etablere passende tekniske foranstaltninger i netværksarkitekturen, således netværksinfrastrukturen opdeles i forskellige netværkssegmenter og med zoner mellem netværk. Opdelingen af netværksinfrastrukturen i netværkssegmenter skal særligt yde beskyttelse af virksomhedens industrielle kontrolsystemer. Foranstaltningen skal bl.a.

sikre, at datakommunikation mellem netværk kan begrænses og kontrolleres. Ligeledes vil bestemmelsen medføre, at ministeren kan fastsætte nærmere regler om segmentering af netværk på en måde, der muliggør relevante sikkerhedstiltag inden for de forskellige segmenter.

Bestemmelsen vil desuden medføre, at ministeren kan fastsætte nærmere regler om etablering af et fysisk eller logisk undernetværk såsom demilitariserede netværkszoner (DMZ), således at datatrafik fra usikre netværk eller administrative netværk ikke deler udstyr eller terminerer direkte i netværk med fx industrielle kontrolsystemer. Dette vil medføre, at netværksarkitekturen skal opbygges på en måde, der sikrer barrierer mellem produktionsmiljøer og øvrige miljøer, herunder, men ikke afgrænset til, test- og udviklingsmiljøer. Det foreslås, at der differentieres i hvilke virksomheder, der skal efterleve de foreslåede krav, således at de mere forsyningskritiske virksomheder skal følge flere elementer af kravene.

Det foreslås i § 8, stk. 2, *nr. 3*, at klima-, energi- og forsyningsministeren fastsætter nærmere regler om sikkerhedskrav til geografisk placering af drift af net- og informationssystemer.

Det foreslås på baggrund af bestemmelsen, at der fastsættes nærmere regler om, at outsourcing til leverandører skal ske på baggrund af en risikovurdering, der iagttager væsentlige risici forbundet herved, og inddrager geopolitiske, organisatoriske og fysiske risici samt cybersikkerhedsrisici. Som led heri foreslås det, at virksomhederne bl.a. vil skulle forholde sig til efterretningstjenesternes trusselsvurderinger.

Der forventes bl.a. at blive fastsat nærmere regler om, at anlæg og net- og informationssystemer med betydning for leveringen af tjenesten, herunder behandling af data, skal placeres i EU/EØS eller i et tredjeland, som Europakommissionen har truffet tilstrækkelighedsafgørelse om, jf. artikel 45 i forordning 2016/679/EU (databeskyttelsesforordningen).

Såfremt virksomheders kontrolrum og nødkontrolrum til overvågning af dansk energiinfrastruktur, der omfattes af dette lovforslag, er placeret uden for dansk territorium, skal virksomhederne i tilfælde af en hændelse kunne relokere til et kontrolrum med komplet driftsfunktionalitet beliggende på dansk territorium.

Den foreslåede bestemmelse vil desuden indebære, at ministeren kan fastsætte nærmere regler om hvorfra, der kan ydes service og vedligehold samt hvorfra, der kan opnås fjernadgang til net- og informationssystemer med

betydning for leveringen af tjenesten. Det foreslås, at der differentieres i hvilke virksomheder, der skal efterleve de foreslåede krav, således at de mere forsyningskritiske virksomheder skal følge flere elementer af kravene.

Det foreslås i § 8 stk. 2, *nr. 4*, at klima-, energi- og forsyningsministeren fastsætter nærmere regler om sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer.

Bestemmelsen gennemfører dele af NIS 2-direktivets artikel 21, stk. 2, litra e, hvorefter vigtige og væsentlige enheder træffer passende foranstaltninger til sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer.

Det foreslås på baggrund af bestemmelsen, at der fastsættes nærmere regler om, at klima-, energi- og forsyningsministeren kan stille krav om, at virksomheder skal sørge for at opretholde et passende sikkerhedsniveau i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer. Således foreslås det, at der vil blive stillet krav til sikkerheden samt til sikkerhedsprocedurer, der sikrer at der etableres relevante sikkerhedsforanstaltninger, i net- og informationssystemers fulde levetid, herunder i projektfaser. Dette vil desuden indebære, at der foretages sikkerhedsvurderinger af, om der opretholdes det nødvendige sikkerhedsniveau. Ligeledes foreslås det, at ministeren kan stille krav om, at virksomheder løbende skal vurdere sikkerhedsrisici og iværksætte foranstaltninger til at mitigere risici. Dette gælder fx ved sammenlægning eller opkøb af virksomheder, ved udbud og licitationer, ved indkøb af net- og informationssystemer, ændringer i systemløsninger eller i forbindelse med anlægsprojekter.

Derudover foreslås det, at virksomheder skal sikre, at sikkerhed er integreret i udviklingsdesignet fra begyndelsen, samt at der sker tilstrækkelig adskillelse mellem net- og informationssystemer, der har betydning for leveringen af tjenesten, og øvrige miljøer såsom udviklings- og testmiljøer. Det foreslås, at der kan fastsættes nærmere regler om hvorvidt denne adskillelse af miljøer skal være fysisk eller logisk.

Det foreslås i § 8 stk. 2, *nr. 5*, at klima-, energi- og forsyningsministeren fastsætter nærmere regler om backup-styring og genopretning af net- og informationssystemer til sikring af driftskontinuitet for leveringen af tjenesten.

Bestemmelsen gennemfører dele af NIS 2-direktivets artikel 21, stk. 2, litra c, hvorefter vigtige og væsentlige enheder træffer passende foranstaltninger om driftskontinuitet såsom backup-styring og reetablering efter en katastrofe.

Det foreslås på baggrund af bestemmelsen, at der fastsættes nærmere regler om, at klima-, energi- og forsyningsministeren kan fastsætte nærmere regler, der skal sikre, at virksomheder identificerer tolerancemål til at sikre genopretning og driftskontinuitet for de identificerede net- og informationssystemer. Dette vil indebære, at virksomheder skal have udarbejdet tekniske genoprettelsesplaner, og skal have foretaget test af, om genopretning er mulig og fungerer efter hensigten på baggrund af backup-kopien.

På baggrund af bestemmelsen, foreslås det, at ministeren kan fastsætte nærmere regler om at virksomhederne skal kunne relokere til fuldt funktionsdygtige nødkontrolrum, der oppebærer samme redundante driftskapacitet og sikkerhedsniveau for fysisk sikring og cybersikkerhed som kontrolrum, der benyttes i daglig drift, herunder at fuldt kompetent personale relokeres og uden forsinkelse kan starte op og varetage tilsvarende opgaveudførelse. I denne sammenhæng kan ministeren fastsætte nærmere regler om, at virksomheden skal iagttage behovet for redundante administrative arbejdspladser og cybersikkerhed i forbindelse med, at opgaveudførsel er flyttet. Dette vil bl.a. indebære, at sikringsplaner tager højde for både opretholdelse af operationel nøddrift og sikkerhed for forskellige personalegrupper.

Det foreslås desuden, at der stilles krav om, at virksomheder skal kunne etablere foranstaltninger, der muliggør dekobling af net- og informationssystemer fra internettet, eller som muliggør isolering af internt kontrollerede netværk, eller at virksomheden på anden vis kan inddæmme eller afslutte datakommunikation eller afbryde adgang til net- og informationssystemer.

Det foreslås, at der differentieres i hvilke virksomheder, der skal efterleve de foreslåede krav, således at de mere forsyningskritiske virksomheder skal følge flere elementer af kravene.

Det foreslås i § 8 stk. 2, *nr. 6*, at klima-, energi- og forsyningsministeren fastsætter nærmere regler om etablering af logning til at understøtte alarmer, efterforskningsarbejde, hændelseshåndtering og monitorering af uregelmæssigheder i net- og informationssystemer.

Den foreslåede bestemmelse gennemfører dele af NIS 2-direktivets artikel 21, stk. 2, litra b, hvorefter vigtige og væsentlige enheder træffer passende foranstaltninger til håndtering af hændelser. Den foreslåede bestemmelse går videre end NIS 2-direktivet, idet der direkte stilles krav om, at virksomhederne skal etablere logning.

Det foreslås på baggrund af bestemmelsen, at der fastsættes nærmere regler om logning og monitorering, som del af virksomheders cyberberedskab. Med bestemmelsen vil det sikres, at virksomheders logning og monitorering skal bidrage til effektiv hændelseshåndtering og muliggøre automatiserede tiltag til at opdage og reagere på anormal aktivitet uanset, om der er tale om utilsigtet eller ondsindet aktivitet samt begrænse konsekvenser heraf.

Derudover vil bestemmelsen medføre, at virksomheder skal træffe passende foranstaltninger, der sikrer visibilitet i netværksinfrastrukturen og gør virksomhederne i stand til at opdage og reagere på anormal aktivitet i net- og informationssystemer.

Den foreslåede bestemmelse skal ligeledes sikre, at virksomheder håndterer logdata forsvarligt og på en måde, der opretholder integriteten og fortroligheden af logdata med henblik på, at disse kan benyttes i forbindelse med bl.a. efterforskning, dokumentation og evaluering.

Med den foreslåede ordning sikres det endvidere, at brugeraktivitet logges med det formål at identificere uautoriseret adgang til virksomhedens netværk og net- og informationssystemer. Det følger heraf, at logdata skal beskyttes mod uautoriseret adgang.

Virksomheden skal etablere logning på en måde, der sikrer alarmer for net- og informationssystemer med betydning for leveringen af tjenesten. Ud fra en risikobaseret tilgang, skal logning kunne fungere på tværs af virksomhedens samlede aktiviteter uagtet net- og informationssystemernes placering, og foranstaltningerne skal sikre at alarmer kan modtages. Disse foranstaltninger kan bl.a. omfatte at mønstre i events kan detekteres. Dette kan fx være eksterne scanningsaktiviteter på virksomhedens internetvendte løsninger, kritisk portkommunikation og ip-adresser samt ændringer i industrielle kontrolsystemers systemopsætning.

Det foreslås i § 8 stk. 2, *nr. 7*, at klima-, energi- og forsyningsministeren fastsætter nærmere regler om etablering af procedurer for løbende kontrol af cybersikkerheden i og omkring net- og informationssystemer.

Bestemmelsen gennemfører dele af NIS 2-direktivets artikel 21, stk. 2, litra f og g, hvorefter vigtige og væsentlige enheder skal have politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici og skal have grundlæggende cyberhygiejnepraksisser.

Det foreslås på baggrund af bestemmelsen, at der fastsættes nærmere regler om, at virksomhederne skal etablere politikker og procedurer for kontrol af virksomhedens tekniske foranstaltninger til at opretholde modstandsdygtighed over for cybertrusler. Desuden foreslås det, at virksomhederne etablerer politikker og procedurer for vurdering af effektiviteten af virksomhedens tekniske foranstaltninger og styring af cybersikkerhedsrisici. Dette vil medføre, at der kan fastsættes nærmere regler om, at virksomheder eksempelvis skal implementere årshjulsprocedurer til systematisk at foretage sanering og vedligehold af sikkerheden i net- og informationssystemer. Således implementerer den foreslåede bestemmelse sammen med den foreslåede § 6, stk. 2, nr. 6 NIS2-direktivets artikel 21, stk. 2, litra f.

Bestemmelsen skal også sikre, at der er overensstemmelse mellem virksomhedernes overordnede beredskabsplan, og at der implementeres procedurer til systematisk at gennemføre og dokumentere genopretningstest.

Endeligt foreslås det på baggrund af bestemmelsen, at der kan fastsættes nærmere regler om, at virksomheder skal have de nødvendige procedurer for etableringen af sikkerhedsforanstaltninger på mobile enheder såsom procedurer for opdatering og anvendelse af antivirusbeskyttelse. Hertil foreslås det desuden, at der skal etableres tilstrækkelig fysisk sikring ved komponenter, der giver styringsadgang til leveringen af tjenesten. Dette vil eksempelvis betyde at mobile enheder og computere, der giver styringsadgang til kontrolrumsfunktioner, skal sikres på lignende vilkår som kontrolrummet.

Det foreslås, at der differentieres i hvilke virksomheder, der skal efterleve de foreslåede krav, således at de mere forsyningskritiske virksomheder skal følge flere elementer af kravene.

Det foreslås i § 8 stk. 2, *nr. 8*, at klima-, energi- og forsyningsministeren fastsætter nærmere regler om brug af sikret tale-, video- og tekstkommunikation og sikrede nødkommunikationssystemer.

Bestemmelsen gennemfører dele af NIS 2-direktivets artikel 21, stk. 2, litra j, hvorefter vigtige og væsentlige enheder skal træffe passende foranstaltninger om brug af løsninger med sikret tale-, video- og tekstkommunikation og sikrede nødkommunikationssystemer internt i enheden, hvor det er relevant.

Det forventes at ministeren fastsætter nærmere regler om beskyttelse af informationer med henblik på at opretholde fortrolighed, integritet og tilgængelighed. Bestemmelsen skal sikre at informationer i transit eller lagret og uanset format fx trykt, elektronisk eller mundtligt sikres med passende tekniske foranstaltninger. Det foreslås, at virksomheden skal udarbejde procedurer og tilvejebringe en sikkerhedsbevidst kultur, så behandling af net- og informationssystemer sker forsvarligt. Bestemmelsen skal ligeledes sikre, at virksomheden kan opretholde nødkommunikationskanaler med tilsvarende beskyttelsesniveau for net- og informationssystemer.

Det foreslås desuden, at virksomheder skal etablere nødkommunikation og sikre at kommunikation kan opretholdes, samt at virksomheder skal kunne varetage sektor- og myndighedskommunikation i krisesituationer eller ved øvrige hændelser, hvor denne foranstaltning vil være relevant.

Hertil foreslås det, at ministeren kan fastsætte nærmere regler om, at virksomheder skal anvende sikret tale-, video- og tekstkommunikation og nødkommunikationssystemer, der i relevant omfang er sikret ved kryptografi eller kryptering.

Det foreslås i § 8 stk. 2, *nr. 9*, at klima-, energi- og forsyningsministeren fastsætter nærmere regler om brug af kryptering samt politikker og procedurer, der skal understøtte sikkerheden og fortroligheden af net- og informationssystemer, der er kritiske for leveringen af virksomhedens tjeneste.

Bestemmelsen gennemfører NIS 2-direktivets artikel 21, stk. 2, litra h, hvorefter vigtige og væsentlige enheder skal have politikker og procedurer vedrørende brug af kryptografi og, hvor det er relevant, kryptering.

Ministeren forventes på baggrund af bestemmelsen at indføre nærmere regler for anvendelse af kryptografi og tekniske krav for adgang til net- og informationssystemer.

Det forslås at virksomhederne, ud fra en risikobaseret tilgang, anvender kryptografi og krypteringsteknikker til at etablere forskellige beskyttelsesformål for kritisk information og kommunikation, der bl.a. skal sikre fortrolighed, integritet og autenticitet

Virksomheden gennemfører tekniske tiltag, så de er forenelige med stabil drift for industrielle kontrolsystemer og –processer. Det foreslås endvidere at virksomheden skal etablere foranstaltninger som f.eks. sikkerhedsprotokoller, samt procedurer for forvaltning af administration af eksempelvis nøgler og certifikater. Dette vil bl.a. sikre backup af data.

Endvidere kan der fastsættes nærmere regler om, at datatrafik på virksomhedens trådløse netværk skal være krypteret med tidssvarende tekniske protokoller og opdateret kryptografiske løsninger.

Det foreslås i § 8 stk. 2, *nr. 10*, at klima-, energi- og forsyningsministeren fastsætter nærmere regler om multifaktorautentificering eller kontinuerlig autentificering og adgangsbeskyttelse til sikring mod uautoriseret adgang til virksomhedernes net- og informationssystemer.

Bestemmelsen gennemfører dele af NIS 2-direktivets artikel 21, stk. 2, litra i og j, hvorefter vigtige og væsentlige enheder skal træffe passende foranstaltninger vedrørende adgangskontrolpolitikker og brug af løsninger med multifaktorautentificering eller kontinuerlig autentificering.

Ministeren forventes at stille krav til begrænsning af adgang, herunder fjernadgang, til lokationer, kontrolrums- og serverrumsfaciliteter samt for adgang til net- og informationssystemer.

Yderligere foreslås der krav om, at den fysiske sikring af anlæg, herunder sikringen af anlæg med netværksadgang jf. de foreslåede § 7, stk. 2, nr. 2-3 gør brug af elektronisk adgangsstyring, herunder autentificering og multifaktorgodkendelsesløsninger. Dette kan f.eks. være en kombination af adgangskort og –kode og aktivitetsbestemte adgangskoder.

Den foreslåede bestemmelse skal medvirke til at beskytte tjenesten mod uautoriseret adgang og muliggøre identifikation og autentifikation af identiteten, der anmoder om adgang samt effektiv styring af brugeradgange i hele livscyklussen. Den foreslåede elektroniske adgangsstyring vil ligeledes muliggøre, at virksomheden kan modtage alarmer ved anormal aktivitet.

Det følger af bestemmelsen, at virksomheden sikrer klart definerede regler for, hvilke medarbejdere eller medarbejdergrupper, der kan tilgå forskellige dele af et anlæg eller net- og informationssystemer. Dette indebærer, at virksomhederne skal have procedurer for hvordan adgange og fjernadgange til kritiske anlæg og net- og informationssystemer tildeles, ændres og lukkes for både virksomhedens egne medarbejdere såvel som for gæster, konsulenter, eksterne samarbejdspartnere og leverandører. Det følger desuden af bestemmelsen, at ministeren kan fastsætte nærmere regler om, at fjernadgang til net- og informationssystemer med betydning for leveringen af tjenesten ikke må ske fra offentligt tilgængeligt Wi-Fi.

Det foreslås i § 8 stk. 2, *nr. 11*, at klima-, energi- og forsyningsministeren fastsætter nærmere regler om foranstaltninger til forebyggelse og håndtering af hændelser.

Bestemmelsen gennemfører dele af NIS 2-direktivets artikel 21, stk. 2, litra b, hvorefter vigtige og væsentlige enheder skal træffe passende foranstaltninger til håndtering af hændelser.

Det foreslås efter bestemmelsen, at der fastsættes nærmere regler om, at virksomheder skal, sikre en koordineret proces for rapportering af svagheder i virksomhedens cybersikkerhed. Det foreslås endvidere, at der kan fastsættes regler for håndtering af cyberhændelser og utilsigtede hændelser, der kan påvirke sikkerheden af net- og informationssystemer med betydning for leveringen af tjenesten.

Dette omfatter brug af bl.a. logdata til fx. detektion af anormal og uautoriseret aktivitet i net- og informationssystemer. Med den foreslåede ordning, sikres de at virksomheden skal kunne reagere på alarmer eller hændelser uanset, hvor i organisation en hændelse opstå, herunder hvis en hændelse opstår hos en samarbejdspartner, der har adgang til virksomhedens net- og informationssystemer. I sådanne tilfælde skal virksomheden være i stand til at foretage mitigerende foranstaltninger såsom frakobling af udstyr og afbrydelse af leverandøradgange.

Den foreslåede bestemmelse skal også sikre, at virksomheden indfører passende forebyggende foranstaltninger til at minimere utilsigtet påvirkning af net- og informationssystemer og til at undgå hændelser, der forårsager tab af visibilitet og kontrol med leveringen af tjenesten.

Det foreslås desuden, at der kan fastsættes nærmere regler om, at der sikres overensstemmelse mellem sikkerhedstiltag hos virksomheden og samarbejdspartnere med adgang til net- og informationssystemer med betydning for leveringen af tjenesten.

Med den foreslåede bestemmelse sikres det, at virksomheden skal have indgået aftaler om ansvar og kommunikation i forbindelse med håndtering af cyberhændelser. Ligeledes skal det sikres, at der kan foretages rapportering af hændelser efter en ensartet metode på tværs af virksomheden, herunder at der indhentes rapportering om hændelser af betydning for virksomhedens leveringen af tjenesten fra samarbejdspartnere.

Til § 9 [Kapitel 3]

Der er i NIS 1-direktivet ikke nærmere regulering om brug af særlige informations- og kommunikationstjenester (IKT)-produkter, -tjenester og -processer.

Gældende beredskabsregulering indeholder heller ikke nærmere regulering om brug af særlige informations- og kommunikationstjenester (IKT)-produkter, -tjenester og –processer.

Det følger af den foreslåede § 9, *stk. 1*, at klima-, energi- forsyningsministeren efter forhandling med forsvarsministeren kan fastsætte regler om, at væsentlige og vigtige enheder skal anvende 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 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.

Bestemmelsen vil gennemføre artikel 24, stk. 1, i NIS 2-direktivet. Det følger af artikel 24, stk. 1, at for at påvise 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.

Klima-, Energi- Forsyningsministeriet har lagt vægt på, at der for fastsættelse af krav til anvendelse af særlige IKT-produkter, -tjenester og -processer til foretages en ensretning med den af Forsvarsministeriet foreslåede ordning for at anvende særlige IKT-produkter mv. [Bestemmelsen svarer således til den ordning, der følger af § 8 i Forsvarsministeriets forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau.]

Den foreslåede bestemmelse svarer endvidere indholdsmæssigt til NIS 2-direktivets artikel 24, stk. 1, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Det er Klima-, Energi- Forsyningsministeriets vurdering, 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.

Til § 10 [Kapitel 3]

Ifølge gældende beredskabsregulering (beredskabsbekendtgørelserne nr. 821 2446 og 2647) har Energinet de overordnede, koordinerende planlægningsmæssige og operative opgaver vedrørende beredskabssituationerne i el- og gassektoren, herunder at videreformidle relevante meddelelser og in-

formationer mellem myndighederne og el- og naturgassektorens virksomheder samt at fremskaffe data og andre informationer om sektoren af betydning for samfundets beredskab.

Energinet varetager denne koordinerende og operative rolle i el- og naturgassektorernes beredskab, da Energinet har det overordnet ansvar for funktionen og balanceringen af el- og gastransmissionsnettet. Således er det nødvendigt at Energinet har visse instruktionsbeføjelser overfor virksomhederne i deres beredskab, samt at de modtager information om sårbarheder, trusler og hændelser i sektorerne, da disse hurtigt kan påvirke transmissionsnettet og potentielt medføre kaskadeeffekter ud i el- og naturgassektorerne.

Derfor skal Energinet i planlægning af beredskabet i el- og naturgassektorerne udarbejde en vurdering af sårbarheden for el for hhv. det samlede el- og naturgasforsyningssystem jf. § 6, stk. 2 i bekendtgørelsen for beredskab i elsektoren og bekendtgørelse for beredskab i naturgassektoren. I tillæg hertil skal Energinet jf. bekendtgørelse om it-beredskab for el- og naturgassektorerne, årligt udarbejde vurdering af it-relaterede risici og sårbarheder for det sammenhængende elforsyningssystem og det sammenhængende naturgasforsyningssystem. I vurderingerne skal indgå risici og sårbarheder afledt af sammenhænge med nabolandenes forsyningssystemer.

Desuden skal Energinet som led i den koordinerende planlægning af beredskabet i el- og naturgassektorerne lave sektorberedskabsplaner for hhv. det samlede el- og naturgasforsyningssystem jf. § 8 i bekendtgørelsen for beredskab i elsektoren og bekendtgørelse for beredskab i naturgassektoren. Sektorberedskabsplanerne skal udarbejdes under hensyntagen til el- og naturgassystemernes sammenhænge med nabolandenes systemer. Sektorberedskabsplanen skal angive hvordan Energinet for el- og naturgassektoren hhv. som helhed planlægger at håndtere en beredskabssituation på en koordineret måde, herunder sikring af en samordnet situationsopfattelse hos virksomhederne, samt relevante dele af det indhold der i virksomhedernes egne beredskabsplaner. Endvidere foreskriver § 16 i bekendtgørelse om it-beredskab for el- og naturgassektorerne at, sektorberedskabsplanerne skal indeholde en beskrivelse af, hvordan Energinet planlægger at håndtere en it-beredskabssituation, der berører flere virksomheder, herunder:1) Ansvarsfordelingen mellem virksomheder og Energinet, 2) Beskrivelse af kommunikationsveje og forholdsregler ved kompromittering af kommunikationsveje. 3) Krav Energinet i en it-beredskabssituation stiller til form,

indhold og hyppighed af situationsrapporter fra virksomhederne til Energinet, 4) Hvorledes Energinet vil informere virksomhederne om it-beredskabssituationen, herunder form, indhold og hyppighed, således at Energinet kan tilsikre en samordnet situationsopfattelse hos virksomhederne i el- og naturgassektorerne, 5) En instruktion om anvendelse af specifik kryptering af informationer og driftsordre, hvis relevant, 6) Planer for segmentering af fælles it-infrastruktur eller driftsinfrastruktur i relevante scenarier, hvis relevant.

I krisesituationen har Energinet endvidere ansvaret for at koordinere sektorens håndtering af krisesituationen og genetableringen af forsyningen i el- og gassektoren, herunder for at udpege repræsentanter til de lokale beredskabsstabe og deltage i NOST, hvis det er relevant. Desuden har Energinet ansvaret for at informere Energistyrelsen og andre centrale myndigheder fx politiet via de lokale beredskabsstabe, om situationen i sektoren.

Energinet endvidere skal sikre, at virksomheden når som helst i en beredskabssituation kan forestå el- og naturgassektorens krisehåndtering og kan fremskaffe relevante og opdaterede informationer om elsektorens forhold til brug for myndighedernes krisehåndtering i el- og naturgassektoren, herunder om situationen i nabolandenes forsyningssystemer af relevans for denne krisehåndtering.

Herudover skal Energinet, i medfør af § 16 i henholdsvis i bekendtgørelse om beredskab for elsektoren og bekendtgørelse om beredskab i naturgassektoren, gennemføre foranstaltninger for at sikre, at sandsynligheden for en henholdsvis en strømafbrydelse og en naturgasafbrydelse holdes på et rimeligt niveau. Efter samme bestemmelser skal Energinet endvidere gennemføre foranstaltninger for at sikre, at der kan udføres en hurtig og koordineret reetablering af henholdsvis elforsyningen og naturgasforsyningen i tilfælde af afbrydelser. Ligesom det er Energinets ansvar at sikre, at generne for elforbrugerne, naturgasforbrugerne og for samfundet i øvrigt ved en afbrydelse mindskes i muligt omfang.

Det følger endvidere af § 18 i henholdsvis i bekendtgørelse om beredskab for elsektoren og bekendtgørelse om beredskab i naturgassektoren, at Energinet skal etablere et formaliseret samarbejde om beredskabsforhold i elsektoren og i naturgassektoren, bl.a. gennem informationsvirksomhed og møder om beredskabsforhold.

Energinet skal arbejde for at koordinere sine beredskabsplaner med de systemansvarlige virksomheder i nabolandene i muligt omfang og for en hensigtsmæssig informationsudveksling med disse virksomheder om planlægningsmæssige og operative forhold, jf. § 18 i bekendtgørelse om beredskab for elsektoren og i bekendtgørelse om beredskab i naturgassektoren

Det følger af § 19 i henholdsvis bekendtgørelse om beredskab for elsektoren og bekendtgørelse om beredskab i naturgassektoren, at Energinet senest 1. maj skal fremsende en årlig redegørelse til Energistyrelsen om status for henholdsvis elsektorens – og naturgassektorens beredskab, herunder om virksomhedens beredskabsarbejde i det forløbne år. Energistyrelsen kan fastsætte nærmere rammer herfor.

Desuden skal Energinet, i medfør af § 21, stk. 2 i henholdsvis bekendtgørelse om beredskab for elsektoren og bekendtgørelse om beredskab i naturgassektoren, afholde beredskabsøvelser i anvendelse af sektorberedskabsplanen skal heri inddrage væsentlige dele af virksomhedernes planer.

Endvidere skal Energinet, i medfør af § 5 i bekendtgørelse om it-beredskab for el- og naturgassektorerne, varetage de overordnede koordinerende opgaver i forbindelse med håndteringen af it-beredskabshændelser, der omfatter flere virksomheder. De skal ligeledes efter § 5, stk. 2, etablere et formaliseret samarbejde om it-beredskabsforhold, der har til formål at fremme koordineringen af såvel planlægningen som udøvelsen af it-beredskabet. Efter § 5, stk. 3-5, skal Energinet bistå med at skaffe kontaktoplysninger til andre virksomheder og myndigheder i en akut situation, ligesom de skal give virksomhederne oplysningerne om aktuelle driftstilstande, ligesom Energinet til enhver tid skal kunne modtage og videreformidle informationer af betydning for it-beredskabet til andre virksomheder i el- og naturgassektorerne.

Endeligt varetager Energinet en række forpligtigelser i forbindelse med rapportering af evt. hændelser hos sig selv og andre virksomheder i el- og naturgassektorerne til Energistyrelsen og Center for Cybersikkerhed jf. § 21 i bekendtgørelse om it-beredskab for el- og naturgassektorerne og § 23 i hhv. bekendtgørelse om beredskab for elsektoren og beredskab for naturgassektoren.

Det foreslås med *§ 10*, at klima-, energi- og forsyningsministeren fastsætter nærmere regler om ministerens og Energinets varetagelse af, koordinerende planlægningsmæssige og operative opgaver vedrørende beredskab, jf. § 6, stk. 1 og stk. 2, § 7, stk. 1 og stk. 2 og § 8, stk. 1.

Bestemmelsen viderefører dele af den gældende bestemmelse i elforsyningslovens § 85 b, stk. 2 og gasforsyningslovens § 15 a, stk. 2.

Det forventes endvidere de gældende regler angående Energinets koordinerende opgaver i beredskabsbekendtgørelserne for elsektoren og naturgassektoren videreføres for el- og gassektoren, dog med tilføjelse af brintsektoren såfremt der måtte etableres et brinttransmissionssystem i Danmark, samt tilføjelse af de nye aktører, der vil omfattes af beredskabsreguleringen i delsektorerne for el-, gas. Disse aktører er hovedsageligt dikteret af NIS2 og CER-direktivernes bilag om disses anvendelsesområde.

Det forventes samtidig at vil blive fastsat nærmere regler om at de, koordinerende planlægningsmæssige og operative opgaver vedrørende beredskab i oliesektoren og de nye delsektorer fjernvarme og fjernkøling vil blive varetaget af Energistyrelsen.

Til § 11 [kapitel 3]

§ 25 og § 26 i bekendtgørelse om beredskab for elsektoren og bekendtgørelse om beredskab for naturgassektoren regulerer Energinet og Energistyrelsens muligheder for at pålægge og ændre foranstaltninger som virksomhederne i el- og naturgassektorerne skal træffe i tilfælde af beredskabssituationer omfattende sikkerhedsrelaterede hændelser og beredskabssituationer i bredere forstand. Beredskabssituationer omfattende sikkerhedsrelaterede hændelser sigter hovedsageligt på situationer hvor der er øget trussel for fysiske angreb mod det danske samfund, eller hvor et sådan angreb har fundet sted. Beredskabssituationer i bredere forstand kan være alt fra stormflod, orkaner, cyberangreb, solstorm til isvinter og tørke.

§ 25 beskriver således at Energinet i tilfælde beredskabssituationer der omfatter sikkerhedsrelaterede hændelser, efter der er blevet fastsat et sikkerhedsberedskabsniveau i henhold til den nationale beredskabsplan, kan træffe beslutning om hvilke sikkerhedsberedskabsforanstaltninger der skal gennemføres for el- og naturgassektoren, herunder hvilke virksomheder og

anlæg der skal omfattes heraf. Energinet kan i perioden fra en sikkerhedsrelateret hændelse er erkendt og indtil et sikkerhedsberedskabsniveau er fastsat, iværksætte forberedelser i virksomhederne, således at sikkerhedsberedskabsforanstaltningerne hurtigt kan iværksættes. Når Energinet har underrettet de relevante virksomheder om at der fastsat et sikkerhedsberedskabsniveau og de sikkerhedsberedskabsforanstaltninger der virksomheden skal træffe, skal virksomheden gennemføre sikkerhedsberedskabsforanstaltningerne og underrette Energinet om at de er blevet gennemført.

Siden reglernes indførelse i 2005, er der sket visse ændringer i den nationale beredskabsplanlægning, hvorfor der ikke længere er sikkerhedsberedskabsniveauer i den nationale beredskabsplan. Derfor har der været praksis at Energinet i samråd med Energistyrelsen har fastsat et sektorberedskabsniveau, som erstatning for sikkerhedsberedskabsniveau, og der i den forbindelse har været meldt en eller flere prædefineret beredskabsforanstaltninger som virksomhederne skulle gennemføre.

Sektorberedskabsniveauet består for nuværende af 5 eskalationstrin for den danske el og naturgassektor. Et øget sektorberedskabsniveau er udtryk for at virksomhederne i el- og gassektoren skal udvise øget opmærksomhed og kan/er blevet akkompagneret af konkrete foranstaltninger, som relevante virksomheder i el- og gassektoren skal iværksætte.

Efter § 26 kan Energinet og Energistyrelsen pålægge virksomhederne i el- og naturgassektorerne at ændre deres foranstaltninger for at sikre en hurtig, koordineret og prioriteret krisehåndtering, herunder gennemførelse af myndighedernes beslutninger i den nationale krisehåndtering. Det samme er gældende hvis der vurderes at være risiko for at beredskabssituation indtræffer. Denne paragraf har således et videre sigte end den gældende § 25, i den aktiveres uagtet om der er tale om beredskabssituation omfattende sikkerhedsrelaterede hændelser eller ej, og uanset om en beredskabssituation er opstået eller det blot vurderes at der er risici for at en beredskabssituation opstår.

Der foreslås med § 11, *stk. 1*, en klar hjemmel til at fastsætte og udmelde sektorberedskabsniveauer (før sikkerhedsberedskabsniveauer) for hele energisektoren eller en eller flere delsektorer.

Der foreslås med § 11, *stk. 2* ligeledes en klar hjemmel til at klima-, energi- forsyningsministeren kan fastsætte og pålægge sektorberedskabs-

foranstaltninger (før sikkerhedsberedskabsforanstaltninger) for hele energisektoren, for en eller flere del-sektorer eller for en eller flere virksomheder, på baggrund af en beredskabssituation omfattende sikkerhedsrelaterede hændelser.

Sikkerhedsrelaterede hændelser skal, som i gældende ret, forstås som hændelser hvor der vurderes at være risiko for eller et konkret antagonistisk angreb vil finde/har fundet sted. Der tænkes således f.eks. spionage, terrorangreb, hybride angreb eller konkrete krigshandlinger. Det er ikke nødvendigt at angrebet eller risikoen for et angreb kan tilskrives en konkret aktør, blot at der mistanke om at et angreb er nærtforestående eller at det faktisk har været udført. Det er heller ikke et krav at angreb eller risiko for angreb er på dansk jord. Et angreb eller risiko for et angreb i et naboland kan således godt udløse brugen af denne paragraf. Angrebet eller risikoen for angreb behøver heller ikke at være rettet mod energiinfrastruktur, men kan også være i andre sektorer der varetager samfundskritiske funktioner. Det er endvidere ikke kun fysiske angreb, men også cyberangreb, der kan afstedkomme brugen af bestemmelserne i stk. 1 og 2.

Det forventes endvidere på baggrund af de foreslåede bestemmelser i stk. 1 og 2, at klima-, energi- og forsyningsministeren fremover træffer afgørelse om sektorberedskabsniveau og -foranstaltninger for alle energiarter, som efterfølgende udmeldes til virksomheder af et operationelt kontaktpunkt. Det forventes at Energinet vil blive delegeret kompetencen med til at udmelde sektorberedskabsniveauer og sektorberedskabsforanstaltninger for el- og gassektoren, således Energinet kan fastholde rollen som operationelt kontaktpunkt for el- og gassektoren samt brintsektoren ved etablering af et brinttransmissionsnet. Det forventes at Energistyrelsen bliver delegeret opgaverne med at fastsætte sektorberedskabsniveauet på tværs for hele energisektoren eller delsektorer, og udmeldingsopgaven med at agere operationelt kontaktpunkt for olie, fjernvarme/-køling og brint ved decentral brintforsyning.

Konkret betyder udmelding om et øget sektorberedskabsniveau, at der udmeldes konkrete sektorberedskabsforanstaltninger, som virksomhederne i energisektoren, eller delsektorer skal implementere, med henblik på at øge sikkerheden på f.eks. anlæg, bygninger, installationer og net- og informationssystemer. Den konkrete implementering af de enkelte sektorberedskabsforanstaltninger for, hver virksomhed vil afhænge af virksomhederne og deres anlæg, idet fysiske indretninger, kontraktforhold og anden lovgivning tilskriver at visse beredskabsforanstaltninger ikke kan gennemføres

fuldt ud, eller må modificeres for passe til virksomheden, deres anlæg og deres net- og informationssystemer. Der kommunikeres af sikkerhedsmæssige årsager ikke offentligt om sektorberedskabsforanstaltningerne, men disse vil blive gjort bekendt til virksomhederne der er omfattet af loven af Energistyrelsen.

Det foreslås i § 11, *stk. 3*, at klima-, energi- forsyningsministeren i en beredskabssituation kan bestemme, at de i § 11, stk. 2 nævnte sektorberedskabsforanstaltninger samt andre foranstaltninger, der skal foretages efter loven eller regler udstedt i medfør af loven, midlertidigt skal intensiveres og suppleres med yderligere foranstaltninger for at sikre en hurtig, koordineret og prioriteret krisehåndtering, herunder gennemførelse af myndighedernes beslutninger i den nationale krisehåndtering.

Det foreslåede stk. 3 er således i udgangspunktet en forsættelse af den gældende § 26 i bekendtgørelse om beredskab for elsektoren og bekendtgørelse om beredskab for naturgassektoren. Dog med den ændring at beføjelsen i udgangspunktet tilfalder klima-, energi- og forsyningsministeren og ikke Energinet. Der er således også tale om et bredere anvendelsesområde end de situationer som den foreslåede § 11, stk. 1 og 2 sigter på, idet der efter stk. 3 også kan skrues op og ned for foranstaltninger i tilfælde af f.eks. stormflod, brande, pandemier etc. som ikke er antagonistiske sikkerhedshændelser. Stk. 3 har ligeledes til formål at sikre at virksomhedernes ressourcer i form af personale, materiel, kritiske reservedele m.m. kan indsættes på en måde, som bedst muligt sikrer genetableringen af energiforsyning og markedsmekanismerne i energisektorerne.

Det foreslås med § 11, *stk. 4*, at Energinet i en beredskabssituation omfattende sikkerhedsrelaterede hændelser, i særlige tilfælde, hvor klima-, energi- forsyningsministeren ikke kan fastsætte og udmelde sektorberedskabsniveauer og foranstaltninger, jf. stk. 1, 2 og 3 kan varetage opgaven på ministerens vegne. Energinet kan kun varetage opgaven for el-, gas- og brintsektorerne.

Det foreslåede stk. 4, tænkes brugt i situationer hvor klima-, energi- og forsyningsministeren måtte være afskåret fra at varetage sine opgaver efter stk. 1-3. Der kunne således være hvor klima-, energi- og forsyningsministeren er ramt af en beredskabssituation der gør at det ikke er muligt at bruge de normale kommunikationsveje til el-, gas- og brintvirksomhederne. Årsagen til at Energinet gives muligheden for at varetage denne opgave er, at Energinet har særlige kommunikationsveje direkte til en række

virksomheder i el-, gas- og brintsektoren, der sikrer en særlig redundans for deres kommunikation.

Til § 12 [Kapitel 4]

For el og gas sektorerne er der fastsat regler om at indberette beredskabshændelser, som vedrører det klassiske beredskab i bekendtgørelse om beredskab i elsektoren og bekendtgørelse om beredskab i gassektoren. Ifølge bekendtgørelsernes § 22, stk. 1, 1. pkt., skal virksomheder udarbejde en evaluering af større eller usædvanlige hændelser, som i væsentligt omfang har aktiveret virksomhedens beredskab. Der stilles krav til indhold af evalueringen, samt at den senest 3 måneder efter hændelsen skal fremsendes til Energistyrelsen. Energistyrelsen kan ifølge bekendtgørelsernes § 22, stk. 1, 2. pkt., pålægge virksomheder at udarbejde sådanne evalueringer. Virksomheder skal efter § 23 i bekendtgørelserne, omgående underrette Energinet om nærmere angivne hændelser af relevans for beredskabssituationer i overensstemmelse med sektorberedskabsplanen.

Regler for at indberette beredskabshændelser om it-beredskab for virksomheder i el og gassektorerne fremgår af bekendtgørelse om it-beredskab i el- og naturgassektorerne. Det fremgår af bekendtgørelsens § 21, stk. 1, at it-sikkerhedshændelserne, der i væsentligt grad reducerer virksomhedens funktionalitet eller funktionaliteten af andre dele af el- og naturgassektoren, omgående skal meddeles Energinet. Virksomheder skal desuden ifølge bekendtgørelsens § 22, stk. 1, udarbejde evalueringer af hændelser der i væsentligt omfang aktiverer virksomhedens it-beredskab. Der opstilles nærmere scenarier, hvor det kræves at der udarbejdes en evaluering. Der er fastsat indholdsmæssige krav til evalueringen i § 22, stk. 2, mens der i § 22, stk. 3, stilles krav om at evalueringen senest 3 måneder efter hændelsen fremsendes til Energistyrelsen.

De nærmere regler om at indberette beredskabshændelser for oliesektoren fremgår af bekendtgørelse om beredskab af oliesektorens §§ 14 og 15. Bestemmelser regulerer både fysiske beredskabshændelser og it-beredskabshændelser. Ifølge § 14, stk. 1, skal virksomheder og den centrale lagermyndighed uden ugrundet ophold foretage meddelelse til Energistyrelsen om hændelser, der i væsentlig grad reducerer deres funktionalitet eller funktionaliteten af andre dele af oliesektoren. Efter § 15, stk. 1, skal virksomheder og den centrale lagermyndighed udarbejde en evaluering af hændelser, som meddeles i medfør af § 14, stk. 1. Hændelsesevalueringen

skal fremsendes senest tre måneder efter hændelsen til energistyrelsen, jf. § 15, stk. 3.

Der stilles ikke krav i om indberetning af beredskabshændelser i andre delsektorer i energisektoren.

Det følger af den foreslåede *§ 12,* at klima-, energi- og forsyningsministeren kan fastsætte regler for underretning og indrapportering af hændelser, væsentlige cybertrusler og nærvedhændelser.

Det forventes, at der på baggrund af den foreslåede bestemmelse fastsættes nærmere regler om, at virksomheder uden unødigt ophold skal foretage underretning om enhver væsentlig hændelse og at en underretning skal indeholde oplysninger, der gør det muligt at fastslå eventuelle grænseoverskridende virkninger af hændelsen.

Den foreslåede bestemmelse i stk. 1, vil gennemføre artikel 23, stk. 1, i NIS 2-direktivet og artikel 15, stk. 1, 1. pkt., i CER-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. Fremgår endvidere at underretningen i sig selv ikke medfører et øget ansvar for den underrettende enhed, hvilket vil være gældende for underretninger efter den foreslåede § 12.

Det forudsættes, at underretningerne af de relevante myndigheder vil skulle foretages via en fælles digital indgang, såsom Virk.dk. Dette vil sikre, at de berørte virksomheder alene skal foretage én samlet underretning, som fordeles samtidigt til de relevante myndigheder. Dermed sikres det, at både den relevante kompetente myndighed hurtigt og effektivt vil kunne varetage sine myndighedsopgaver.

I overensstemmelse med præambelbetragtning nr. 83, 2. pkt., vil ministeren fastsætte nærmere regler om at de foreslåede forpligtelser til at foretage underretning ved hændelser, væsentlige cybertrusler og nærvedhændelser, finder anvendelse på virksomheder, uanset om virksomhederne 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.

Ministeren forventes på baggrund af bestemmelsen, at fastsætte nærmere regler der præciserer, hvilke hændelser virksomheder skal underrette myndighederne om. Ministeren vil gennemføre CER-direktivets artikel 15, stk. 1, 3. pkt, og NIS 2-direktivers artikel 23, stk. 3, ved fastsættelsen af de nærmere regler, om hvilke hændelser der skal foretages underretning om.

Det følger af CER-direktivets artikel 15, stk. 1, 3. pkt., at med henblik på at fastslå en forstyrrelses omfang tages navnlig følgende kriterier i betragtning; a) antallet og andelen af brugere, der er berørt af forstyrrelsen, b) forstyrrelsens varigheden og c) det geografiske område, der er berørt af forstyrrelsen, idet der tages hensyn til, om det er et geografisk isoleret område.

NIS 2-direktivets artikel 23, stk. 3, 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.

Ministeren kan fastsætte regler, hvor tærsklen for at virksomheder skal foretage underretninger af hændelser er mindre, end hvad der fremgår af CER- og NIS 2-direktiverne, da dette ville kunne understøtte et bedre indblik i det aktuelle trusselsbillede. Et mere præcist trusselsbillede kan anvendes til at foretage de nødvendige nationale foranstaltninger, for at opretholde en mere resilient energisektor.

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 i medfør af det foreslåede § 13, 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 3.3. i lovforslagets almindelige bemærkninger.

Med den foreslåede bestemmelse kan klima-, energi- og forsyningsministeren fastsætte nærmere regler til formkrav af underretninger, herunder hvilke informationer der skal fremgå af underretninger og hvilke frister der gælder i forhold til underretning. Ministeren vil desuden med baggrund i bestemmelsen, kunne fastsætte regler, om hvem der skal underrettes ved hændelser.

Ved de nærmere regler om underretning af hændelser forventes det, at der fastsættes regler om at underretning skal ske på følgende måde; 1) en tidlig varsling, som skal angive, om hændelsen 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 hændelsen, 2) en hændelsesunderretning, som skal ajourføre oplysningerne fra den tidlige varsling, jf. nr. 1, og give en indledende vurdering af hændelsen, herunder dens alvor og indvirkning samt kompromitteringsindikatorerne, hvor sådanne foreligger, sendes uden unødigt ophold og under alle omstændigheder inden for 72 timer efter, at den pågældende har fået kendskab til hændelsen, 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 i nr. 2 omhandlede hændelsesunderretning. 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 virksomhed forelægge en statusrapport på det pågældende tidspunkt og en endelig rapport senest en måned efter, at hændelsen er håndteret.

Med den foreslåede bestemmelse fastlægges der en flertrinstilgang for underretninger om væsentlige hændelser, som følger NIS 2- direktivets arti-

kel 23, stk. 4. De nærmere regler, som udmøntes på baggrund af bestemmelsen, skal dermed forstås og anvendes i overensstemmelse med direktivernes forudsætninger.

Underretnings fremgangsmåden vil desuden gennemføre CER-direktivets artikel 15, stk. 1, 1. og 2. pkt., hvoraf fremgår, at medlemsstaterne sikrer, at kritiske enheder uden unødigt ophold underretter den kompetente myndighed om hændelser, der i betydelig grad forstyrrer eller har potentiale til i betydelig grad at forstyrre leveringen af væsentlige tjenester. Medlemsstaterne sikrer, at kritiske enheder, med mindre det operationelt ikke er muligt, indgiver en første underretning senest 24 timer efter at være blevet opmærksom på en hændelse, efterfulgt, hvor det er relevant, af en detaljeret rapport senest en måned derefter. Det fremgår endvidere af artikel 15, stk. 2 at underretninger efter artiklen ikke medfører et øget ansvar for kritiske enheder hvilket vil være gældende for underretninger efter den foreslåede § 12.

Virksomheder 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.

Den berørte virksomhed vil skulle sende en endelig rapport senest en måned efter forelæggelsen af den første hændelsesunderretningen. I tilfælde af at hændelsen fortsat er igangværende på tidspunktet for indgivelsen af den endelige rapport, skal den berørte virksomhed forelægge en statusrapport. Den endelige rapport vil i så fald skulle indgives senest en måned efter, at virksomheden har håndteret 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 hændelser og give virksomheder 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 forventes desuden, at der fastsættes nærmere regler om, at såfremt en hændelse måtte have grænseoverskridende karakter, skal virksomhederne også rette henvendelse til CSIRT'en i ovenstemmelse med forudsætningen i NIS 2-direktivets artikel 23, stk. 6, hvorefter CSIRT'en via det centrale kontaktpunkt uden unødigt ophold vil 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 virksomhedens sikkerhed og kommercielle interesser samt fortrolig behandling af de afgivne oplysninger.

Til § 13 [Kapitel 4]

Der er ikke fastsat nærmere regler i energisektoren, 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 *§ 13,* at klima-, energi- og forsyningsministeren kan fastsætte regler for virksomheders pligt til at underrette modtagere af deres tjenester, myndigheder eller juridiske personer, som udfører myndighedsopgaver, om trusler eller hændelser der kan påvirke eller har potentiale til at påvirke virksomhedens levering af tjenester.

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

Desuden vil bemyndigelsesbestemmelsen 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.

Ved udnyttelsen af bemyndigelsesbestemmelsen forudsættes det i overensstemmelse med NIS 2-direktivets præambelbetragtning nr. 103, at virksomheder 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 virksomheder 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.

I overensstemmelse med præambel betragtning nr. 103 i NIS 2-direktivet skal oplysninger om væsentlige cybertrusler stilles gratis til rådighed for modtagerne i et let forståeligt sprog.

Til § 14 [Kapitel 4]

Ifølge § 21, stk. 7, bekendtgørelse om it-beredskab for el- og naturgassektoren, kan Energinet efter høring af den meddelende virksomhed oplyse offentligheden om den konkrete hændelse, hvis offentlighedens kendskab hertil er nødvendigt for at forebygge en hændelse eller håndtere en igangværende hændelse.

Ifølge § 14, stk. 3, i bekendtgørelse om beredskab i oliesektoren, kan Energistyrelsen efter høring af den meddelende virksomhed i stk. 1 oplyse offentligheden om konkrete it-beredskabshændelser, hvis offentlighedens kendskab hertil er nødvendigt for at forebygge en hændelse eller håndtere en igangværende hændelse.

Efter den foreslåede § 14, *stk. 1,* kan klima-, energi- og forsyningsministeriet efter høring af en virksomhed, der er ramt af en hændelse, informere offentligheden om hændelsen, hvis offentliggørelsen er nødvendig for at forebygge eller håndterer hændelsen, eller hvor offentliggørelse af hændelsen på anden vis er i offentlighedens interesse.

Bestemmelsen vil – sammen med den foreslåede stk. 2 – gennemføre artikel 23, stk. 7, i NIS 2-direktivet.

Bestemmelsen gennemfører også artikel 15, stk. 4, sidst, i CER-direktivet.

Bestemmelsen skal forstås og anvendes i overensstemmelse med NIS 2- og CER-direktivernes forudsætninger.

Den foreslåede bestemmelse indebærer, at klima-, energi- og forsyningsministeren kan orientere offentligheden om en hændelse, hvis orienteringen er i offentlighedens interesse. Hvorvidt offentliggørelse er nødvendig for at forebygge eller håndtere en hændelse, eller hvorvidt offentliggørelse af hændelsen på anden vis er i offentlighedens interesse, vil afhænge af en konkret vurdering af sagens nærmere omstændigheder.

Offentliggørelse vil også kunne ske til en afgrænset del af offentligheden, eksempelvis sådan at offentliggørelse kun sker til andre virksomheder i energisektoren eller dele af denne sektor. Ligeledes vil offentliggøres kunne afgrænses til relevante aktører ud fra en vurdering af klima-, energi- og forsyningsministeren.

Klima-, Energi- og Forsyningsministeriet vil i medfør af bestemmelsen skulle høre den berørte enhed, før der sker offentliggørelse af hændelsen. Det forudsættes, at enheden så vidt muligt vil skulle have en rimelig frist til at afgive bemærkninger til høringen, dog uden at formålet med offentliggørelsen forspildes.

Formålet med høringen vil være at sikre, at klima-, energi- og forsyningsministeren kan træffe afgørelse om offentliggørelse på et oplyst grundlag, herunder foretage en afvejning af hensynet til den konkrete enhed over for

hensynet til orientering af offentligheden. Forhold som kan have betydning for vurderingen af, om der skal ske offentliggørelse er blandt andet; 1) antallet af brugere som er berørt af hændelsen, 2) hvilke sektorer som er ramt af hændelsen, 3) hvilke tjenester der er påvirket af hændelsen, 4) hvilke typer af oplysninger som hændelsen vedrører, 5) den indvirkning, som hændelser kunne have på økonomiske og samfundsmæssige aktiviteter, miljøet, den offentlige sikkerhed eller befolkningens sundhed.

Det bemærkes, at forvaltningslovens § 27, om offentlige ansattes tavshedspligt, skal overholdes ved vurderingen af, hvorvidt der skal ske orientering af offentligheden. Dette omfatter bl.a. hensynet til enkeltpersoners private forhold, forretningshemmeligheder samt hensynet til forebyggelse, efterforskning og forfølgning af lovovertrædelser. Desuden skal de hensyn som fremgår af den foreslåedes lovs kapitel 10 om fortrolighed indgå i overvejelser om orientering af offentligheden.

Der stilles ikke i bestemmelsen nærmere krav til formen for orienteringen. Orientering af offentligheden kan således ske på den måde, som klima-, energi- og forsyningsministeren finder bedst egnet under hensyn til den berørte virksomhed, hændelsens karakter, den geografiske udstrækning, den forventede betydning for bestemte dele af offentligheden m.v.

Rammer en hændelse flere sektorer, eller har en hændelse potentiale til at ramme flere sektorer, forudsættes det, at der forud for offentliggørelse sker en koordinering mellem de relevante kompetente myndigheder.

Det foreslås, at det som udgangspunkt er Klima-, Energi- og Forsyningsministeriet, der foretager offentliggørelsen af en væsentlig hændelse, jf. dog det foreslåede stk. 2, idet ministeriet vil være nærmest til at foretage afvejningen af virksomhedens eventuelle interesse i, at der ikke sker offentliggørelse over for hensynet til offentligheden.

Efter den foreslåede bestemmelse i § 15, *stk. 2,* kan klima-, energi- og forsyningsministeren i situationer efter stk. 1, kræve at virksomheden foretager offentliggørelse af hændelsen.

Den foreslåede bestemmelse vil gennemføre NIS 2-direktivets artikel 27, stk. 7, sidst. Hvorefter medlemsstater efter høring af en virksomhed, kan kræve at virksomheden informere offentligheden om hændelsen.

Efter den foreslåede bestemmelse, kan klima-, energi- og forsyningsministeren i situationer efter stk. 1, kræve at det er virksomheden som offentliggøre hændelsen. Offentliggørelsen af hændelsen skal dermed følge de samme kriterier og krav som er beskrevet ovenfor til stk. 1, og kan ikke ske uden forudgående høring af virksomheden.

Der henvises i øvrigt til bemærkningerne til § 14, stk. 1.

Til § 15 [Kapitel 4]

Det følger af den foreslåede bestemmelse i *§ 15,* at enhver kan underrette Klima-, Energi- og Forsyningsministeriet om væsentlige hændelser, cybertrusler og nærvedhændelser, der negativt påvirker eller vurderes at kunne påvirke tilgængelighed, integritet eller fortrolighed af data, informationssystemer, digitale netværk eller digitale servicer i energisektoren.

Den foreslåede bestemmelse indebærer, at alle offentlige og private virksomheder samt privatpersoner kan underrette Klima-, Energi- og Forsyningsministeriet om hændelser, der negativt påvirker eller vurderes at kunne påvirke tilgængelighed, integritet eller fortrolighed af data, informationssystemer, digitale netværk eller digitale services, hvilket indholdsmæssigt svarer til begrebet »sikkerhedshændelse« efter § 2, nr. 1, i lov om Center for Cybersikkerhed. Det bemærkes i den forbindelse, at begrebet »digitale services« skal forstås i overensstemmelse med begrebet »digitale tjenester« i lov om Center for Cybersikkerhed.

Underretning af Klima-, Energi- og Forsyningsministeriet ved større sikkerhedshændelser skaber de bedst mulige forudsætninger for, at Klima-, Energi- og Forsyningsministeriet kan udnytte erfaringer med cybertrusler og sikkerhedsrisici på tværs af samfundet – og dermed skabe et samlet overblik over den aktuelle sikkerhedstilstand i energisektoren i Danmark. Underretninger sætter således Klima-, Energi- og Forsyningsministeriet i stand til at varsle hurtigere om trusler og styrke grundlaget for rådgivningen om risici og passende sikkerhedstiltag.

Den foreslåede bestemmelse gennemfører NIS 2-direktivets artikel 30, stk. 1, litra a og b, hvorefter det følger af 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 om-

handlet i litra a), uanset om de er omfattet af dette direktivs anvendelsesområde, for så vidt angår væsentlige hændelser, cybertrusler og nærvedhændelser.

Det bemærkes at frivillige underretninger undtages fra aktindsigt efter lovens § 27. Der henvises i øvrigt til de specielle bemærkninger til lovforslagets § 27.

Til § 16 [Kapitel 5]

For at få adgang til klassificeret information stilles der krav om sikkerhedsgodkendelse i medfør af Justitsministeriets cirkulære nr. 10338 af 17. december 2014 om sikkerhedsbeskyttelse af informationer af fælles interesse for landene i NATO eller EU, andre klassificerede informationer samt informationer af sikkerhedsmæssig beskyttelsesinteresse i øvrigt (sikkerhedscirkulæret). Kravet om sikkerhedsgodkendelse efter sikkerhedscirkulæret gælder for ansatte i offentlige myndigheder, ansatte i private virksomheder, der løser opgaver for offentlige myndigheder, og ansatte i private virksomheder, hvis der i øvrigt i medfør af særlovgivning stilles krav om sikkerhedsgodkendelse for at udføre deres funktion.

Energistyrelsen træffer i dag afgørelser om sikkerhedsgodkendelser for så vidt angår ansatte og konsulenter i Energinet samt konsulenter, som indgår i samarbejdsforhold med Energistyrelsen i regi af den Nationale Operative Stab eller Lokale Beredskabsskaber efter Lov om Energinet og Sikkerhedscirkulæret. Energistyrelsen har ikke hjemmel til at sikkerhedsgodkende personer inden for energisektoren, der ikke er ansat i eller udfører opgaver for Energistyrelsen eller en anden offentlig myndighed. Desuden har klima-energi- og forsyningsministeren i dag ikke bemyndigelse til at fastsætte nærmere regler om sikkerhedsgodkendelse i energisektoren.

I perioden fra 2019 til 2023 har Energistyrelsen truffet afgørelser om sikkerhedsgodkendelse af personer inden for energisektoren, der ikke var ansat i eller udfører opgaver for Energistyrelsen, ud fra en retsvildfarelse om, at sikkerhedscirkulæret indeholdt hjemmel hertil.

Klima-, Energi- og Forsyningsministeriet vurderer, at der er behov for en hjemmel til sikkerhedsgodkendelse af personer, der har direkte adgang til at påvirke energiforsyningen, for at sikre fornødne personelsikkerhed i energisektoren.

Det følger af den foreslåede § 16, *stk. 1, 1. pkt.* at klima-, energi- og forsyningsministeren efter forhandling med justitsministeren kan fastsætte regler

om, at personer, der har direkte adgang til at påvirke forsyningen i energisektoren, skal sikkerhedsgodkendes af Klima-, Energi- og Forsyningsministeriet.

Ved direkte adgang til at påvirke energiforsyningen forstås ansatte og konsulenter med væsentlige fysiske eller logiske adgange og rettigheder, f.eks. fysisk adgang til virksomhedens kontrolrum eller virksomhedens forsyningskritiske anlæg, eller domænerettigheder eller lignende privilegerede rettigheder til virksomhedens kritiske systemer og netværk.

Bemyndigelsen forventes udmøntet ved udstedelse af en bekendtgørelse, der fastsætter nærmere regler for, hvilke personer i energisektoren der skal gennemgå sikkerhedsundersøgelse med henblik på afgørelse om sikkerhedsgodkendelse. Ved fastsættelse af regler herom vil der blive lagt vægt på, at sikkerhedsgodkendelser kun omfatter personer i virksomheden, der har direkte adgang til at påvirke energiforsyningen. Det forventes, at der f.eks. vil blive lagt vægt på personens konkrete opgaveroller i virksomheden samt virksomhedens forsyningsstørrelse og kritikalitet for den samlede energiforsyning i Danmark.

Efter den foreslåede bestemmelse forventes der også fastsat nærmere regler om kriterier for, på hvilke betingelser en virksomhed i energisektoren vil kunne anmode om sikkerhedsundersøgelse. Det bemærkes i den forbindelse, at gennemførelse af sikkerhedsgodkendelse vil ske på grundlag af en anmodning fra virksomheden og forudsætter, at vedkommende har meddelt samtykke dertil.

Det vil bero på en risikovurdering foretaget af virksomheden, hvilke personer eller personalegrupper der har direkte til at påvirke energiforsyningen i virksomheden.

Det følger af den foreslåede § 16, stk. *1, 2. pkt.*, at klima-, energi- og forsyningsministeren efter forhandling med justitsministeren kan fastsætte regler om ansøgning om, betingelser for og meddelelse og tilbagekaldelse af sikkerhedsgodkendelser.

Det forventes på den baggrund, at der fastsættes nærmere regler om ansøgning og afgørelser om sikkerhedsgodkendelser, samt meddelelse om og tilbagekaldelse af afgørelser om sikkerhedsgodkendelser. Dette omfatter bl.a. administrative krav i forbindelse med indgivelse af en ansøgning, hvilken myndighed der træffer afgørelse, krav om afmelding, hvis en person ikke længere har en funktion, som forudsætter en sikkerhedsgodkendelse, og bestemmelser om, at afgørelsen tilbagekaldes, hvis en person ikke længere opfylder kravene til godkendelsen.

På den baggrund forventes eksempelvis fastsat nærmere regler om, at det er virksomhedernes ansvar at foretage ID/CV-kontrol med tilfredsstillende resultat, inden der ansøges om sikkerhedsgodkendelser.

Det følger af den foreslåede *§ 16, stk. 2*, at klima-, energi- og forsyningsministeren efter forhandling med justitsministeren kan fastsætte nærmere regler om, på hvilke betingelser en virksomhed kan få foretaget baggrundskontrol af personer med henblik på at vurdere en potentiel sikkerhedsrisiko for virksomheden. Baggrundskontrollen kan efter bestemmelsens 2. pkt., angå personer, der: 1) varetager følsomme opgaver i eller til fordel for en kritisk enhed, navnlig vedrørende den kritiske enheds modstandsdygtighed, 2) er bemyndiget til at få direkte adgang eller fjernadgang til en kritisk enheds lokaler, oplysninger eller kontrolsystemer, herunder i forbindelse med den kritiske enheds sikkerhed eller 3) overvejes ansat i stillinger, der indebærer opgavevaretagelse efter nr. 1 og/eller nr. 2.

Den foreslåede bestemmelse gennemfører artikel 14, stk. 1, i 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), hvorefter medlemsstaterne angiver, på hvilke betingelser en kritisk enhed i behørigt begrundede tilfælde og under hensyntagen til medlemsstatsrisikovurderingen har tilladelse til at indgive anmodninger om baggrundskontrol af personer, der a) varetager følsomme opgaver i eller til fordel for en kritisk enhed, navnlig vedrørende den kritiske enheds modstandsdygtighed, b) er bemyndiget til at få direkte adgang eller fjernadgang til en kritisk enheds lokaler, oplysninger eller kontrolsystemer, herunder i forbindelse med den kritiske enheds sikkerhed, c) overvejes ansat i stillinger, der hører under kriterierne i litra a) eller b).

Baggrunden for CER-direktivets artikel 14, stk. 1, beskrives i præambelbetragtning nr. 32, hvoraf det bl.a. fremgår, at risikoen for, at ansatte i kritiske enheder eller deres kontrahenter misbruger for eksempel deres adgangsret inden for den kritiske enheds organisation til at skade og forvolde skade, giver anledning til stigende bekymring.

Efter den foreslåede bestemmelse vil klima-, energi- og forsyningsministeren efter forhandling med justitsministeren kunne fastsætte nærmere regler, der sammen med bestemmelsen vil skulle gennemføre CER-direktivets artikel 14.

Det foreslås, at klima-, energi- og forsyningsministeren bemyndiges til at fastsætte nærmere regler om, på hvilke betingelser en virksomhed i energisektoren vil kunne anmode om baggrundskontrol af en person, således at særlige sektorspecifikke hensyn kan varetages.

Det bemærkes i den forbindelse, at gennemførelse af baggrundskontrol vil ske på grundlag af en anmodning fra en virksomhed i energisektoren og forudsætter, at den pågældende person har meddelt samtykke dertil.

Bemyndigelsen i den foreslåede § 16, stk. 2, forventes udmøntet ved udstedelse af en bekendtgørelse, der fastsætter nærmere regler for, på hvilke betingelser virksomheder kan få foretaget baggrundskontrol af personer. Der vil i den forbindelse bl.a. kunne lægges vægt på, at den pågældende person har følsomme opgaver eller er bemyndiget adgang til virksomhedens lokaler. Det forventes i energisektoren at kunne være personer med uledsaget adgang til kontrolrum (f.eks. rengøringspersonale) eller adgang til forsyningsanlæg (f.eks. gartnere og vagter) eller softwareudviklere og konsulenter, som sidder med f.eks. vedligeholdelse og test af systemer, der anvendes til at styre og overvåge produktion, transmission og distribution af energi.

Det vil bero på en risikovurdering foretaget af virksomheden, hvilke personer eller personalegrupper, der vil være omfattet af reglerne om baggrundskontrol.

Det forudsættes i øvrigt, at udstedelse af nærmere regler og den efterfølgende administration af ordningen om baggrundskontrol efter den foreslåede *§ 16, stk. 2*, som minimum vil ske i overensstemmelse med kravene i CER-direktivets artikel 14, stk. 2 og 3.

Det fremgår bl.a. af CER-direktivets artikel 14, stk. 2, at anmodninger om baggrundskontrol vurderes inden for en rimelig frist og behandles i overensstemmelse med national ret og nationale procedurer samt relevant og gældende EU-ret, herunder EU-regulering om beskyttelse af personoplysninger. Baggrundskontrollen skal være forholdsmæssig og strengt begrænset til, hvad der er nødvendigt, og den skal udelukkende foretages med henblik på at vurdere en potentiel sikkerhedsrisiko for den berørte kritiske enhed.

CER-direktivets artikel 14, stk. 3, fastsætter bl.a., at baggrundskontrollen mindst skal bekræfte identiteten af den person, som er genstand for baggrundskontrollen, og at der skal foretages en kontrol af strafferegistre for den pågældende person for lovovertrædelser, der er relevante for en bestemt stilling.

Til § 17 [Kapitel 6]

Det følger af gældende ret i elforsyningslovens § 51d og gasforsyningslovens § 30 a, stk. 5-7 at de virksomheder der i dag er pålagt krav om beredskabsplanlægning, fysisksikring og cybersikkerhed i el- og gassektorerne halvårligt skal betale et beløb til Klima-, Energi- og Forsyningsministeriet til dækning af omkostningerne af ministeriets tilsyn med virksomhedernes overholdelse af regler udstedt i medfør af elforsyningslovens § 85 b, stk. 4 og 85 c, stk. 6, samt gasforsyningslovens § 15 a, stk. 4 og 15 b, stk. 6.

Gebyrernes størrelse er blevet fastsat ved bekendtgørelse i bekendtgørelse nr. 805 af 15. juni 2023 om betaling for myndighedsbehandling i Energistyrelsen. Gebyrerne er fastsat som generelle grundbeløb fordelt på 4 kategorier, gradueret således, at gebyret er størst for virksomheder i kategori 1 og lavest for virksomheder i kategori 4. De 4 gebyrkategorier for gebyropkrævningen er baseret på den kategorisering, der foretages af virksomhederne efter it-beredskabsbekendtgørelsen dog under hensyntagen til antallet af klasse 1 anlæg som virksomheden ejer. Klassificeringen af anlæg foretages efter elberedskabsbekendtgørelsen og naturgasberedskabsbekendtgørelsen.

Efter gældende ret er følgende aktiviteter og opgaver gebyrfinansieret: Hvilke opgaver/aktiviteter er refusionsberettiget: Godkendelse af beredskabsmateriale, herunder; dialog om mangler, fejl, rykkere (Efter indsendelse til tilsyn), tid brugt på fysiske tilsyn, herunder; forberedelse af tilsyn (udarbejdelse af skabeloner, læse beredskabsmateriale, booke rejse o.lign.), rejsetid til og fra virksomheden, udarbejdelse af tilsynsrapport samt nødvendig uddannelse af medarbejder der skal foretage tilsyn.

Følgende opgaver/aktiviteter er ikke gebyrfinansieret efter gældende ret: udarbejdelse af vejledningsmateriale, vejledning om krav til beredskabsmateriale (før indsendelse til tilsyn), udarbejdelse af påbud eller politianmeldelser, udarbejdelse/revision af lovgivning.

Endvidere er der visse andre udgifter som Klima-, Energi- og Forsyningsministeriet afholder som led i administrationen af ordningen, der ligeledes ikke er omfattet af den gældende gebyrfinansiering. Disse er udgifter til klassificering af virksomhedernes anlæg og niveauinddeling af virksomhederne efter reglerne i § 4, udarbejdelse af risiko og sårbarhedsscenarier, som virksomhederne skal bruge i deres risiko og sårbarhedsvurderingsarbejde, den halvårlige gebyropkrævning af virksomhederne, herunder indhentelse

af faktureringsoplysninger fra virksomhederne, vejledningen af virksomhederne i reglernes konkrete anvendelse på deres virksomhed, samt håndtering af hændelsesindberetninger fra virksomhederne.

Endeligt er klima-, energi- og forsyningsministerens tilsyn med det almene beredskab og it-beredskabet hos Energinet siden den 1. juli 2019 blevet finansieret via lovfastsat grundbeløb i elforsyningslovens § 51 b og gasforsyningslovens § 30 a, stk. 3, hvor beløbet er en delmængde af et større beløb, der opkræves for tilsyn med Energinets aktiviteter efter de to love. klima-, energi- og forsyningsministeren opkræver i dag årligt gebyr for 1000 timers tilsyn med Energinets almene beredskab og it-beredskab. De 1000 timer er lovmæssigt fordelt med 600 timer til Energinets El TSO og 400 timer til Energinets Gas TSO, hvilket efter Energistyrelsens 2024 timetakts for en gennemsnitsmedarbejder på 746,68 kr. svarer til 746.680 kr. Der er i tillæg til de 1000 timeres tilsyn, som Energistyrelsen fører, også finansieret 50 timers ekstern konsulentbistand til tilsyn med it-beredskab pga. områdets særlige tekniske karakter. Denne udgift udgjorde 62.500 kr., da man anlagde en formodning om at en konsulent kostede 1250 kr. i timen.

Det foreslås i § 17, *stk. 1,* at virksomheder omfattet af loven halvårligt skal betale et beløb til Klima-, Energi- og Forsyningsministeriet til dækning af de omkostninger til tilsyn med virksomhederne efter reglerne i denne lov og regler udstedt i medfør af denne lov. Den halvårlige betaling er en fortsættelse af den hidtidige frekvens for betaling for tilsyn med virksomhedernes beredskabsarbejde. Den halvårlige frekvens sikrer, at der ikke skal betales for store beløb ad gangen, samt at opkrævningen kan finde sted i samme frekvens som andre betalinger for myndighedsbehandling efter elforsyningsloven, gasforsyningsloven og olieberedskabsloven.

Konsekvensen af det foreslåede stk. 1 er, at der sker en udvidelse af den gebyrordning der i dag finansierer klima-, energi- og forsyningsministerens tilsyn med el- og naturgasvirksomhedernes beredskab efter § 85 b og 85 c i elforsyningsloven og § 15 a og b i gasforsyningsloven og regler udstedt i medfør af disse paragraffer. Efter gældende ret efter § 51 d i elforsyningsloven og § 30 a, stk. 5 i gasforsyningsloven og fortsat efter den forslåede § 17, stk. 1, skal virksomhederne betale administrativt fastsatte gebyrer for det tilsyn, de modtager fra klima-, energi og forsyningsministeren. Gebyrerne vil blive fastsat som generelle grundbeløb, der dækker de udgifter som Klima-, Energi- og Forsyningsministeriet har med administration og tilsyn med ordningen. De gældende § 51 d i elforsyningsloven og § 30 a, stk. 5 i

gasforsyningsloven foreslås samtidigt ophævet i disse love, da de i stedet erstattes af den foreslåede § 18, stk. 1.

Udgifterne, der afholdes under den foreslåede stk. 1, er hovedsageligt forbundet med det direkte tilsyn med virksomhedernes overholdelse af reglerne i loven og regler udstedt i medfør af loven. Herunder forberedelse af tilsynet, såsom indhentning af materiale, udsendelse af selvevalueringsskemaer, planlægning af tilsynet i dialog med virksomheden, effektiv transport til og fra virksomheden, afholdelsen af selve det fysiske tilsyn, udgift til eventuel kost og logi i forbindelse med tilsynet, opfølgning på tilsynet, nødvendig uddannelse, efteruddannelse, certificering og recertificering af medarbejderne til at føre tilsynet samt udarbejdelse af påbud eller politianmeldelser. Hertil kommer udgifter til skrivebordstilsynet, der bliver ført i forbindelse med godkendelse af virksomhedernes konklusioner fra risiko og sårbarhedsvurderingerne, beredskabsplaner, it-beredskabsplaner øvelsesplaner, øvelsesindberetninger og hændelser-som-øvelser samt kontrakter med proaktive og reaktive it-sikkerhedstjenester.

Det foreslås med § 17, stk. 1 at udgifter som Klima-, Energi- og Forsyningsministeriet afholder som led i administrationen af ordningen, ligeledes skal finansieres af de generelle grundbeløb i § 17, stk. 1. Disse er udgifter til klassificering af virksomhedernes anlæg og niveauinddeling af virksomhederne efter reglerne i § 4, udarbejdelse af risiko og sårbarhedsscenarier, som virksomhederne skal bruge i deres risiko og sårbarhedsvurderingsarbejde, den halvårlige gebyropkrævning af virksomhederne, herunder indhentelse af faktureringsoplysninger fra virksomhederne, vejledningen af virksomhederne i reglernes konkrete anvendelse på deres virksomhed, samt håndtering af hændelsesindberetninger fra virksomhederne.

Følgende udgifter er forsat ikke finansieret af det foreslåede gebyr i § 17, stk. 1, udarbejdelse af generelt vejledningsmateriale og udarbejdelse/revision af lovgivning.

Det foreslås i § 17, *stk. 2*, at virksomheder ligeledes halvårligt skal betale et beløb til Klima-, Energi- og Forsyningsministeriet til dækning af omkostninger til ad-hoc tilsyn med virksomhederne efter reglerne i denne lov eller efter regler udstedt i medfør af regler i denne lov. Dette gebyr vil blive beregnet individuelt for hver virksomhed, der måtte modtage ad-hoc tilsyn med overholdelsen af reglerne i denne lov eller efter regler udstedt i medfør af denne lov. Gebyret vil være et aktivitetsbaseret gebyr, og vil derfor blive beregnet ud fra antallet af timer, der er medgået til udførelsen af aktiviteten

(ad-hoc tilsynet), ganget med den budgetterede timesats. De udgifter, der kan henregnes til dette gebyr, er de samme som for de generelle grundbeløb virksomhederne skal betale efter stk. 1, med undtagelse af udgifter og timer brugt til nødvendig uddannelse, efteruddannelse, certificering og recertificering af medarbejderne, da disse udgifter allerede er inddækket af de generelle grundbeløb.

Virksomheder vil efter det foreslåede stk. 2 blive faktureret for alle timer, der er pågået ad-hoc tilsynet. Herunder også timer der er brugt i forbindelse indhentning af oplysninger, nærmere undersøgelse af faktiske forhold og vurdering af om ad-hoc tilsyn skal indledes med den pågældende virksomhed, dog kun i de tilfælde hvor der faktisk indledes ad-hoc tilsyn med virksomheden. Fører indhentning af oplysninger, undersøgelse af faktiske forhold og vurdering af om ad-hoc tilsyn skal indledes til, at der ikke skal indledes ad-hoc tilsyn, så afholdes udgiften af tilsynsmyndigheden. Timefaktureringen forsætter til det tidspunkt, hvor tilsynsmyndigheden fremsender endelig afgørelse om tilsynet.

Det foreslås i § 17, *stk. 3,* at klima-, energi- og forsyningsministeren fastsætter regler om størrelsen, betaling og opkrævning af beløb efter stk. 1 og 2, herunder om fordelingen af omkostningerne på kategorier af virksomheder.

Det forventes, at bemyndigelsen vil blive udmøntet således, at der i reglerne for betaling af gebyret efter den foreslåede § 17, stk. 1 vil blive angivet kriterier for virksomheders inddeling i de nævnte kategorier i punkt 3.5.3 i de almindelige bemærkninger, samt hvad gebyret for hver af kategorierne er fastsat til. Det forventes endvidere, at Energistyrelsen vil kunne justere gebyrerne, så de afspejler antallet og størrelsen af de virksomheder i sektorerne, der føres tilsyn med.

Det forventes endvidere at klima-, energi- og forsyningsministeren bruger bemyndigelsen i stk. 3 til at fastsætte, at gebyrer opkrævet efter den foreslåede § 17, stk. 2, vil blive opkrævet som timeafregnede gebyrer, baseret på det samlede antal medgåede timer til ad-hoc tilsyn ganget med den budgetterede timepris i Energistyrelsen, i det år hvor ad-hoc tilsynet afholdes, idet tilsynet som beskrevet i den foreslåede § 19, stk. 2, nr. 3 forventes delegeret til Energistyrelsen.

Der vil således være en fuld omkostningsdækning for Energistyrelsen, hvilket betyder, at udgifterne forbundet med tilsynet og administrationen af ordningen modsvares af de samlede opkrævninger. Ordningen vil dermed hvile i sig selv. Dette vil sikre, at princippet om proportionalitet mellem den ydelse, som virksomheden får, og det gebyr, der opkræves herfor, overholdes.

Det følger af endvidere af det foreslåede § 18, stk. 7, at energi-, forsynings- og klimaministeren vil kunne fastsætte nærmere regler om betaling og opkrævning af det i stk. 1 og stk. 2 nævnte beløb. Det forventes, at der vil blive fastsat regler om, at betalingerne skal ske efter halvårlige fakturaer. Det forventes også, at der vil blive fastsat regler om, at betalingerne skal ske til Energistyrelsen. Det forventes herudover, at der fastsættes regler om efterregulering af beløbet, der betales, så det sikres, at virksomhederne ikke betaler for meget eller for lidt. Det forventes ligeledes, at der fastsættes regler om, hvor hurtigt virksomhederne skal indbetale beløbet efter udstedelse af fakturaen. Det forventes endvidere, at der fastsættes regler om, at der skal betales renter i medfør af renteloven, såfremt der ikke betales rettidigt.

Der henvises til pkt. 3.5 i de almindelige bemærkninger.

Til § 18 [Kapitel 6]

Det foreslås i § 18, *stk. 1,* at virksomheder betaler halvårligt gebyr for behandling af ansøgninger og dispensationer efter reglerne i denne lov eller efter regler udstedt i medfør af loven. Klima-, Energi og Forsyningsministeriet foreslår med bestemmelsen, at virksomheder skal betale et fast vederlag pr. ansøgning efter loven eller regler udstedt i medfør af loven, differentieret alt efter hvad det er der ansøges om. Der tænkes således på virksomheders ansøgninger om samordnet beredskab, ansøgninger om personsammenfald, ansøgning om dispensation efter den generelle dispensationsregel, ansøgning om sikkerhedsgodkendelse af en medarbejder, ansøgning om baggrundskontrol af en medarbejder samt andre ansøgninger der er virksomhedens egen interesse. Reglen finder anvendelse på ansøgninger, uagtet om virksomhederne er tvunget til at ansøge om godkendelsen pga. krav herom i regler efter denne lov eller regler udstedt i med før af denne lov eller ej.

Det foreslås i § 18, *stk. 2,* at Klima-, energi- og forsyningsministeren fastsætter regler om størrelsen, betaling og opkrævning af beløb efter stk. 1. Det forventes af denne bemyndigelse vil blive udmøntet ved at klima-, energi-

og forsyningsministeren administrativt fastsætter et eller flere engangsvederlag, der skal betales pr. ansøgning, som virksomheden indgiver til Energistyrelsen. Betaling afhænger ikke af om virksomheden opnår godkendelse af deres ansøgning eller ej. Der skal således betales blot fordi Energistyrelsen, der forventes at blive delegeret behandlingen af sådanne ansøgninger, skal realitetsbehandle en ansøgning. Det forventes, at ansøgningstyper, der estimeres til gennemsnitligt at have det samme sagsomfang og derfor også sagsbehandlingstid, får fastsat det samme størrelse engangsvederlag.

Det forventes, at gebyrerne for de enkelte ansøgningstyper i første omgang vil blive fastsat på baggrund af klima-, energi- og forsyningsministerens initiale estimering af hvor mange timer det gennemsnitligt tager at behandle en sådan ansøgning ganget med den budgetteret timepris. Efter der er opbygget et tilstrækkeligt datagrundlag gennem medarbejdernes tidsregistrering, vil de initiale estimering erstattes af det konkrete gennemsnitlige tidsforbrug pr. ansøgningstype, hvorefter de fastsatte gebyrer vil blive op- eller nedjusteret på dette grundlag, ligesom hvis den budgetterede timepris ændrer sig, idet gebyrordningen skal balancere over en 4-årig periode i overensstemmelse med Finansministeriets budgetvejledning.

Klima-, energi- og forsyningsministeren bemyndiges i medfør af den foreslåede bemyndigelse i § 18, stk. 2 til at anvende den til enhver tid gældende budgetterede timepris hos den myndighed til hvem tilsynet delegeres til, til fastsættelsen af beløbene der skal betales. Den budgetterede timepris fastsættes på grundlag af gennemsnitlige lønudgifter tillagt en forholdsmæssig andel af generelle fællesomkostninger, relevante henførbare, indirekte omkostninger og direkte øvrige driftsomkostninger, der er forbundet med myndighedsbehandlingen i det pågældende regnskabsår. Energistyrelsens omkostningsfordeling vil følge Finansministeriets vejledninger herfor.

Der vil således være en fuld omkostningsdækning for Energistyrelsen, hvilket betyder, at udgifterne forbundet med tilsynet og administrationen af ordningen modsvares af de samlede opkrævninger. Ordningen vil dermed hvile i sig selv. Dette vil sikre, at princippet om proportionalitet mellem den ydelse, som virksomheden får, og det gebyr, der opkræves herfor, overholdes.

Det forventes derfor ligeledes, at klima-, energi- og forsyningsministeren udmønter bemyndigelsen i stk. 2, således at hvis virksomheden indleverer en mangelfuld ansøgning, så betales der gebyr for behandlingen (afvisningen) af både den ufuldstændige og den endelige ansøgning.

Det følger af endvidere af det foreslåede § 18, *stk. 2*, at klima-, energi- og forsyningsministeren vil kunne fastsætte nærmere regler om betaling og opkrævning af det i stk. 1 og stk. 2 nævnte beløb. Det forventes, at der vil blive fastsat regler om, at betalingerne skal ske efter halvårlige fakturaer. Det forventes også, at der vil blive fastsat regler om, at betalingerne skal ske til Energistyrelsen. Det forventes endvidere, at der fastsættes regler om efterregulering af beløbet, der betales, så det sikres, at virksomhederne ikke betaler for meget eller for lidt. Det forventes herudover, at der fastsættes regler om, hvor hurtigt virksomhederne skal indbetale beløbet efter udstedelse af fakturaen. Det forventes ligeledes, at der fastsættes regler om, at der skal betales renter i medfør af renteloven, såfremt der ikke betales rettidigt.

Der henvises til pkt. 3.5 i de almindelige bemærkninger.

Til § 19 [Kapitel 7]

Ifølge elforsyningslovens § 85 b, stk. 1, skal virksomheder, som er bevillingspligtige efter §§ 10 og 19 eller har tilladelse til elproduktion fra anlæg med en kapacitet på over 25 MW efter § 29 i lov om fremme af vedvarende energi eller § 11, samt elforsyningsvirksomhed, der varetages af Energinet eller denne virksomheds helejede datterselskaber i medfør af § 2, stk. 2 og 3, i lov om Energinet, foretage nødvendig planlægning og træffe nødvendige foranstaltninger for at sikre elforsyningen i beredskabssituationer og andre ekstraordinære situationer. Denne bestemmelse vedrører alene den fysiske sikring og det fysiske beredskab for virksomhederne.

Efter elforsyningslovens § 85 b, skt. 4, kan klima-, energi- og forsyningsministeriet kan fastsætte nærmere regler for udførelsen tilsyn af med det beredskabsarbejde efter stk. 1. De nærmere regler for tilsyn er fastsat i bekendtgørelse om beredskab for elsektoren i bekendtgørelsens kapitel 10. Efter bekendtgørelsen er energistyrelsen tilsynsmyndigheden.

Ifølge gasforsyningslovens § 15 a, stk. 1, skal selskaber, der er bevillingspligtige efter § 10, samt Energinet og denne virksomheds helejede datterselskaber, der varetager gasvirksomhed i medfør af § 2, stk. 2 og 3, i lov om Energinet skal foretage nødvendig planlægning og træffe de nødvendige foranstaltninger for at sikre gasforsyningen i beredskabssituationer og andre ekstraordinære situationer. Denne bestemmelse vedrører alene den fysiske sikring og det fysiske beredskab for selskaberne.

Klima-, energi- og forsyningsministeren kan på baggrund af gasforsyningslovens § 15 a, stk. 4, fastsætte nærmere regler for udførelsen af selskabernes beredskabsarbejde. De nærmere regler for tilsyn er fastsat i bekendtgørelsen om beredskab for naturgassektoren. Energistyrelsen er tilsynsmyndigheden for selskabernes overholdelse af beredskabsreguleringen.

Ifølge elforsyningslovens § 85 c, stk. 1, skal virksomheder, som er bevillingspligtige efter §§ 10 og 19 eller har tilladelse til elproduktion fra anlæg med en kapacitet på over 25 MW efter § 29 i lov om fremme af vedvarende energi eller § 11, Energinet og dennes helejede datterselskaber samt virksomheder, der yder balancering af elsystemet, skal opretholde et it-beredskab, herunder planlægge og træffe nødvendige foranstaltninger for at sikre beskyttelsen af kritiske it-systemer, der er af betydning for elforsyningen. Ifølge gasforsyningslovens § 15 b, stk. 1, skal selskaber, der er bevillingspligtige efter § 10, samt Energinet og dennes helejede datterselskaber, der varetager gasforsyningsvirksomhed i henhold til § 2, stk. 2 og 3, i lov om Energinet, skal opretholde et it-beredskab, herunder planlægge og træffe nødvendige foranstaltninger for at sikre beskyttelsen af kritiske it-systemer, der er af væsentlig betydning for gasforsyningen. Bestemmelserne vedrører alene sikringen og beredskabet af virksomhedernes kritiske it-systemer

Efter elforsyningslovens § 85 c, stk. 6 og gasforsyningslovens § 15 b, stk. 6, fastsætter klima-, energi- og forsyningsministeren nærmere regler for udførelsen af tilsyn med virksomhedernes it-beredskab efter stk. 1. De nærmere regler for tilsyn er fastsat i bekendtgørelse om it-beredskab for el- og naturgassektorerne. Efter bekendtgørelsen er Energistyrelsen tilsynsmyndigheden.

Ifølge olieberedskabslovens § 17, stk. 1, fører klima-, energi- og forsyningsministeren tilsyn med, at loven og regler udstedt i henhold til loven overholdes. Olieberedskabslovens indeholder i § 16, beredskabspligter for virksomheder omfattet af loven. Klima-, energi- og forsyningsministeren fører således tilsyn med olievirksomhedernes beredskab. Efter olieberedskabslovens § 17, stk. 5, kan klima-, energi og forsyningsministeren fastsætte nærmere regler om fremsendelse af oplysninger til brug for tilsyn, om virksomhedernes medvirken i tilsyn og om virksomhedernes fremsendelse af revisorerklæring. De nærmere regler er fastsat i bekendtgørelse om beredskab for oliesektorens § 18.

Der er ikke nærmere regler for tilsyn af virksomheders beredskab i fjernvarme og -kølesektoren.

Det følger af den foreslåede § 19, *stk. 1*, at klima-, energi- og forsyningsministeren fører tilsyn med om virksomhederne opfylder sine forpligtelser i henhold til loven og regler fastsat i medfør af loven. Efter den foreslåede bestemmelse skal klima-, energi- og forsyningsministeren således føre tilsyn med virksomheder i sektorerne for el, gas, olie samt fjernvarme og -køling.

Det følger af den foreslåede § 19, *stk. 2*, at klima-, energi og forsyningsministeren kan, som led i tilsyn ud fra en konkret vurdering af omstændigheder, anvende følgende tilsynsforanstaltninger over for virksomhederne: 1) Foretage kontrol hos virksomheden og inspicere de lokaler virksomheden bruger til at levere sine tjenester samt foretage stikprøvekontrol. 2) Foretage regelmæssige kontrol- og tilsynsbesøg hos virksomheder. 3) Foretage ad hoc-audits. 4) Foretage sikkerhedsscanninger og penetrationstests af virksomhedens net- og informationssystemer samt fysiske lokationer. Tilsynsmyndigheden er ansvarlig for eventuelle skader virksomheden pådrager sig med disse test. 5) Kræve at få udleveret oplysninger, der er nødvendige for at vurdere de foranstaltninger til net- og informationssystemer samt modstandsdygtighed, som virksomheden har indført efter loven og regler udsted i medfør af loven. 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.

Den foreslåede bestemmelse vil gennemføre artikel 32, stk. 1 og 2, i NIS 2-direktivet og artikel 21, stk. 1 og 2, i CER-direktivet.

Det følger af NIS 2-direktivets artikel 32, stk. 1, at medlemsstater skal sikre, at de tilsynsforanstaltninger, der pålægges virksomheder, for så vidt angår forpligtelser fastsat i direktivet, er effektive og er forholdsmæssige under hensyntagen til omstændighederne i hver enkelt sag. Efter CER-direktivet skal medlemsstater sikre, tilsynsbeføjelserne kun kan udøves med forbehold af passende garantier. Disse garantier skal navnlig sikre, at en sådan udøvelse finder sted på en objektiv, gennemsigtig og forholdsmæssig måde, og at de berørte kritiske enheders rettigheder og legitime interesser såsom beskyttelse af forretningshemmeligheder garanteres behørigt, herunder deres ret til at blive hørt, til et forsvar og til effektive retsmidler ved en uafhængig domstol.

Efter bestemmelsen i NIS 2-direktivet artikel 32, stk. 2, skal medlemsstaterne sikre, at de kompetente myndigheder, når de udfører deres tilsynsopgaver vedrørende virksomheder, som minimum har beføjelse til at pålægge virksomhederne; 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 bestemmelsen i CER-direktivets artikel 21, stk. 1, skal medlemsstater sikre at de kompetente myndigheder har beføjelser og midler til; a) at foretage inspektioner på stedet af den kritiske infrastruktur og de lokaler, som den kritiske enhed anvender til at levere sine væsentlige tjenester, og eksternt tilsyn med de foranstaltninger, som kritiske enheder har truffet, b) at foretage eller kræve revision af kritiske enheder. Efter CER-direktivets artikel 21, stk. 2, skal medlemsstaterne sikre, at de kompetente myndigheder har beføjelser og mider til, hvor det er nødvendigt for udførelsen af deres opgaver i henhold til dette direktiv, at kræve, at kritiske enheder, inden for en rimelig tidsfrist, giver; a) de oplysninger, der er nødvendige for at vurdere, hvorvidt de foranstaltninger, der træffes af disse enheder for at sikre deres modstandsdygtighed, b) dokumentation for faktisk gennemførelse af disse foranstaltninger, herunder resultaterne af en revision foretaget af en uafhængig og kvalificeret revisor udvalgt af denne enhed og foretaget på dennes regning.

Det bemærkes at der efter direktivernes bestemmelser, fremgår, at der kan foretages »eksternt tilsyn«, hvilket er en formulering, der efter Klima-,

Energi- og Forsyningsministeriet opfattelse kan give anledning til fortolkningstvivl. I den engelske sprogversion af NIS 2-direktivet anvendes formuleringen »off-site supervision«. Efter Klima-, Energi- og Forsyningsministeriets opfattelse udgør eksternt tilsyn, forstået som off-site supervision, et tilsyn uden fysisk tilstedeværelse *på stedet*, altså eksempelvis udført på skriftligt grundlag. Disse former for tilsyn kan beskrives som administrative tilsyn.

Det bemærkes ligeledes at NIS 2-direktivets, artikel 32, stk. 2, litra a anvender udtrykket »på stedet«, Klima-, Energi- og Forsyningsministeriet vurderer at dette udtryk kan forstås i overensstemmelse med CER-direktivets artikel 21, stk. 1, litra a. Kontrol »på stedet« må efter Klima-, Energi- og Forsyningsministeriet opfattelse omfatte både; 1) områder, hvor virksomhederne har materiale eller anlæg, som anvendes til at levere virksomhedens tjeneste og 2) lokaler, som virksomheden anvender til at levere sine tjenester. Klima-, Energi- og Forsyningsministeriet vurderer at udtrykket »hos virksomheden« vil lede til mindre fortolkningstvivl og samtidig dække over udtrykket »på stedet«. Det foreslås derfor, at bestemmelsen anvender udtrykket »hos virksomheden«.

Baggrunden for artikel 21, stk. 1, og stk. 2, 1. pkt., er beskrevet i CER-direktivets præambelbetragtning nr. 40, hvoraf det bl.a. fremgår, at medlemsstaterne bør sikre, at deres kompetente myndigheder har visse specifikke beføjelser til at sikre en korrekt anvendelse og håndhævelse af direktivet i forbindelse med kritiske enheder, når disse enheder hører under deres jurisdiktion som fastsat i direktivet.

Det bemærkes, at de dele af direktivernes bestemmelser, der angår rent myndighedsinterne forhold, eller som allerede følger af almindelige forvaltningsretlige principper eller den almindelige adgang til domstolsprøvelse, ikke er afspejlet i lovteksten. Den foreslåede bestemmelse vil således fokusere på, hvilke konkrete tilsynsforanstaltninger de kompetente myndigheder vil kunne anvende over for enhederne.

Eksempelvis er CER-direktivets artikel 21, stk. 4, ikke afspejlet direkte i lovteksten. Det følger af den nævnte artikel, at medlemsstaterne skal sikre, at de tillagte beføjelser kun kan udøves med forbehold af passende beskyttelsesforanstaltninger, og at disse beskyttelsesforanstaltninger navnlig skal sikre, at en sådan udøvelse finder sted på en objektiv, gennemsigtig og forholdsmæssig måde, og at de berørte kritiske enheders rettigheder og legitime interesser såsom beskyttelse af forretningshemmeligheder garanteres

behørigt, herunder deres ret til at blive hørt, til et forsvar og til effektive retsmidler ved en uafhængig domstol. Det samme gælder eksempelvis CER-direktivets artikel 21, stk. 5, som overordnet fastsætter krav til samarbejde mellem de kompetente myndigheder efter henholdsvis NIS 2-direktivet og CER-direktivet.

Ligeledes fremgår det af NIS 2-direktivets artikel 32, stk. 2, litra a, om at 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.

Klima-, Energi- og Forsyningsministeriet har vurderet at der i energisektoren er et behov for regelmæssige kontrolbesøg hos virksomheder i energisektoren uagtet om virksomhederne efter NIS 2-direktivet må anses for at være vigtige eller væsentlige enheder, da energisektoren leverer tjenester til mange sektorer af særlig kritisk betydning. De regelmæssige kontrolbesøg omfatter både proaktive og reaktive kontrolbesøg. Den foreslåede bestemmelse vil dermed gå videre end minimumskravene i NIS2- og CER-direktiverne. Bestemmelsen skal derudover forstås og anvendes i overensstemmelse med direktivets forudsætninger og eventuelle fortolkningsbidrag fra Kommissionen, ENISA eller andre af EU's institutioner.

I overensstemmelse med forudsætningerne i NIS 2-direktivets præambelbetragtning nr. 123 bør udførelsen af tilsynsopgaven ikke unødigt hæmme den berørte virksomheds forretningsaktiviteter. Hvor en tilsynsmyndighed udfører sin tilsynsopgave vedrørende en virksomhed, 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 tilsynsmyndigheden myndighed minimere indvirkningen på den berørte enheds forretningsaktiviteter.

Tilsynsmyndigheden bør desuden videreføre den tilsynspraksis der har været gældende indenfor de allerede omfattede virksomheder og sektorer. Praksissen har hidtil været, at tilsynsmyndigheden har ført tilsyn ud fra en dialogbaseret og værdiskabende tilgang. Formålet med tilsyn er således at dele erfaringer mellem myndigheder og virksomheder for at opnå en mere sikker sektor. Hensynet til samarbejde og værdiskabelse af sikkerhed i energisektoren, bør således også indgå i en proportionalitetsvurdering ved anvendelsen af tilsynsforanstaltninger, håndhævelsesforanstaltninger eller sanktioner.

Det foreslås i § 19, *stk. 3,* at klima-, energi- og forsyningsministeren kan fastsætte nærmere regler om tilsyn og kontrol af virksomhederne, herunder omfanget, udførelsen og hyppigheden af tilsyns- og kontrolbesøg. Med den foreslåede bestemmelse bemyndiges ministeren til at fastsætte nærmere regler både for det administrative tilsyn af virksomheder, men også kontrol- og tilsynsbesøg hos virksomhederne.

Efter bestemmelsen vil de nærmere regler, som ministeren kan fastsætte regler om, blandt andet være »omfanget« af tilsyns- og kontrolbesøg. Udtrykket omfanget skal forstås bredt, i den forstand det både kan relatere sig til det tidsmæssige omfang af tilsynet og i hvilken geografisk udstrækning, der skal ske tilsyn med virksomheden.

Ministeren kan desuden fastsætte nærmere regler om udførelsen af tilsyn. Bestemmelsen vil medføre at ministeren kan fastsætte nærmere regler om tilsynet skal ske ved et fysisk tilsyn med fremmøde hos virksomheden eller om tilsynet skal ske som et eksternt tilsyn. Ministeren vil ligeledes kunne fastsætte nærmere regler, for hvad et fysisk tilsyn vil indebære. Eksempelvis kan der fastsættes regler om, at tilsynsmyndigheden skal have adgang til særlige områder som serverrum, for at observere at der er den korrekte sikkerhed.

Efter bestemmelsen vil ministeren også kunne fastsætte nærmere regler om hyppigheden af tilsyn. Der vil i den forbindelse kunne fastsættes regler om, at tilsyn skal ske årligt eller efter anden frekvens som kan være forskellige fra virksomhed til virksomhed. Der kan desuden fastsættes regler om, at der kan ændres op og ned i frekvensen af tilsyn for virksomheder på baggrund af tidligere tilsyn af samme virksomhed.

Den foreslåede bemyndigelsesbestemmelse vil også medføre, at der kan fastsættes regler om den tidsmæssige og geografiske udstrækning af tilsyn, der er proportionelle med den type virksomhed, som der skal føres tilsyn hos. Dette findes hensigtsmæssigt af hensyn til at virksomheder inden for energisektoren, der kontroller energimængder af en vis størrelse, kan have en betydelig effekt på den samlede forsyningssikkerhed i Danmark. Sådanne virksomheder kan anvende komplekse net- og informationssystemer som kræver et længerevarende tilsyn, for at systemer i tilstrækkeligt grad kan undersøges om virksomheden efterlever de gældende krav. Størrelsen af virksomheder og mængden af tjenester som virksomheden leverer, kan også påvirke den samlede kompleksitet, som bør understøttes af regler om længere og mere dybdegående tilsyn. Desuden kan virksomheder også

strække sig over mange lokaliteter, hvor hver lokation hos virksomheden kan introducere nye og særegne trusler. Modsatvis findes der også virksomheder inden for sektoren, som kun i mindre grad kan påvirke energiforsyning. Disse virksomheder kan være mindre komplekse og et tilsyn kan udføres i tilstrækkelig grad på mindre tid og i begrænset geografisk udstrækning. Bestemmelsen har derfor til formål, at der med udviklingen i sektoren kan fastsættes regler om den tidsmæssige og geografiske udstrækning af tilsyn, der er proportionelle med den type virksomhed der skal føres tilsyn hos.

På baggrund af det ovenstående, forventes det, at den foreslåede bestemmelse vil blive anvendt til at fastsætte differentierede regler om tilsyn. Det forventes, at der vil blive fastsat regler, hvorefter virksomheder inddeles i forskellige kategorier eller niveauer, som fastsættes ud fra både objektive og skønsmæssige kriterier om virksomhedens kritikalitet. Omfanget, udførelsen og hyppigheden af tilsyn hos virksomheder forventes at blive baseret på denne niveauinddeling.

Det foreslås i § 19, *stk. 4*, at klima-, energi- og forsyningsministeren kan fastsætte regler om udlevering og dokumentation af tilsynsmateriale og formkrav til tilsynsmateriale, herunder regler om hvilke sprog materialet skal udarbejdes på.

Den foreslåede bestemmelse vil medføre, at ministeren kan fastsætte regler om, at oplysninger eller materiale til brug for tilsyn udleveres på en bestemt måde, på et bestemt sprog og i en bestemt form.

Eksempelvis vil der kunne fastsættes regler om, at virksomhederne skal anvende bestemte skemaer eller skabeloner ved udleveringen af tilsynsmateriale. Ligeledes vil der kunne fastsættes regler om, at virksomhederne forpligtes til at registrere visse oplysninger ved brug af en bestemt hjemmeside.

Der vil eksempelvis kunne stilles krav om anvendelse af bestemte skemaer eller skabeloner. Der vil også kunne stilles krav om at der skal foretages indtastninger på en hjemmeside.

Der henvises i øvrigt til afsnit 3.6 i lovforslagets almindelige bemærkninger.

Til § 20 [Kapitel 7]

Rådets direktiv 2008/114/EF af 8. december 2008 om indkredsning og udpegning af europæisk kritisk infrastruktur og vurdering af behovet for at beskytte den bedre indeholder ikke bestemmelser om rådgivende EU-delegationers adgang til oplysninger, systemer og faciliteter.

Der er ikke andre love inden for energisektoren, der indeholder bestemmelser om rådgivende EU-delegationers adgang til oplysninger, systemer og faciliteter.

Det følger af den foreslåede § 21, *stk. 1,* at rådgivende missioner som er nedsat i medfør af CER-direktivet, efter tilladelse fra klima-, energi- og forsyningsministeren kan føre tilsyn med virksomheder som betragtes som enheder af særlig europæisk betydning i medfør af reglerne i § 5, stk. 1.

Den foreslåede bestemmelse vil gennemføre CER-direktivets artikel 18, stk. 1 og 2, som beskriver den særlige tilsynsordning for enheder af europæisk betydning. Det følger af CER-direktivets artikel 18, stk. 2, at kommissionen på eget initiativ eller efter anmodning fra en eller flere medlemsstater kan tilrettelægge en rådgivende mission, under forudsætning af at den medlemsstat, som har identificeret den pågældende kritiske enhed, samtykker.

Det følger af CER-direktivets artikel 18, stk. 5, at en rådgivende mission består af eksperter fra den medlemsstat, hvor den kritiske enhed af særlig europæisk betydning er beliggende, eksperter fra de medlemsstater, hvortil eller hvori den væsentlige tjeneste leveres, og repræsentanter fra Kommissionen.

Den foreslåede bestemmelse opfylder den særlige tilsynsordning som følger af CER-direktivets artikel 18, stk. 1, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Det følger af den foreslåede § 21, *stk. 2,* at rådgivende missioner kan anvende tilsynsforanstaltninger efter § 19, stk. 2, nr. 1-7, i det omfang anvendelsen af foranstaltninger er nødvendig for at gennemføre den pågældende rådgivende mission.

Den foreslåede bestemmelse gennemfører artikel 18, stk. 7 i CER-direktivet, hvoraf det fremgår, at medlemsstaterne sikrer, at kritiske enheder af særlig europæisk betydning giver rådgivende missioner adgang til oplysninger, systemer og faciliteter, der vedrører levering af deres væsentlige

tjenester, og som er nødvendige for at gennemføre den pågældende rådgivende mission.

CER-direktivets artikel 18, stk. 7, skal ses i lyset af CER-direktivets artikel 18, stk. 1 og 2, hvoraf det følger, at efter anmodning fra en medlemsstat, som har identificeret en kritisk enhed af særlig europæisk betydning, tilrettelægger Kommissionen en rådgivende mission for at vurdere de foranstaltninger, som denne kritiske enhed har truffet for at opfylde sine forpligtelser om modstandsdygtighedsforanstaltninger.

Efter CER-direktivets artikel 18, stk. 3, skal den medlemsstat som har identificeret den kritiske enhed af europæisk betydning, efter en begrundet anmodning fra Kommissionen eller berørte medlemslande, give Kommissionen; a) de relevante dele af den kritiske enheds risikovurdering, b) en oversigt over relevante foranstaltninger enheden har truffet, c) tilsyns- eller håndhævelsestiltag, herunder vurderinger af overholdelse eller udstedte påbud.

Klima-, Energi- og Forsyningsministeriet vurderer, at CER-direktivets artikel 18, stk. 3, litra a) og b) angår myndighedsinterne pligter fra Danmark til Kommissionen. Da bestemmelserne vedrører pligter for medlemsstaterne, kan Kommissionen anvende dem direkte. Det vurderes derfor, at de ikke er nødvendige at skrive ind i den foreslåede bestemmelse.

Med den foreslåede bestemmelse, gives der tilsynstiltag til Kommissionen og den rådgivende mission, som skal føre tilsyn med kritiske enheder af særlig europæisk betydning. Bestemmelsen gennemfører således CER-direktivets artikel 18, stk. 3, litra c.

Det er Klima-, Energi- og Forsyningsministeriets vurdering at CER-direktivets artikel 18, stk. 7, indeholder en indbygget begrænsning af hvilke tilsynstiltag, den rådgivende mission kan anvende. Dermed indeholder den foreslåede bestemmelse en indbygget begrænsning i, hvilke tilsynsforanstaltninger Kommissionens rådgivende mission kan anvende. Det fremgår af bestemmelsen, at den rådgivende mission kan bruge de tilsynsforanstaltninger der er nødvendige for at gennemføre den pågældende mission. Eksempelvis gælder det at, hvis den rådgivende mission har til formål, at undersøge den fysiske sikring eller perimetersikringen hos virksomheden, kan missionen således ikke på baggrund af denne bestemmelse også få adgang til net- og informationssystemer.

Efter den foreslåede § 20, *stk. 3,* kan den rådgivende missions tilsynsforanstaltninger efter § 19, stk. 2, nr. 1-7, begrænses i det omfang, det er nødvendigt for at beskytte; 1) Statens sikkerhed eller rigets forsvar, 2) rigets udenrigspolitiske eller udenrigsøkonomiske interesser, herunder forholdet til fremmede magter eller mellemfolkelige institutioner og 3) private og offentlige interesser, hvor hemmeligholdelse efter forholdets særlige karakter er påkrævet.

Den foreslåede undtagelsesbestemmelse medfører, at der kan ske begrænsning af tilsynsforanstaltninger som den rådgivende mission kan anvende, ud over den begrænsning som er indeholdt i den foreslåede stk. 2.

Den foreslåede bestemmelse implementerer og kodificerer CER-direktivets artikel 18, stk. 8, hvoraf det følger, at rådgivende missioner gennemføres i overensstemmelse med gældende national ret i den medlemsstat, hvor de finder sted, idet den pågældende medlemsstats ansvar for national sikkerhed og beskyttelse af sine sikkerhedsmæssige interesser respekteres. Ligeledes understøttes den foreslåede bestemmelse af CER-direktivets artikel 1, stk. 6, hvorefter det gælder, at direktivet ikke berører medlemsstaternes ansvar for at beskytte national sikkerhed og forsvar og deres beføjelse til at beskytte andre væsentlige statslige funktioner, herunder sikring af statens territoriale integritet og opretholdelse af lov og orden.

Efter den foreslåede § 20, *stk. 4,* er det klima-, energi- og forsyningsministeren der træffer afgørelse om begrænsning af rådgivende missioners tilsynsforanstaltninger efter stk. 3.

Ifølge den foreslåede bestemmelse, vil klima-, energi- og forsyningsministeren kunne træffe afgørelser om, at den rådgivende mission ikke kan anvende visse tilsynsforanstaltninger eller begrænses i anvendelsen af en specifik tilsynsforanstaltning. Eksempelvis kan klima-, energi- og forsyningsministeren træffe afgørelse om, at den rådgivende mission kun kan kræve at få udleveret visse oplysninger.

Klima-, energi- og forsyningsministeren kan ligeledes over for virksomheden, som er udpeget som kritisk enhed af europæisk betydning, træffe afgørelse om, at de ikke skal efterleve visse tilsynsforanstaltninger fra den rådgivende mission. Som eksempel kan der meddeles afgørelse til den pågældende virksomhed om, at de ikke skal efterleve visse tilsynsforanstaltninger eller dele af tilsynsforanstaltninger, som anvendes af den rådgivende mission.

Det forventes med den foreslåede bestemmelse, at afgørelser om begrænsning af tilsynsforanstaltninger, som anvendes af den rådgivende mission i vidt muligt omfang, skal foretages inden den rådgivende mission påbegynder et tilsyn. Dette betyder, at klima-, energi- og forsyningsministeren, ved anmodning om en rådgivende mission, kan foretage tilsyn og kontrol af en kritisk enhed af særlig europæisk betydning, med det formål, at afgrænse om information hos den kritiske enhed af særlig europæisk betydning, er beskyttelsesværdig information efter stk. 3.

Klima-, energi- og forsyningsministeren kan i tilfælde af tvivl, om information vedrørende den kritiske enhed af særlig europæisk betydning er beskyttelsesværdig, rette henvendelse til Politiets Efterretningstjeneste, som er national sikkerhedsmyndighed, eller til Forsvarets Efterretningstjeneste, som er national sikkerhedsmyndighed på Forsvarsministeriets område.

Der henvises i øvrigt til bemærkninger til den foreslåede § 5.

Til § 21 [Kapitel 8]

Bekendtgørelse nr. 11 af den 7. januar 2011 om identifikation og udpegning af europæisk kritisk infrastruktur på energiområdet og vurdering af behovet for bedre beskyttelse indeholder håndhævelsesbeføjelser i form af påbud.

Elforsyningsloven og gasforsyningsloven indeholder begge håndhævelsesforanstaltningerne om påbud, inddragelse af bevilling og it-revision. Efter de gældende regler skal forhold, der strider mod den gældende regulering bringes i orden straks eller inden for en af klima- energi- og forsyningsministeren nærmere angivet frist.

Olieberedskabsloven indeholder håndhævelsesforanstaltninger, om at kunne anvende påbud, ved manglende overholdelse af beredskabsreglerne.

Det følger af den foreslåede § 21, *stk. 1*, at klima- energi og forsyningsministeren ud fra en konkret vurdering af omstændighederne i hver enkelt sag kan anvende følgende håndhævelsesforanstaltninger over for en virksomhed: 1) påbyde virksomheden at træffe foranstaltninger, der er nødvendige for at forhindre eller afhjælpe en hændelse, 2) meddele virksomheden påbud og forbud for at sikre overholdelsen af de krav, der er fastsat i loven eller regler udstedt i medfør af loven, 3) påbyde virksomheden at underrette de fysiske eller juridiske personer, til hvilke den leverer tjenester eller

udfører aktiviteter, som potentielt kan være berørt af en væsentlig cybertrussel, om denne trussels karakter samt om eventuelle beskyttelsesforanstaltninger eller afhjælpende foranstaltninger, som de fysiske eller juridiske personer kan træffe som reaktion på denne trussel, 4) påbyde virksomheden at udpege en person med ansvar for i en nærmere fastsat periode at føre tilsyn med virksomhedens overholdelse af §§ 6-9 og §§ 12-14, samt regler udstedt i medfør heraf og 5) påbyde virksomheden i ikke-anonymiseret form og på en nærmere angiven måde at offentliggøre afgørelser om håndhævelsesforanstaltninger efter nr. 1-4 samt resumeer af domme eller bødevedtagelser, hvor der idømmes eller vedtages en bøde.

Den foreslåede bestemmelse vil implementere artikel 32, stk. 4, litra a-h, i 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 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 (foranstaltninger til styring af cybersikkerhedsrisici), eller at efterleve underretningsforpligtelserne i artikel 23 (rapporteringsforpligtelser, 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 dette direktiv på en nærmere angivet måde.

Den foreslåede bestemmelse gennemfører desuden artikel 21, stk. 3, i CER-direktivet, hvoraf det fremgår, at uden at det berører muligheden for at pålægge sanktioner i overensstemmelse med CER-direktivets artikel 22, kan de kompetente myndigheder efter de i CER-direktivets artikel 21, stk. 1, omhandlede tilsynsforanstaltninger eller vurderingen af de i CER-direktivets artikel 21, stk. 2, omhandlede oplysninger, pålægge de berørte kritiske enheder at træffe de nødvendige og forholdsmæssige foranstaltninger for at afhjælpe enhver konstateret overtrædelse af dette direktiv inden for en rimelig frist, der fastsættes af disse myndigheder, og give disse myndigheder oplysninger om de trufne foranstaltninger.

Der lægges med bestemmelsen ikke op til at omfatte virksomheder baseret på antal ansatte og virksomhedens årlige omsætning eller bruttofortjeneste. Bestemmelsen skelner dermed ikke mellem væsentlige og vigtige enheder. Det skyldes, at denne afgrænsning ikke inddrager virksomhedernes forsyningsmæssige størrelse og kritikalitet, og at kun få energivirksomheder vil blive omfattet. Eksempelvis kan koncernkonstruktioner med datterselskaber indebære, at energivirksomheder med stor kritikalitet kan have få ansatte. I stedet lægges der op til for begge direktiver at følge den nuværende afgrænsningsmodel i energisektoren, som er den model, der bl.a. er blevet brugt ved implementering af NIS1-direktivet i energisektoren. Herved er det forsyningsstørrelsen, der primært er afgørende for, om virksomheden omfattes af beredskabsregulering, da forsyningsstørrelsen afspejler virksomhedens kritikalitet for energiforsyningen. Det vurderes, at denne afgrænsning stadig lever op til direktiverne.

Den foreslåede bestemmelse vil finde anvendelse på en bredere kreds, men i øvrigt svare indholdsmæssigt til NIS 2-direktivets artikel 32, stk. 4, litra a-h. Den foreslåede bestemmelse vil også gå videre end, hvad der fremgår af CER-direktivets artikel 21, stk. 3. Bestemmelsen skal derudover forstås og anvendes i overensstemmelse med direktivernes forudsætninger og eventuelle fortolkningsbidrag fra Kommissionen, ENISA eller andre af EU's institutioner. Den foreslåede bestemmelse går dermed videre end, NIS 2- og CER-direktiverne.

Efter CER-direktivets artikel 21, stk. 3, skal håndhævelsesforanstaltningerne navnlig tage hensyn til overtrædelsens grovhed. I overensstemmelse med NIS 2-direktivets artikel 32, stk. 1, skal de foranstaltninger, der anvendes overfor virksomheder 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 § 21, at Klima- Energi og Forsyningsministeriet skal foretage en konkret vurdering af omstændighederne i hver enkelt sag, når der anvendes håndhævelsesforanstaltningerne over for virksomheder.

Klima- Energi og Forsyningsministeriet skal i overensstemmelse med CER-direktivets artikel 21, stk. 3 og 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 revision- eller overvågningsaktiviteter beordret af klima-, energi- og forsyningsministeren efter konstatering af en overtrædelse, og e) afgivelse af urigtige eller klart unøjagtige oplysninger vedrørende net- og informationssikkerhedsrisikostyringsforanstaltninger, modstandsforanstaltninger eller rapporteringsforpligtelser, der er fastsat i §§ 6-9, 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 klima-energi- og forsyningsministeren ved anvendelsen af håndhævelsesforanstaltninger skal overholde retten til forsvar. Dette sikres ved, at et påbud eller forbud efter den foreslåede § 21, stk. 1-5, vil være omfattet af forvaltningslovens regler, herunder bl.a. bestemmelserne i kapitel 3 (om vejledning og repræsentation mv.), kapitel 5 (om partshøring), kapitel 6 (om begrundelse mv.) og kapitel 7 (om klagevejledning). Derudover vil der være mulighed for at påklage afgørelsen til Energiklagenævnet efter den foreslåede § 32, stk. 1, ligesom afgørelsen vil kunne indbringes for domstolene.

Der vil i forbindelse med en afgørelse om påbud eller forbud efter den foreslåede § 21 blive fastsat en frist, inden for hvilken virksomheden skal efterkomme indholdet i afgørelsen. Fristen for hvornår virksomheden skal efterleve håndhævelsesforanstaltningerne skal være proportionel med de anvendte foranstaltninger. I tilfælde af en overhængende fare for at en hændelse kan indtræde på baggrund af virksomhedens forhold, kan der anvendes strakspåbud.

En virksomhed, der modtager en afgørelse om påbud eller forbud efter den foreslåede § § 21, vil i overensstemmelse med den foreslåede bestemmelse i § 21, som vil implementere CER-direktivets artikel 22 og NIS 2-direktivets artikel 34, stk. 2, også kunne ifalde straf for en eventuel overtrædelse af denne lov eller regler udstedt i medfør af loven.

Det foreslås i § 22, stk. 1, *nr. 1*, at klima- energi- og forsyningsministeren kan påbyde virksomheden at træffe foranstaltninger, der er nødvendige for at forhindre eller afhjælpe en hændelse.

Klima- Energi- og Forsyningsministeriet vil i medfør af det foreslåede nr. 1, eksempelvis kunne give virksomhederne påbud om at foretage en fornøden softwareopdatering med henblik på at forhindre eller imødegå en hændelse.

Det foreslås med § 22, stk. 1, *nr. 2*, at klima- energi- og forsyningsministeren kan meddele virksomheden 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 klima- energi- og forsyningsministeren kunne angive, hvilke nærmere foranstaltninger virksomheden skal træffe. Klima- energi- og forsyningsministeren kan på baggrund af trusselsbilleder eller konkrete informationer fra de danske efterretningstjenester forbyde virksomheder at anvende materiel eller services fra aktører fra tredjelande, såfremt det vurderes, at det kan udgøre en trussel for virksomhedens sikkerhed og beredskab eller på anden måde kompromittere virksomhedens evne til at levere tjenester eller udføre sine aktiviteter.

Det foreslås med § 22, stk. 1, *nr. 3*, at klima- energi- og forsyningsministeren kan pålægge virksomheden at underrette de fysiske eller juridiske personer, til hvilke den leverer tjenester eller udfører aktiviteter, som potentielt kan være berørt af en væsentlig cybertrussel, om denne trussels karakter

samt om eventuelle beskyttelsesforanstaltninger eller afhjælpende foranstaltninger, som de fysiske eller juridiske personer kan træffe som reaktion på denne trussel.

Bestemmelsen skal ses i sammenhæng med den foreslåede bestemmelse i § 13, som indeholder en forpligtelse for virksomheder 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 virksomhederne også informere de pågældende modtagere om den væsentlige cybertrussel.

Med det foreslåede nr. 3, vil klima- energi- og forsyningsministeren kunne fastsætte, at der skal foretages underretning af modtagerne af virksomhedens tjenester, uanset om virksomheden selv vurderer, at det er relevant.

Det foreslås med § 22, stk. 1, *nr. 4*, at klima- energi- og forsyningsministeren kan påbyde virksomheden at udpege en person med ansvar for i en nærmere fastsat periode at føre tilsyn med virksomhedens overholdelse af §§ 6-9 og §§ 12-14.

Virksomheden vil enten kunne udpege en ansat eller en ekstern person. Den pågældende person vil skulle monitorere virksomhedens overholdelse af krav til foranstaltninger til styring af enten fysiske eller logiske risici i medfør af de foreslåede bestemmelser om foranstaltningerne og underretning. Klima-, Energi- og Forsyningsministeriet kan påbyde virksomheden at udpege flere personer til at føre tilsyn med overholdelse af §§ 6-9 og §§ 12-14, hvis virksomhedens størrelse eller særlig teknisk forståelse for foranstaltninger kræver det, eller hvis det i øvrigt findes relevant for at sikre et tilstrækkelig grundigt tilsyn.

Det foreslås med § 22, stk. 1, *nr. 5*, at klima- energi- og forsyningsministeren kan påbyde virksomheden 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.

Det forudsættes, at virksomheden ikke pålægges at offentliggøre oplysninger om tekniske indretninger eller fremgangsmåder eller om drifts- eller forretningsforhold el.lign, for så vidt det er af væsentlig økonomisk betydning for den virksomhed, som oplysningerne angår. Definitionen af oplys-

ninger vedrørende tekniske indretninger m.v. skal forstås i overensstemmelse med § 30, nr. 2, i offentlighedsloven og skal fortolkes i overensstemmelse med denne bestemmelses forarbejder og relevant praksis.

Det forudsættes desuden, at virksomheden ikke pålægges at offentliggøre oplysninger, der kan udnyttes af ondsindede aktører og derved udgøre en sikkerhedsmæssig risiko for virksomheden. Sådanne oplysninger kan eksempelvis være nærmere information om, hvilke foranstaltninger der ikke er blevet fundet tilstrækkelige på baggrund af tilsyn og kontrol.

Det forudsættes endvidere, at virksomheden ikke pålægges at offentliggøre oplysninger om enkeltpersoners forhold, medmindre disse oplysninger indgår i enhedens navn. Oplysninger om enkeltpersoners forhold kan eksempelvis være oplysninger om navne, adresser eller private telefonnumre på medarbejdere eller andre berørte parter.

Der henvises i øvrigt til afsnit 3.7 i lovforslagets almindelige bemærkninger.

Til § 22 [Kapitel 8]

Ifølge elforsyningslovens § 85 c, stk. 2, og gasforsyningslovens § 15 b, stk. 2, kan klima-, energi- og forsyningsministeren påbyde virksomheder, som ikke har efterkommet påbud om overholdelse af bestemmelsernes stk. 1, at foretage en it-revision af kritiske it-systemer ved en uafhængig revisor godkendt af tilsynsmyndigheden.

Efter olieberedskabslovens § 17, stk. 4, kan klima-, energi- og forsyningsministeren, bestemme at virksomheder skal fremsende en revisorerklæring om rigtigheden af fremsendte oplysninger.

Det følger af den foreslåede § 22, *stk. 1,* at klima-, energi- og forsyningsministeren kan ved manglende opfyldelse af påbud efter § 21, stk. 1, nr. 1-5, påbyde virksomheder at få foretaget en revision af net- og informationsforanstaltninger, modstandsdygtighedsforanstaltninger og kritiske systemer ved en uafhængig revisor. Udgifterne til revisionen afholdes af virksomheden.

Den foreslåede bestemmelse vil bygge videre på gældende bestemmelser fra el- og gassektoren, hvor ministeren kan påbyde virksomheder at foretage en revision. Den foreslåede bestemmelse, vil kunne anvendes i flere tilfælde end tidligere. Som efter gældende regulering vil bestemmelsen

finde anvendelse på net- og informationssystemer, svarende til it-beredskab, desuden vil klima-, energi- og forsyningsministeren påbyde virksomheder at få foretaget revision af modstandsforanstaltninger, som anvendes ved den fysiske sikring af virksomheden.

Revisionen adskiller sig fra det generelle tilsyn, som der foreslås efter loven ved, at revisionen skal udføres af en uafhængig revisor fremfor tilsynsmyndigheden, og at revisionen ikke er bundet af de tilsyns- og kontrolrammer som anvendes af tilsynsmyndigheden.

Efter den foreslåede bestemmelse, kan klima-, energi- og forsyningsministeren påbyde en revision, når håndhævelsesforanstaltninger der er meddelt efter § 21, stk. 1-5, ikke vurderes tilstrækkeligt efterlevet. Påbud kan dermed ske på baggrund af tilsyn, hvor tilsynsmyndigheden bliver opmærksom på manglende overholdes af påbud hos virksomheder eller hvis sådan viden opnås gennem andre kanaler.

Det følger af den foreslåede § 22, at Klima-, Energi og Forsyningsministeriet skal foretage en konkret vurdering af omstændighederne i hver enkelt sag, hvor virksomheden påbydes at foretage en revision. Et påbud om revision skal være proportionelt med de mangler, som er konstateret hos virksomheden.

Klima-, Energi- og Forsyningsministeriet skal ved påbud om revision 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 og e) afgivelse af urigtige eller klart unøjagtige oplysninger vedrørende net- og informationssikkerhedsrisikostyringsforanstaltninger, modstandsforanstaltninger eller rapporteringsforpligtelser, der er fastsat i §§ 6-9, 12, 13, 15 og 16, 2) overtrædelsens varighed, 3) den pågældende virksomheds 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 certificeringsme-

kanismer er overholdt, og 8) i hvilken udstrækning de fysiske eller juridiske personer, der holdes ansvarlige for overtrædelsen, samarbejder med de kompetente myndigheder.

Revisionen er afgrænset til de net- og informationssystemer, modstandsdygtighedsforanstaltninger og kritiske it-systemer indgår i virksomhedens opfyldelse af regler efter loven og regler udstedt i medfør af loven. Dermed vil en revision påbudt efter den foreslåede bestemmelse, ikke omfatte virksomhedens generelle regnskaber. Generelle administrative it-systemer vil være omfattet af en sådan revision, da cyberangreb ofte bruger sådanne systemer som en angrebsvinkel, til eksempelvis at tilegne sig adgang til andre systemer. Desuden vil revisionen have kompetence til at undersøge virksomhedens risikostyringsforanstaltninger.

Det følger af den foreslåede § 22, *stk. 2,* at klima-, energi og forsyningsministeren kan påbyde virksomheder at gennemføre tiltag, som på baggrund af en revision efter stk. 1, vurderes nødvendige for at opretholde et tilstrækkeligt beredskab.

Efter den foreslåede bestemmelse, er virksomheder dermed ikke bundet af konklusionerne efter en afholdt revision, som er påbudt efter § 22, stk. 1. Virksomhederne kan dog påbydes at gennemføre tiltag på baggrund af revisionen. Bestemmelsen indebærer dermed, at klima-, energi- og forsyningsministeren skal gennemgå rapporter udarbejdet på baggrund af en revision.

Det følger af den foreslåede § 22, *stk. 3,* at klima-, energi- og forsyningsministeren kan fastsætte nærmere regler for, hvordan den uafhængige revisor udpeges og godkendes.

Bestemmelsen har til formål at sikre, at der fastsættes regler som understøtter, at den udpegede revisor er uafhængig af virksomheden, som skal have foretage revision.

Til § 23 [Kapitel 8]

Ifølge elforsyningslovens § 54, stk. 4, kan en bevilling, som er en autorisation til at drive visse elvirksomheder, midlertidigt inddrages, ved en virksomheds overtrædelse af bestemmelser, vilkår eller påbud efter denne lov eller lov om fremme af vedvarende energi eller regler udstedt i medfør af disse love eller en netvirksomheds grove eller gentagne tilsidesættelse af

vilkår stillet af Energinet i medfør af § 31, stk. 2, der berører virksomhedens bevillingspligtige aktivitet, indebærer tilsidesættelse af væsentlige hensyn til elforsyningssikkerheden.

Elforsyningsloven indeholder ikke en bestemmelse om, at fysiske personer med ledelsesansvar midlertidigt kan forbydes at udøve ledelsesfunktioner.

Efter gasforsyningslovens § 33, skt. 1, nr. 1, kan bevillinger til gasvirksomheder inddrages, hvis bestemmelser, vilkår eller påbud efter gasforsyningsloven eller regler udstedt i medfør af loven gentagne gange overtrædes.

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 den 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, såfremt det udviste forhold begrunder en nærliggende fare for misbrug af stillingen. 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 på tid fra 1 til 5 år regnet fra endelig dom, eller indtil videre.

Efter straffelovens § 79, stk. 4, kan Retten kan under behandlingen af de i straffelovens § 79, stk. 1 og 2 nævnte sager ved kendelse udelukke den pågældende fra at udøve virksomheden, indtil sagen er endeligt afgjort. Det kan ved dommen i sagen bestemmes, at anke ikke har opsættende virkning.

Det foreslås i § 24, *stk. 1,* at hvis håndhævelsesforanstaltninger, der er pålagt i medfør af § 21, nr. 1-4 og § 22, stk. 1 og 2, vist sig at være utilstrækkelige, kan klima-, energi- og forsyningsministeren fastsætte en frist, inden for hvilken virksomheden skal foretage de nødvendige tiltag for at afhjælpe manglerne eller opfylde myndighedernes krav. Er tiltagene ikke foretaget inden for den fastsatte frist, kan klima-, energi- og forsyningsministeren træffe afgørelse om 1) midlertidigt at suspendere en certificering el-

ler godkendelse vedrørende dele af eller alle de relevante tjenester, virksomheden leverer, eller aktiviteter, der udføres af virksomheden og 2) midlertidigt at forbyde enhver fysisk person med ledelsesansvar på niveau med administrerende direktør eller den juridiske repræsentant hos virksomheden at udøve ledelsesfunktioner i den pågældende virksomhed.

Bestemmelsen vil gennemføre artikel 32, stk. 5, 1. afsnit, i NIS 2-direktivet. Det følger af bestemmelsen, at medlemsstaterne skal sikre, at de kompetente myndigheder i en situation, hvor håndhævelsesforanstaltninger anvendt i medfør af direktivets artikel 32, stk. 4, litra a)-d) og f), er virkningsløse, skal have beføjelse til at fastsætte en frist inden for hvilken den væsentlige enhed skal tage de nødvendige tiltag for at afhjælpe manglerne eller opfylde myndighedernes krav. Hvis de ønskede tiltag ikke tages inden for den fastsatte frist, skal de kompetente myndigheder have beføjelse til: a) midlertidigt at suspendere, eller anmode et certificerings- eller godkendelsesorgan eller en domstol om i overensstemmelse med national ret midlertidigt at suspendere en certificering eller godkendelse vedrørende dele af eller alle de relevante tjenester, der leveres, eller aktiviteter, der udføres, af en væsentlig enhed, og b) at anmode de relevante organer eller domstole om i overensstemmelse med national ret midlertidigt at forbyde enhver fysisk person med ledelsesansvar på direktionsniveau eller som juridisk repræsentant i den pågældende væsentlige enhed at udøve ledelsesfunktioner i den pågældende enhed.

Bestemmelsen vil finde anvendelse på forhold omkring fysisk sikring som falder inden for CER-direktivets område.

Det bemærkes, at de eksisterende muligheder for rettighedsfrakendelse i straffeloven ikke vurderes tilstrækkelige til at sikre korrekt og tilstrækkelig implementering af bestemmelsen i direktivet. Det skyldes navnlig, at rettighedsfrakendelse i medfør af straffelovens § 79 alene kan ske i forbindelse med dom for strafbart forhold, og hvis det udviste forhold begrunder en nærliggende fare for misbrug af stillingen.

Den foreslåede bestemmelse går videre end minimumskravene i NIS2- og CER-direktiverne. Bestemmelsen skal derudover forstås og anvendes i overensstemmelse med direktivets forudsætninger og eventuelle fortolkningsbidrag fra Kommissionen, ENISA eller andre af EU's institutioner.

Det bemærkes i den forbindelse, at det af den danske oversættelse af NIS 2-direktivets artikel 32, stk. 5, 1. afsnit, fremgår, at bestemmelsen kan anvendes, hvor de relevante håndhævelsesforanstaltninger er »virkningsløse«. Denne oversættelse vurderes imidlertid ikke at være forenelig med den engelske udgave af direktivet, hvori »ineffective« er anvendt. Det er således Klima-, Energi- og Forsyningsministeriets vurdering, at formuleringen »virkningsløse« vil udgøre en indholdsmæssig forskydning i forhold til den engelske sprogversion. Det er desuden Klima-, Energi- og Forsyningsministeriets vurdering, at et kriterium om, at foranstaltningerne er »virkningsløse«, vil indebære, at enhver virkning af de anvendte foranstaltninger – uanset om virkningen måtte være utilstrækkelig eller endda negativ – vil betyde, at bestemmelsen ikke vil kunne anvendes. Det vurderes, at dette reelt vil gøre bestemmelsen uanvendelig i praksis i strid med direktivets forudsætninger. Det foreslås på den baggrund, at der i stedet anvendes et kriterie om, at virksomhederne har efterlevet håndhævelsesforanstaltningerne »utilstrækkeligt«, 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 § 21, stk. 1-4 og § 22, stk. 1 og 2, 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 virksomhedens 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.

Det bemærkes i den forbindelse, at Klima-, Energi- og Forsyningsministeriet efter omstændighederne og i relevant omfang vil 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 tilsynsmyndigheden. Det skal ses i lyset af, at muligheden for suspension og forbud ligger i forlængelse af anvendelsen af de øvrige håndhævelsesmuligheder, og at der i en afgørelse om suspension eller forbud forudsættes at skulle indgå en begrundelse for, hvorfor allerede pålagte håndhævelsesforanstaltninger er utilstrækkelige.

Det følger af NIS 2-direktivets artikel 32, stk. 7, at klima-, energi- og forsyningsministeren 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 net- og informationssikkerhedsrisikostyringsforanstaltninger, modstandsforanstaltninger eller rapporteringsforpligtelser, der er fastsat i §§ 6-9, 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 § 23, stk. 1, *nr. 1*, indebærer, at såfremt virksomheden ikke har iværksat tiltag for at afhjælpe manglerne eller efterkomme den kompetente myndigheds krav inden for den fastsatte frist, kan klima-, energi- og forsyningsministeren træffe afgørelse om midlertidigt at suspendere en certificering eller godkendelse vedrørende dele af eller alle de relevante tjenester, virksomheden leverer, eller aktiviteter, der udføres af virksomheden.

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 1, nr. 1, ikke anvendes, før bemyndigelsen i den foreslåede stk. 5, er anvendt.

En afgørelse efter nr. 1 vil være af midlertidig karakter. Der henvises i øvrigt til det foreslåede stk. 2, hvorefter afgørelsen kun kan opretholdes, så længe virksomheden ikke har truffet de nødvendige tiltag for at afhjælpe de mangler eller efterleve de krav fra klima-, energi- og forsyningsministeren, som gav anledning til, at foranstaltningerne blev anvendt.

Den foreslåede bestemmelse i § 23, stk. 1, *nr. 2*, indebærer, at såfremt virksomheden ikke har iværksat tiltag for at afhjælpe manglerne eller efterkomme klima-, energi- og forsyningsministerens krav inden for den fastsatte frist, kan klima-, energi- og forsyningsministeren 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 virksomhed.

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 Klima-, Energi- Forsyningsministeren 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. Der henvises i øvrigt til det foreslåede stk. 2, hvorefter afgørelsen kun kan opretholdes, så længe virksomheden ikke har truffet de nødvendige tiltag for at afhjælpe de mangler eller efterleve de krav fra klima- energi- og forsyningsministeren, som gav anledning til, at foranstaltningerne blev anvendt.

I det omfang en virksomhed eller organisation ikke har en administrerende direktør, vil bestemmelsen omfatte den øverste leder af den pågældende væsentlige enhed, f.eks. en generalsekretær, direktør, koncernchef eller managing partner.

En afgørelse efter nr. 2 vil være af midlertidig karakter, jf. også det foreslåede stk. 2, hvorefter afgørelsen kun kan opretholdes, så længe enheden ikke har truffet de nødvendige tiltag for at afhjælpe de mangler eller efterleve de krav fra myndigheden, som gav anledning til, at foranstaltningerne blev anvendt.

Det foreslås i § 23, *stk. 2,* at midlertidige suspensioner eller forbud, som er pålagt i medfør af stk. 1, kan kun anvendes, indtil virksomheden træffer de nødvendige foranstaltninger til at afhjælpe de mangler eller til at opfylde de krav, som gav anledning til at foranstaltningerne 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 virksomhed træffer de nødvendige foranstaltninger til at afhjælpe manglerne eller opfylde den kompetente myndigheds krav, som gav anledning til, at disse håndhævelsesforanstaltninger blev anvendt.

Klima-, Energi- og Forsyningsministeriet har ikke fundet grundlag for at gå videre end direktivet. Den foreslåede bestemmelse svarer således indholdsmæssigt 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 foreslås i § 23, *stk. 3,* at en afgørelse efter stk. 1 kan af virksomheden eller den fysiske person, afgørelsen vedrører, forlanges indbragt for domstolene. Klima-, energi- og forsyningsministeren anlægger i givet fald sag mod den virksomhed 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 virksomheden 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 og efter § 31 om klage til Energiklagenævnet.

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.

Det følger af det foreslåede § 24, *stk. 4,* at klima-, energi- og forsyningsministeren 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 klima-, energi- og forsyningsministeren 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.

Det forudsættes, at den foreslåede bestemmelse i 1, nr. 1, ikke anvendes, før bemyndigelsen i den foreslåede stk. 5, er anvendt.

Til § 24 [Kapitel 8]

Klima-, Energi- og Forsyningsministeriet skal inden afgørelser hvor en part ikke kan antages at være bekendt med, at ministeriet er i besiddelse af bestemte oplysninger om en sags faktiske grundlag eller eksterne faglige vurderinger, må der ikke træffes afgørelse, før ministeriet har gjort parten bekendt med oplysningerne eller vurderingerne og givet denne lejlighed til at fremkomme med en udtalelse. Det gælder dog kun, hvis oplysningerne eller vurderingerne er til ugunst for den pågældende part og er af væsentlig betydning for sagens afgørelse. Ministeriet kan fastsætte en frist for afgivelsen af den nævnte udtalelse jf. forvaltningslovens § 19, stk. 1 jf. dog undtagelserne i stk. 2.

Det følger af den foreslåede § 24, *stk. 1,* at inden Klima- Energi- og Forsyningsministeriet træffer afgørelse om at anvende håndhævelsesforanstaltninger efter §§ 21-23 underrettes den berørte virksomhed om de påtænkte håndhævelsesforanstaltninger og begrundelsen herfor. Klima- Energi- og Forsyningsministeriet skal give virksomheden en rimelig frist til at fremsætte bemærkninger, undtagen i tilfælde hvor formålet med foranstaltningen ellers ville forspildes.

Den foreslåede bestemmelse vil gennemføre artikel 32, stk. 8, i NIS 2-direktivet. Artikel 32, stk. 8, fastsætter, at de kompetente myndigheder giver en detaljeret begrundelse for deres håndhævelsesforanstaltninger. Inden de kompetente myndigheder træffer sådanne foranstaltninger, underretter de

kompetente myndigheder de berørte enheder om deres foreløbige resultater. De giver også disse enheder en rimelig frist til at fremsætte bemærkninger, undtagen i behørigt begrundede tilfælde, hvor øjeblikkelige foranstaltninger til at forebygge eller reagere på hændelser ellers ville blive hindret.

Den foreslåede bestemmelse svarer således indholdsmæssigt til NIS 2-direktivets artikel 32, stk. 8, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Den foreslåede bestemmelse indeholder en forpligtelse for Klima-, Energi- og Forsyningsministeriet til at sende en såkaldt agterskrivelse til en virksomhed, før der træffes beslutning om at anvende en påtænkt håndhævelsesforanstaltning efter §§ 21-23.

Agterskrivelsen 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 virksomhedens bemærkninger til høringen kan få indflydelse på resultatet, og at Klima-, Energi- og Forsyningsministeriet lader agterskrivelsen få virkning som en afgørelse, hvis virksomheden ikke kommer med bemærkninger til høringen inden dennes udløb.

Agterskrivelsen skal indeholde en rimelig frist for virksomheden til at afgive bemærkninger til agterskrivelsens indhold.

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 3.7 i lovforslagets almindelige bemærkninger.

Til § 25 [Kapitel 9]

Det fremgår af artikel 17, stk. 3, i 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.

Det følger af den foreslåede § 25, *stk. 1*, at hvor en virksomhed leverer tjenester i mere end én medlemsstat i Den Europæiske Union, eller hvor virksomheden leverer tjenester i en eller flere medlemsstater, og virksomhedens net- og informationssystemer er beliggende i en eller flere andre medlemsstater, samarbejder Klima-, Energi- og Forsyningsministeriet med de andre medlemsstaters kompetente myndigheder i relevant omfang. Samarbejdet, indebærer at; 1) Klima-, Energi- og Forsyningsministeriet via det centrale kontaktpunkt, der er nedsat i medfør af NIS 2-direktivet, underretter de kompetente myndigheder i relevante medlemsstater om anvendte tilsyns- og håndhævelsesforanstaltninger, 2) Klima-, Energi- og Forsyningsministeriet kan anmode en anden medlemsstats kompetente myndigheder om at anvende tilsyns- og håndhævelsesforanstaltninger, 3) Klima-, Energi- og Forsyningsministeriet 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 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. afsnit, at den gensidige bistand, der er omhandlet i litra c, kan omfatte anmodninger om oplysninger og tilsynsforanstaltninger, herunder anmodninger om at foretage inspektioner på stedet eller eksternt tilsyn eller målrettede sikkerhedskontroller. En kompetent myndighed, som en anmodning om bistand er rettet til, må ikke afvise anmodningen, medmindre det er fastslået, at den ikke er kompetent til at yde den ønskede bistand, at den bistand, der anmodes om, ikke står i et rimeligt forhold til den kompetente myndigheds tilsynsopgaver, eller anmodningen vedrører oplysninger eller indebærer aktiviteter, som, hvis de blev videregivet eller udført, ville stride mod den medlemsstats væsentlige interesser med hensyn til national sikkerhed, offentlige sikkerhed eller forsvar. Før den kompetente myndighed afslår en sådan anmodning, hører den de øvrige berørte kompetente myndigheder samt, efter anmodning fra en af de berørte medlemsstater, Europa-Kommissionen og ENISA.

Den foreslåede bestemmelse indebærer, at de Klima-, Energi- og Forsyningsministeriet i relevant omfang skal samarbejde med de kompetente myndigheder i andre medlemsstater om deres opgaveudførelse vedrørende enheder, der leverer tjenester i én eller flere medlemsstater, og enheder, hvis net- og informationssystemer er beliggende i én eller flere 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 Klima-, Energi- og Forsyningsministeriet kan anmode en anden medlemsstats kompetente myndigheder om at iværksætte tilsyns- og håndhævelsesforanstaltninger.

Samarbejdet indebærer endvidere, at Klima-, Energi- og Forsyningsministeriet 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 inspektioner på stedet eller målrettede sikkerhedskontroller.

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, offentlige sikkerhed eller forsvar. Før der kan ske afvisning af en anmodning, skal den kompetente myndighed høre de relevante kompetente myndigheder i andre medlemsstater samt, efter anmodning fra en af de relevante kompetente myndigheder i andre medlemsstater, Europa-Kommissionen og ENISA.

Det følger af det forslåede § 25, *stk. 2*, at Klima-, Energi- og Forsyningsministeriet kan efter nærmere aftale 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.

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.

Til § 26 [Kapitel 10]

Efter gældende ret i elforsyningslovens § 85 c, stk. 4 og gasforsyningslovens § 15 b, stk. 4, er det fastsat, at informationer, herunder vurderinger, planer og data, vedrørende sikkerhedsforhold for kritiske it-systemer i virksomheder omfattet af stk. 1 er fortrolige, hvis oplysningerne er væsentlige af hensyn til driften af virksomheden eller det sammenhængende hhv. elsystem og gassystem. Det er nærmere fastsat i § 29 i it-beredskabsbekendtgørelsen for el- og naturgassektorerne, at følsomme oplysninger skal behandles med fortrolighed, og at der ved følsomme oplysninger forstås: oplysninger om konkrete risici og sårbarheder, planmateriale, kritiske dele af beredskabsplaner, herunder hvordan virksomheden eller sektoren vil agere i givne beredskabssituationer, materiale af tilsvarende karakter, der af virksomheden eller Energinet vurderes følsomt. Endvidere fastsætter §

29, stk. 3, at Forsendelse og håndtering af følsomt materiale skal ske på en måde, der sikrer fortrolighed og integritet af materialet, mens § 29, stk. 4, bestemmer at følsomt materiale, som ikke længere benyttes, skal destrueres.

Det er endvidere i § 32 i hhv. elberedskabsbekendtgørelsen og naturgasberedskabsbekendtgørelsen, med hjemmel i elforsyningslovens § 85 b, stk. 3 og 4, og gasforsyningslovens § 15 a, stk. 3 og 4, angivet, at sårbarhedsvurderinger og klassificering efter § 11, stk. 1 og 2, samt kritiske dele af beredskabsplaner og andet materiale af tilsvarende karakter skal behandles fortroligt og ikke må komme uvedkommende i hænde.

Desuden bestemmer § 32, stk. 2 og 3, at materialet kan opbevares i elektronisk form og skal opbevares således, at uautoriseret adgang, sletning, ødelæggelse, ændring og offentliggørelse forhindres, at forsendelse og håndtering af følsomt materiale skal ske på måde, der sikrer fortrolighed og integritet af materialet, og at følsomt materiale, som ikke længere benyttes, skal destrueres.

Endeligt bestemmer § 32, stk. 4 at hvis følsomt materiale kompromitteres, skal skadevirkningerne opgøres og vurderes. For materiale hos virksomhederne foretages denne opgørelse og vurdering af Energinet og for andet materiale foretages dette af Energistyrelsen. Energistyrelsen afgør i samråd med Energinet og Rigspolitiet, om der er behov for, at materialet eller dele af dette skal ændres, og kan give pålæg herom til den pågældende virksomhed.

Næsten tilsvarende bestemmelser findes i olieberedskabsbekendtgørelsens § 19, der dog har den ekstra tilføjelse i stk. 3, 2. pkt. at udstederen af følsomme oplysninger har pligt til at gøre modtageren opmærksom på eventuelle krav til håndteringen af følsomt materiale.

Endeligt så regulerer § 84, stk. 8 og § 84 a, stk. 1, i lov om elforsyning og § 46 i lov om gasforsyning til en vis grad virksomhedernes behandling af fortrolige oplysninger. Disse bestemmelser er dog målrettet kommercielt følsomme oplysninger. Formålet med disse bestemmelser er at tilsikre, at virksomheder ikke må videregive kommercielt følsomme oplysninger til andre med det resultat, at et andet selskab får konkurrencemæssige fordele i forhold til øvrige selskaber. Det er ikke hensigten med den foreslåede § 29, at sikre kommercielt følsomme oplysninger, men hensigten at sikre, at

virksomheder beskytter oplysninger, der kan være med til at bringe energiforsyningen i fare.

Den foreslåede § 26, *stk. 1*, skal i udgangspunktet ses som en videreførelse af de ovenstående paragraffer i hhv. elforsyningsloven, gasforsyningsloven og de fire beredskabsbekendtgørelser, med undtagelse af bestemmelserne om kommercielt følsomme oplysninger.

Først og fremmest er formålet at designere, at en lang række at informationer, der bliver udarbejdet og bruges som led i denne lov af både virksomheder og myndigheder, herunder EU-Kommissionen og dennes rådgivende missioner efter § 20, indeholder informationer, som er beskyttelsesværdige, og derfor skal behandles med fortrolighed, af alle der er besiddelse af disse informationer.

Der er f.eks. tale om informationer, herunder personoplysninger, indgivet i forbindelse ansøgning om sikkerhedsgodkendelse eller baggrundskontrol. Der er endvidere tale om risiko og sårbarhedsvurderinger, planmateriale, beredskabsplaner, sikringsplaner, tekniske informationer om opbygning af anlæg og netværksstrukturer, samt data der bruges af virksomhederne til at levere deres tjenester.

Den foreslåede bestemmelse indebærer, at informationer som nævnt i det forrige afsnit skal holdes fortrolige, såfremt det skønnes nødvendigt af hensyn til virksomhedens egen sikkerhed, andre virksomheders sikkerhed eller energiforsyningen på lokalt, regionalt, nationalt eller europæisk niveau. Det er som udgangspunkt udstederen eller ejeren af oplysningerne, der vurderer oplysningernes fortrolighed, samt drager nødvendige foranstaltninger for at beskytte disse. Bestemmelsen har til formål at modvirke, at oplysninger anvendes til at forvolde skade på den enkelte virksomhed og skade på energiforsyningen generelt værende det i en eller flere af delsektorerne.

Ved risiko og sårbarhedsvurderinger forstås i denne bestemmelse beskrivelser af konkrete sårbarheder eller scenarier, der kan afstedkomme en krisesituation eller et angreb, herunder cyberangreb. Vurderinger henviser både til virksomhedens egne vurderinger af egne systemer samt vurderinger af det samlede energisystems sårbarheder.

Ved planmateriale, beredskabsplaner, sikringsplaner forstås i denne bestemmelse beskrivelser af procedure, handlinger eller foranstaltninger, der

skal forhindre eller forebygge en krisesituation eller et angreb, herunder cyberangreb.

Ved data forstås i denne bestemmelse følsomme informationer bl.a. data om systemets drift, adgange eller brugerstyring. Disse data beskriver systemers opsætning og adgangsstyring.

Bestemmelsen i det foreslåede stk. 1 ændrer ikke ved, at virksomhederne skal udlevere informationer til Energistyrelsen eller EU-Kommissionen og dennes rådgivende missioner efter § 20, i tilsynsøjemed.

Den foreslåede bestemmelse har endvidere som formål at sikre, at personer der virker inden for den offentlige forvaltning, har tavshedspligt omkring de beskyttelsesværdige informationer, i henhold til forvaltningslovens § 27, stk. 2, 2. pkt., idet omfang at informationerne ikke allerede var omfattet af en af de andre bestemmelser i forvaltningslovens § 27. Informationerne falder således, grundet designeringen som fortrolig ved lov og bekendtgørelse, ind under anvendelsesområdet for forvaltningslovens § 27, stk. 2, 2. pkt. Det betyder at personer der virker inden for den offentlige forvaltning vil kunne ifalde strafansvar efter straffelovens § 152 og §§ 152 c-152 f, såfremt personen bryder sin tavshedspligt om disse informationer.

Den foreslåede bestemmelse indskrænker ikke, at informationer, der ved tilsyn eller på anden vis kommer Energistyrelsen i hænde, vil være omfattet af reglerne om aktindsigt i henhold til lov om offentlighed i forvaltningen, forvaltningsloven samt lov om aktindsigt i miljøoplysninger i de tilfælde, hvor det skønnes, at oplysningerne er miljøoplysninger efter definitionen i § 3 i miljøoplysningsloven.

Der skal således ved vurderingen af, om der kan gives aktindsigt, efter reglerne i offentlighedsloven, forvaltningsloven og miljøoplysningsloven, i de nævnte typer informationer, vurderes om disse informationer falder ind under disse loves nogle af disse loves undtagelsesbestemmelser, f.eks. angående undtagelse af oplysninger af hensyn til statens sikkerhed eller rigets forsvar, undtagelse af oplysninger af hensyn til rigets udenrigspolitiske interesser m.v. og undtagelse af oplysninger om private forhold og drifts- eller forretningsforhold m.v.

Endvidere vil den foreslåede bestemmelse have den virkning, at der er en formodning om at arkivlovens § 27, stk. 1, nr. 1, 2, 5 og 6 finder anvendelse på de nævnte informationer, som myndigheder, samt selskaber, institutioner, foreninger m.v. der efter arkivloven er forpligtiget til at aflevere til offentligt arkiv i henhold til arkivlovens regler. Det betyder, at disse myndigheder, samt selskaber, institutioner, foreninger m.v. er forpligtiget til at drøfte med det modtagne arkiv om fastsættelse af en tilgængelighedsfrist, der er så lang som mulig i henhold til § 27, stk. 1.

Det foreslås i § 26, *stk. 2*, at klima-, energi- og forsyningsministeren fastsætter nærmere regler om hvordan virksomheder og myndigheder opbevarer, behandler og deler informationer som nævnt i stk. 1.

Den foreslåede bestemmelse har den virkning, at klima-, energi- og forsyningsministeren bemyndiges til administrativt at fastsætte de nærmere regler for, hvordan virksomheder og myndigheder opbevarer, behandler og deler den type informationer, som der er blevet designeret som fortrolige efter stk. 1.

Det er forventningen, at ministeren vil fastsætte bestemmelser, der pålægger virksomheder og myndigheder selv at gøre opmærksom på, hvordan de forventer, at deres fortrolige informationer bliver behandlet af myndighederne og andre virksomheder, når sådanne fortrolige informationer deles og udveksles. Det forventes dog samtidigt, at ministeren fastsætter regler om at virksomhederne, desuagtet sådanne instruktioner, skal udlevere de fortrolige informationer, når det er påkrævet i henhold til lovforslagets bestemmelser eller i regler udstedt i medfør i loven, f.eks. i tilsynsøjemed og som led i overholdelsen af underretningspligter.

Endvidere er det forventningen, at ministeren fastsætter bestemmelser om at fortrolige informationer ikke må komme uvedkommende i hænde og at informationer skal udarbejdes, opbevares og deles på en sådan måde, at der ikke kan opnås uautoriseret adgang, ske sletning, ødelæggelse, ændring eller utilsigtet offentliggørelse af disse informationer.

Det er desuden forventningen, at ministeren fastsætter bestemmelser om at fortrolige informationer, som ikke længere benyttes, skal destrueres, medmindre det forsat skal kunne udleveres til tilsyn, i forbindelse med efterforskning eller påkræves bevaret i anden lovgivning såsom arkivloven, forvaltningsloven og offentlighedsloven.

Endeligt er det forventningen, at ministeren fastsætter bestemmelser om, at hvis fortrolige informationer kompromitteres eller mistænkes for at være kompromitteret, så skal skadevirkningerne opgøres og vurderes, ligesom virksomheden skal underrette tilsynsmyndigheden og andre virksomheder, hvor kompromitteringen potentielt kan få konsekvenser for disse virksomheders levering af deres tjenester.

Det er ikke forventningen, at ministeren bruger den foreslåede bemyndigelse til at fastsætte regler på et detaljeniveau, der minder om de regler, der er for klassificeret materiale efter Sikkerhedscirkulæret.

Til § 27 [Kapitel 10]

Det følger af den foreslåede *§ 27*, at underretning efter § 15 er undtaget fra aktindsigt efter lov om offentlighed i forvaltningen og partsaktindsigt efter forvaltningsloven.

Den foreslåede bestemmelse implementerer NIS 2-direktivets art. 30, nr. 2, 2. afsnit, 1 pkt. "[…] samtidig med at de sikrer fortroligheden og passende beskyttelse af de oplysninger, der er afgivet af den underrettende enhed". Bestemmelsen er enslydende med en tilsvarende bestemmelse i det lovforslag fra der implementerer NIS 2, på Forsvarsministeriets ressort. Klima-, Energi- og Forsyningsministeriet har videreført bestemmelsens ordlyd i dette lovforslag for at sikre ensartet implementering af NIS2-direktivet for de dele direktivet, hvor der er ikke er nationale eller sektorhensyn, der taler for særlig sektor implementering.

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 Energistyrelsen, som kompetent myndighed, om et sådant hackerangreb. Derfor foreslås det med bestemmelsen, at underretningerne i deres helhed undtages fra aktindsigtsreglerne efter lov om offentlighed i forvaltningen og forvaltningsloven, herunder partsaktindsigt efter forvaltningsloven. Undtagelsen omfatter underretningssagen som helhed, og vil derfor også omfatte de processkridt der tages af på baggrund af underretningen efter § 15.

Undtagelsen fra aktindsigt omfatter derimod ikke virksomheders eller fysiske personers adgang til at gøre sig bekendt med oplysninger, herunder personoplysninger, der vedrører deres egne forhold.

Den foreslåede undtagelse fra aktindsigt i § 15 omfatter ikke retten til aktindsigt efter miljøoplysningsloven, såfremt den enkelte underretning efter § 15, skulle indeholde miljøoplysninger. Man kan således forsat få aktindsigt i miljøoplysninger efter miljøoplysningslovens regler, såfremt underretningen efter § 15 indeholder miljøoplysninger.

[Der skal være en beskrivelse af konsekvenserne ved at offentlighedsloven ikke finder anvendelse jf. lovkvalitetsvejledningens afsnit 6.6.]

Til § 28 [Kapitel 10]

Forvaltningslovens §§ 28-32 fastsætter rammerne for forvaltningsmyndigheders videregivelse af oplysninger til en anden forvaltningsmyndighed. Det følger af forvaltningslovens § 28, stk. 1, at for videregivelse af oplysninger om enkeltpersoner (personoplysninger) til en anden forvaltningsmyndighed gælder reglerne i databeskyttelseslovens §§ 6-8, § 10, § 11, stk. 1, § 38 og § 40. Det følger af § 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. Bestemmelsen regulerer imidlertid ikke videregivelse til udenlandske myndigheder.

Det følger af artikel 1, stk. 6, i 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.

Derudover reguleres videregivelse af oplysninger, der ville stride mod væsentlige interesser af hensyn til den nationale sikkerhed, offentlige orden eller forsvar bl.a. i Justitsministeriets cirkulære nr. 10338 af 17. december 2014 om sikkerhedsbeskyttelse af information af fælles interesse for landende i NATO eller EU, andre klassificerede informationer samt informationer af sikkerhedsmæssig beskyttelsesinteresse i øvrigt (Sikkerhedscirkulæret), forvaltningslovens regler om tavshedspligt og videregivelse af oplysninger samt straffelovens regler om tavshedspligt.

Det følger af den foreslåede § 28, *stk. 1*, at Klima-, Energi- og Forsyningsministeriet og andre relevante myndigheder, kan videregive oplysninger til andre medlemsstaters myndigheder og til institutioner i Den Europæiske Union for at varetage de myndighedsopgaver som følger af denne lov, NIS 2-direktivet eller CER-direktivet.

Bestemmelsen indebærer, at de relevante myndigheder, CSIRT'en og det centrale kontaktpunkt som led i den nationale gennemførelse af direktiverne, kan videregive oplysninger til andre medlemsstater eller EU-institutioner, hvis det er nødvendigt for at sikre overholdelsen af forpligtelserne i NIS 2- og CER-direktiverne.

Det følger således af NIS 2-direktivets artikel 3, stk. 5 at de kompetente myndigheder senest d. 17. april 2025 og derefter hvert andet år underretter; 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. Efter artikel 3, stk. 6 kan medlemsstaterne frem til d. 17. april 2025, på anmodning efter af Kommissionen underrette Kommissionen om navne op de væsentlige og vigtige enheder, der er omhandlet af stk. 5, litra b, som gengivet ovenfor.

Det følger endvidere 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, Klima-, Energi- og Forsyningsministeriet eller det centrale kontaktpunkt således i relevant

omfang skulle videregive oplysninger, som er modtaget i medfør af de foreslåede bestemmelser i §§ 12 og 15 om hændelsesunderretninger, til øvrige berørte medlemsstater og ENISA.

Det følger af CER-direktivets artikel 7, stk. 2, at medlemsstaterne efter identifikationen af de kritiske enheder i henhold til artikel 6, stk. 1, sender uden unødigt ophold sender følgende oplysninger til Kommissionen: a) en liste over væsentlige tjenester i pågældende medlemsstat, hvis der er yderligere væsentlige tjenester sammenlignet med den i artikel 5, stk. 1, omhandlede liste over væsentlige tjenester, b) antallet af identificerede kritiske enheder for hver sektor og delsektor anført i bilaget og for hver væsentlig tjeneste, c) eventuelle tærskler, der anvendes til at specificere et eller flere af kriterierne i stk. 1. Tærskler som omhandlet i første afsnits litra c) kan forelægges som de er eller i aggregeret form.

Klima-, energi og forsyningsministeren vil således igennem det centrale kontaktpunkt kunne videresende de ovennævnte oplysninger til Kommissionen, med hjemmel i lovforslagets § 28, stk. 1.

Det følger af CER-direktivets artikel 9, stk. 3, at de centrale kontaktpunkter senest den 17. juli 2028 og derefter hvert andet år en sammenfattende rapport for Kommissionen og for Gruppen for Kritiske Enheders Modstandsdygtighed omhandlet i artikel 19 om de underretninger, de har modtaget, herunder antallet af underretninger, arten af de hændelser, der er underrettet om, og de tiltag, der er taget i overensstemmelse med artikel 15, stk. 3.

Her vil klima-, energi- og forsyningsministeren have hjemmel i den foreslåede § 28, stk. 1, til at videregive de nævnte informationer til det centrale kontaktpunkt for Danmark efter CER-direktivet, således de disse informationer kan indgå i den sammenfattende rapport til Kommissionen og Gruppen for Kritiske Enheders Modstandsdygtighed.

Det følger endvidere af CER-direktivets artikel 11, stk. 1 og 2, at når det er relevant, konsulterer medlemsstaterne hinanden vedrørende kritiske enheder med henblik på at sikre en konsekvent anvendelse af dette direktiv. Sådanne konsultationer skal navnlig finde sted vedrørende kritiske enheder, der: a) anvender kritisk infrastruktur, som er fysisk sammenkoblet mellem to eller flere medlemsstater, b) er en del af selskabsstrukturer, som er sammenkoblet eller forbundet med kritiske enheder i en anden medlemsstat, c)

er blevet identificeret som kritiske enheder i en medlemsstat, og som leverer væsentlige tjenester til eller i andre medlemsstater. De i stk. 1 omhandlede konsultationer tager sigte på at styrke kritiske enheders modstandsdygtighed og, hvor det er muligt, mindske disses administrative byrde.

Her vil klima-, energi- og forsyningsministeren have hjemmel i den foreslåede § 28, stk. 1, til at konsultere med kompetente myndigheder, CSIRT'er og Centrale Kontaktpunkter i andre medlemsstater for at sikre konsekvent anvendelse direktivet på kritiske enheder.

Det følger endvidere af CER-direktivets artikel 15, stk. 3, at på grundlag af oplysninger leveret af en kritisk enhed i en underretning om en hændelse, jf. den foreslåede § 12, orienterer den relevante kompetente myndighed via det centrale kontaktpunkt andre berørte medlemsstaters centrale kontaktpunkter, hvis hændelsen har eller kunne have betydelig indvirkning på kritiske enheder og kontinuiteten i leveringen af væsentlige tjenester til eller i en eller flere andre medlemsstater. Det følger af samme bestemmelse, at centrale kontaktpunkter, der fremsender og modtager sådanne oplysninger, i overensstemmelse med EU-retten eller national ret skal behandle disse oplysninger på en måde, der respekterer deres fortrolighed og beskytter den berørte kritiske enheds sikkerhed og kommercielle interesser.

Efter bestemmelsen i CER-direktivets artikel 15, stk. 3, vil Klima-, Energi- og Forsyningsministeriet således i relevant omfang skulle videregive oplysninger, som er modtaget i medfør af de foreslåede bestemmelser i §§ 12 og 15 om hændelsesunderretninger, til øvrige berørte medlemsstater.

På baggrund af CER-direktivets artikel 17, stk. 2, skal myndighederne endvidere videregive oplysninger til Kommissionen om identiteten af kritiske enheder, som leverer væsentlige tjenester til eller i seks eller flere medlemsstater, samt om de oplysninger, som enhederne leverer i henhold til den foreslåede bestemmelse i § 5, stk. 2.

Det følger af CER-direktivets artikel 18, stk. 3, skal medlemsstaten efter en begrundet anmodning fra Kommissionen eller en eller flere medlemsstater, hvortil eller hvori den væsentlige tjeneste leveres, som har identificeret en kritisk enhed af særlig europæisk betydning som en kritisk enhed i henhold til artikel 6, stk. 1, Kommissionen følgende: a) de relevante dele af den kritiske enheds risikovurdering, b) en oversigt over relevante foranstaltninger, der er truffet i overensstemmelse med artikel 13, c) tilsyns- eller håndhævelsestiltag, herunder vurderinger af overholdelse eller udstedte

påbud, som den kompetente myndighed har taget i henhold til artikel 21 og 22 med hensyn til den pågældende kritiske enhed.

Her vil klima-, energi- og forsyningsministeren have hjemmel i den foreslåede § 28, stk. 1, til at fremsende de oplysninger der er nævnt, til Kommissionen eller til andre EU-medlemsstater, jf. dog § 28, stk. 2 i lovforslaget.

Endeligt følger det af CER-direktivets artikel 18, stk. 4, at medlemsstater, hvor det er nødvendigt, skal kunne rådgive Kommissionen om, hvorvidt den kritiske enhed af særlig europæisk betydning opfylder sine forpligtigelser i henhold til direktivet kapitel III, og, hvis det er relevant, hvilke foranstaltninger der kunne træffes for at forbedre den pågældende kritiske enheds modstandsdygtighed.

Artikel 18, stk. 4, fastsætter endvidere at den kompetente myndighed, der har identificeret en kritisk enhed i henhold til artikel 6, stk. 1 i CER-direktivet, skal give Kommissionen og de medlemsstater, hvortil eller hvori den væsentlige tjeneste leveres oplysninger om de foranstaltninger, som den kompetente myndighed og kritiske enhed af særlig europæisk betydning har truffet i medfør af den udtalelse Kommissionen har givet den kritiske enhed af særlig europæisk betydning og den kompetente myndighed efter artikel 18, stk. 4, 3. afsnit.

Her vil klima-, energi- og forsyningsministeren have hjemmel i den foreslåede § 28, stk. 1, til at fremsende de oplysninger til Kommissionen eller til andre EU-medlemsstater som CER-direktivets artikel 18, stk. 4 påkræver, jf. dog § 28, stk. 2 i lovforslaget.

Til § 29 [Kapitel 10]

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 NIS 2-direktivet, og artikel 1, stk. 8, i CER-direktivet, som fastsætter, at de forpligtelser, der er fastsat i de to direktiver, 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.

Baggrunden for artikel 1, stk. 8, beskrives i CER-direktivets præambelbetragtning nr. 11, hvoraf det fremgår, at ingen medlemsstat bør være forpligtet til at meddele oplysninger, hvis videregivelse vil stride mod væsentlige

interesser med hensyn til dens nationale sikkerhed, og at EU-regler eller nationale regler om beskyttelse af klassificerede informationer og hemmeligholdelsesaftaler er relevante.

Klima-, Energi- og Forsyningsministeriet har lagt vægt på, at der foretages en direktivnær minimumsimplementering af bestemmelsen. Den foreslåede bestemmelse svarer indholdsmæssigt til NIS 2-direktivets artikel 2, stk. 11 og CER-direktivets artikel 1, stk. 8, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Der er en vis usikkerhed om fortolkningen af bestemmelsens udstrækning.

Det er Klima-, Energi- og Forsyningsministeriets 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 Klima-, Energi- og Forsyningsministeriets 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), er det er Klima-, Energi- og Forsyningsministeriets 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 virksomhed mere generelt kan undlade at efterkomme oplysningsforpligtelserne over for de kompetente myndigheder, herunder som led i myndighedernes tilsyn. Det er Klima-, Energi- og Forsyningsministeriets opfattelse, at det kun vil være i yderst sjældne tilfælde, at videregivelse af en virksomheds oplysninger til Klima-, Energi- og Forsyningsministeriet eller CSIRT'en 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 virksomhed eller Klima-, Energi- og Forsyningsministeriet eller CSIRT'en 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 og artikel 15, stk. 3, i CER-direktivet, 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.

Mens det følger af CER-direktivets artikel 15, stk. 3, at på grundlag af oplysninger leveret af en kritisk enhed i en underretning om en hændelse, orienterer den relevante kompetente myndighed via det centrale kontaktpunkt andre berørte medlemsstaters centrale kontaktpunkter, hvis hændelsen har eller kunne have betydelig indvirkning på kritiske enheder og kontinuiteten i leveringen af væsentlige tjenester til eller i en eller flere andre medlemsstater. Det følger videre, at centrale kontaktpunkter, der fremsender og modtager sådanne oplysninger, i overensstemmelse med EU-retten eller national ret skal behandle sådanne på en måde, der respekterer deres fortrolighed og beskytter den berørte kritiske enheds sikkerhed og kommercielle interesser.

Den foreslåede bestemmelse vil finde anvendelse, uanset om oplysningerne modtages direkte fra den pågældende nationale myndighed eller via andre, herunder Europa-Kommissionen.

Til § 30 [Kapitel 10]

Det følger af den foreslåede *§ 30,* at klima-, energi- og forsyningsministeren 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 virksomheder 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 virksomheder skal foretage underretninger om hændelser i medfør af de foreslåede §§ 12-15. 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 den foreslåede § 35, skal efterkommes ved anvendelse af bestemte internetløsninger såsom Virk.dk.

Der kan med hjemmel i bestemmelsen fastsættes regler om, at skriftlige henvendelser til relevante myndigheder, herunder Energistyrelsen, Energinet, 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 virksomhed 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 virksomheds computere ikke fungerer, at enheden har mistet koden til sin digitale signatur, eller at der opstår lignende hindringer, som det er op til virksomheden 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 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 § 31 [Kapitel 11]

Det følger af elforsyningslovens § 89, gasforsyningslovens § 51, VE-lovens § 66, og olieberedskabslovens § 21, at Energiklagenævnet behandler klager over afgørelser truffet af klima-, energi-, og forsyningsministeren efter denne lov eller regler udstedt i medfør af loven. Desuden regulerer bestemmelserne, hvilke formelle krav der er til klager. Beredskabsforpligtelser for energisektoren finder anvendelse på virksomheder, som reguleres af de ovenfor nævnte love.

Det følger af den foreslåede § 31, *stk. 1,* at Energiklagenævnet behandler klager over afgørelser truffet af klima-, energi- og forsyningsministeren eller anden statslig myndighed efter denne lov eller regler udstedt i henhold til loven.

Det bemærkes i den forbindelse, at hvis klima-, energi- og forsyningsministeren har bemyndiget en under ministeriet oprettet institution eller anden myndighed til at udøve beføjelserne, vil klageadgangen følge denne bemyndigelse. Klager over afgørelser efter denne lov truffet af en myndighed under ministeriet, kan således påklages direkte til Energiklagenævnet. Klageren skal ikke udnytte den ulovsbestemte rekursmulighed, før der kan ske klage til energiklagenævnet.

Det følger af den foreslåede § 31, *stk. 2,* at klima-, energi- og forsyningsministerens afgørelser nævnt i stk. 1, ikke kan indbringes for anden administrativ myndighed end Energiklagenævnet. Afgørelserne kan ikke indbringes for domstolene, før den endelige administrative afgørelse foreligger.

Bestemmelsen er en videreførelse af gældende bestemmelser om Energiklagenævnet i elforsyningslovens, gasforsyningsloven, olieberedskabsloven m.v., som regulerer energisektoren. Det foreslås at samme regler om administrativ klageadgang anvendes i beredskabsreguleringen for energisektoren.

Det følger af den foreslåede § 31, *stk. 3,* at klage skal være indgivet skriftligt inden 4 uger efter, at afgørelsen er meddelt.

Bestemmelsen er en videreførelse af gældende bestemmelser om Energiklagenævnet i elforsyningslovens, gasforsyningsloven, olieberedskabsloven m.v., som regulerer energisektoren. Det foreslås at samme regler om klagefrist anvendes i beredskabsreguleringen for energisektoren.

Klagefristen vil først begynde at løbe fra en endelig administrativ afgørelse er truffet. Hvis klageren har anvendt rekursmuligheden, vil fristen da først løbe fra den dato, hvor rekursmyndigheden meddeler klageren afgørelsen.

Det følger af den foreslåede § 31, *stk. 4,* at Energiklagenævnets formand kan efter nærmere aftale med nævnet træffe afgørelse på nævnets vegne i sager, der behandles efter denne lov eller regler udstedt i henhold til loven.

Henset til at ikke alle sager som nævnet skal behandle efter loven eller regler udstedt i henhold til loven, nødvendigvis kræver stillingtagen fra et samlet nævn, foreslås det, at der i stk. 4 gives formanden mulighed for efter aftale med de øvrige nævnsmedlemmer selv at træffe afgørelse i nogle sager eller typer af sager.

Bestemmelsen er en videreførelse af gældende bestemmelser om Energiklagenævnet i elforsyningslovens, gasforsyningsloven, olieberedskabsloven m.v., som regulerer energisektoren. Det foreslås, at samme regler om formandens kompetence til at træffe afgørelser på vegne af nævnet, anvendes i beredskabsreguleringen for energisektoren.

Det følger af den foreslåede § 31, *stk. 5*, at søgsmål til prøvelse af afgørelser truffet af Energiklagenævnet efter loven eller de regler, der udstedes efter loven, skal være anlagt inden 6 måneder efter, at afgørelsen er meddelt den pågældende. Er afgørelsen offentlig bekendtgjort, regnes fristen dog altid fra bekendtgørelsen.

Bestemmelsen er en videreførelse af gældende bestemmelser om Energiklagenævnet i elforsyningslovens, gasforsyningsloven, olieberedskabsloven m.v., som regulerer energisektoren. Det foreslås at samme regler om frist for indbringelse hos domstolene anvendes i beredskabsreguleringen for energisektoren.

Det følger af den foreslåede § 31, *stk. 6*, at Energiklagenævnet, i forbindelse med behandling af en klage, kan indhente oplysninger der er nødvendige for behandling af klagen fra virksomheder omfattet af loven samt myndigheder der træffer afgørelser efter loven eller regler udstedt i medfør af loven.

Den foreslåede bestemmelse sikrer, at Energiklagenævnet kan indhente de oplysninger, der er nødvendige for at behandle klagesager.

Til § 3 [Kapitel 11]

Ifølge elforsyningslovens § 90, gasforsyningslovens § 52 og olieberedskabslovens fastsætte nærmere regler om; 1) adgang til klage over afgørelser, 2) at visse afgørelser ikke skal kunne inde bringes for klima-, energi- og forsyningsministeren, 3) betaling af gebyrer for at klage til Energiklagenævnet.

Det følger af den foreslåede § 32, *stk. 1,* at klima-, energi- og forsyningsministeren kan fastsætte regler om adgangen til at klage over afgørelser, der efter loven eller regler udstedt i henhold til loven træffes af klima., energi- og forsyningsministeren, herunder at visse afgørelser ikke skal kunne indbringes for Energiklagenævnet.

Det forventes på baggrund af nr. 1, at der fastsættes nærmere regler om, at afgørelser truffet efter lovens kapitel 5 om baggrundstjek og sikkerhedsgodkendelser eller regler udstedt i medfør af kapitel 5 ikke kan påklages til Energiklagenævnet.

Afgørelser om baggrundstjek og sikkerhedsgodkendelser for energisektoren anvendes som en foranstaltning til at sikre mod eksempelvis insider trusler, eller for at sikre at der ikke snydes med personers identitet, i forbindelse med de skal have adgang til kritisk infrastruktur. Baggrundtjek og sikkerhedsgodkendelser vedrører således områder knyttet til statens sikkerhed.

Afgørelser vedrørende baggrundtjek og sikkerhedsgodkendelser er ikke noget der knytter sig særligt til Energiklagenævnets kendskab til juridiske eller tekniske spørgsmål på energiområdet.

Da afgørelser om sikkerhedsgodkendelser vedrører statens sikkerhed og falder uden for Energiklagenævnets almindelige behandlingsområde, vurderes det, at Energiklagenævnet ikke skal være klageinstans for denne type af afgørelser.

Det bemærkes i den forbindelse, at afgørelser om baggrundstjek og sikkerhedsgodkendelser kan indbringes for domstolene ligesom alle andre myndighedsafgørelser, jf. Grundlovens § 63, stk. 1.

Efter den foreslåede § 32, stk. 2, *nr. 1, 1. pkt.,* kan erhvervsministeren fastsætte regler om, at kommunikation med Energiklagenævnet skal ske digitalt.

Bestemmelsen vil medføre, at der ved bekendtgørelse kan fastsættes regler om, at borgere og virksomheder har pligt til at kommunikere digitalt med Energiklagenævnet, og at svaret fra Energiklagenævnet sendes digitalt.

Bemyndigelsen til fastsættelse af regler vedrørende Energiklagenævnet tillægges erhvervsministeren, da ressortansvaret for Energiklagenævnet er tillagt erhvervsministeren, jf. kongelig resolution af 8. juni 2016.

Efter den foreslåede § 32, stk. 2, nr. 1, *2. pkt.*, kan ministeren herunder udstede regler om anvendelse af et bestemt digitalt system.

Bestemmelsen vil indebære, at erhvervsministeren kan anvende bestemmelsen til at fastsætte regler om f.eks. pligtmæssig brug af et digitalt system, herunder f.eks. Klageportalen, ved indgivelse af klage i medfør af loven, og at svar fra Energiklagenævnet sendes digitalt. Med digitalt system menes, at der kan laves regler om brug af bestemte digitale systemer, herunder selvbetjeningsløsninger, særlige digitale formater, digital signatur eller lignende.

Efter den foreslåede § 32, stk. 2, nr. 1, *3. pkt.*, skal der ved fastsættelse af regler efter 1. pkt. fastsættes regler om fritagelse for obligatorisk anvendelse for visse personer og virksomheder.

Det følger af den foreslåede § 32, stk. 2, *nr. 2,* at erhvervsministeren kan fastsætte regler om betaling af gebyr ved indbringelse af en klage for Energiklagenævnet.

Bestemmelsen vil medføre, at der ved bekendtgørelse kan fastsættes regler om Energiklagenævnets behandling af klager i medfør af denne lov samt om gebyrbetaling for sådan klageindgivelse ved Energiklagenævnet.

Bemyndigelsen vil bl.a. kunne anvendes til at kunne fastsætte regler om nævnets, formandens og sekretariatets opgaver og beføjelser. Den foreslåede bemyndigelse vil bl.a. også give mulighed for at fastsætte regler om indsendelse og behandling af klager. Denne adgang suppleres af den foreslåede § 17, stk. 2, der vil give mulighed for at fastsætte regler om obligatorisk anvendelse af et bestemt digitalt system, herunder f.eks. Klageportalen. Den foreslåede bemyndigelse giver endvidere mulighed for at udstede regler om eventuel anvendelse af en postkassemodel, dvs. en model hvor klagen indgives til nævnet via 1. instansen.

Herudover vil bemyndigelsen kunne anvendes til at fastsætte regler om frister, herunder regler der supplerer klagefristen, der fremgår direkte af den foreslåede § 31, stk. 3. Den foreslåede bemyndigelse vil også dække fastsættelse af regler om indsendelse af oplysninger.

Endvidere vil erhvervsministeren kunne fastsætte regler om betaling af gebyr ved indbringelse af en klage for Energiklagenævnet. Herunder vil der bl.a. kunne fastsættes regler om gebyrets størrelse og beregning. Der vil eksempelvis kunne være tale om engangsgebyr ved indgivelse af klagen.

Den foreslåede bestemmelse vil også kunne anvendes til at fastsætte regler om, at gebyret kun delvist skal dække nævnets udgifter ved klagebehandlingen, at det er klager, som skal betale omkostningerne i form af gebyret og at gebyret skal betales helt eller delvist tilbage, hvis klager får helt eller delvist medhold i sin klage.

Bemyndigelsen til fastsættelse af regler vedrørende Energiklagenævnet tillægges erhvervsministeren, da ressortansvaret for Energiklagenævnet er tillagt erhvervsministeren, jf. kongelig resolution af 8. juni 2016.

Det følger af den foreslåede § 32, stk. 2, *nr. 3,* at erhvervsministeren kan fastsætte nærmere regler om Energiklagenævnets sammensætning vednævnets behandling af afgørelser efter denne lov eller regler udstedt i medfør af loven.

Bestemmelsen vil indebære, at den korrekte sagkundskab kan sammensættes ved behandling af klagesager over afgørelser vedrørende beredskab og cybersikkerhed i energisektoren.

Beføjelsen til at fastsætte nærmere regler om Energinævnets sammensætning tillægges erhvervsministeren, da ressortansvaret for Energiklagenævnet er tillagt erhvervsministeren, jf. kongelig resolution af 8. juni 2016.

Til § 33 [Kapitel 11]

Det følger af den foreslåede *§ 33,* at Klima-, energi- og forsyningsministeren kan bemyndige en under ministeriet oprettet institution eller anden myndighed til at udøve de beføjelser, der i denne lov er tillagt ministeren.

Bestemmelsen vil indebære, at klima-, energi- og forsyningsministeren kan bemyndige en under Klima-, Energi- og Forsyningsministeriet oprettet statslig myndighed, f.eks. Energistyrelsen, til at udøve beføjelser, der i loven er tillagt ministeren.

Bestemmelsen vil desuden kunne anvendes til, at klima-, energi- og forsyningsministeren kan indgå i forhandlinger med andre ministre om at bemyndige statslige myndigheder oprettet under vedkommende ministerie til at udøve beføjelser tillagt til klima-, energi- og forsyningsministeren i denne lov.

Lovgivningen vil således være fremtidssikret i det tilfælde, at det i fremtiden vurderes, at en anden statslig myndighed vil være bedre passende til at

udøve visse af ministerens beføjelser, end den oprindeligt udpegede myndighed. Herudover vil klima-, energi- og forsyningsministeren have mulighed for at forhandle om inddragelse af andre ministeriers kompetencer, som disse måtte findes relevante for den hensigtsmæssige forvaltning af reguleringen for beredskab i energisektoren

Det skal dog bemærkes, at et sådant pålæg ikke kan meddeles Forsyningstilsynet i forhold til de opgaver, som tilsynet skal varetage efter loven, herunder også henset til Forsyningstilsynets uafhængighed, jf. § 2 i lov om Forsyningstilsynet. Grænserne for Energistyrelsens beføjelser i henhold til loven vil fremgå af bekendtgørelsen om Energistyrelsens opgaver og beføjelser.

Til § 34 [Kapitel 11]

Det følger af den foreslåede *§ 34,* at Klima-, energi- og forsyningsministeren kan fastsætte regler eller træffe bestemmelser med henblik på at gennemføre eller anvende internationale konventioner og EU-regler om forhold, der er omfattet af denne lov, herunder forordninger, direktiver og beslutninger om beredskab og beskyttelse af energiinfrastruktur på søterritoriet og den eksklusive økonomiske zone.

Europa-Kommissionen er flere steder i CER- og NIS 2-direktiverne tillagt kompetence til at vedtage retsakter, der nærmere udmønter bestemte dele af direktivet. Energisektoren er desuden underlagt anden regulering fra EU om beredskab i energisektoren.

Det følger bl.a. af CER-direktivets artikel 5, stk. 1, at Kommissionen tillægges beføjelse til at vedtage en delegeret retsakt i overensstemmelse med direktivets artikel 23 senest den 17. november 2023 for at supplere CER-direktivet ved at udarbejde en ikke-udtømmende liste over væsentlige tjenester i sektorerne og delsektorerne anført i direktivets bilag. Kommissionen har ved sin delegerede forordning (EU) 2023/2450 af 25. juli 2023 til supplering af Europa-Parlamentets og Rådets direktiv (EU) 2022/2557 opstillet en ikke-udtømmende liste over væsentlige tjenester.

Desuden følger det af CER-direktivets artikel 13, stk. 6, at Kommissionen vedtager gennemførelsesretsakter med henblik på at fastsætte de nødvendige tekniske og metodiske specifikationer vedrørende anvendelsen af modstandsdygtighedsforanstaltninger efter artikel 13, stk. 1.

Det følger endvidere af CER-direktivets artikel 18, stk. 6, at Kommissionen vedtager en gennemførelsesretsakt med regler for de proceduremæssige ordninger for tilrettelæggelse af rådgivende EU-delegationer.

Det fremgår derudover af CER-direktivets artikel 19, stk. 6, at Kommissionen kan vedtage gennemførelsesretsakter, hvori der fastlægges proceduremæssige ordninger, som er nødvendige for Gruppen for Kritiske Enheders Modstandsdygtigheds funktion.

I medfør af artikel 21, stk. 5, 2. led, i NIS 2-direktivet kan Europa-Kommissionen 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 gennemførelsesretsakter om foranstaltninger til styring af cybersikkerhedsrisici følger Europa-Kommissionen i videst muligt omfang europæiske og internationale standarder samt relevante tekniske specifikationer. Europa-Kommissionen samarbejder med samarbejdsgruppen som er nedsat i medfør af NIS 2 artikel, stk. 1, og ENISA om udkastene til gennemførelsesretsakter.

Det følger desuden af NIS 2-direktivets artikel 23, stk. 11, at Europa-Kommissionen kan vedtage gennemførelsesretsakter, der yderligere præciserer typen af oplysninger, formatet og proceduren for en underretning indgivet i henhold til artikel 23, stk. 1 (underretning af myndighederne om hændelser), og artikel 30 (frivillig meddelelse af relevante oplysninger) og for en meddelelse, der er indgivet i henhold til artikel 23, stk. 2 (oplysning til modtagerne af tjenester).

Det følger endvidere af NIS 2-direktivets artikel 24, stk. 2, at Europa-Kommissionen tillægges beføjelser til at vedtage delegerede retsakter for at supplere NIS 2-direktivet ved at præcisere, hvilke kategorier af væsentlige og vigtige enheder der skal anvende visse certificerede IKT-produkter, -tjenester og -processer eller indhente en attest i henhold til en europæisk cybersikkerhedscertificeringsordning, der er vedtaget i henhold til artikel 49 i Europa-Parlamentets og Rådets forordning (EU) 2019/881 af 17. april 2019 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed), om cybersikkerhedscertificering af informations- og kommunikationsteknologi og om ophævelse af forordning (EU) nr. 526/2013 (forordningen

om cybersikkerhed). Disse delegerede retsakter vedtages, når der er identificeret utilstrækkelige cybersikkerhedsniveauer og de skal indeholde en gennemførelsesperiode.

Den foreslåede bestemmelse vil give Klima-, energi- og forsyningsministeren hjemmel til at gennemføre Europa-Kommissionens retsakter og internationale konventioner om beredskab for energisektoren.

Til § 35 [Kapitel 11]

Efter gældende ret i elforsyningslovens § 84, varmeforsyningslovens § 23 d, fjernkølingslovens § 8 c, olieberedskabslovens § 17, stk. 2, undergrundslovens § 26 og gasforsyningslovens § 45, kan klima-, energi- og forsyningsministeren indhente oplysninger som er nødvendige for varetagelsen af alle opgaver eller nogle specifikke opgaver ministeren har efter disse love, fra virksomheder omfattet af disse love. I forarbejderne til de nævnte paragraffer fremgår det at der bl.a. er tale om regnskaber, regnskabsmateriale, udskrift af bøger, andre forretningspapirer og elektronisk lagrede data. Det fremgår også i forarbejderne til undergrundsloven

Det følger af den foreslåede § 35, *stk. 1,* at klima-, energi- og forsyningsministeren og Energinetkan indhente oplysninger, der er nødvendige for varetagelsen af deres opgaver efter loven, efter bestemmelser fastsat i henhold til loven eller efter EU-retsakter eller internationale forpligtelser om forhold omfattet af loven, fra virksomheder omfattet af loven.

Klima-, energi- og forsyningsministeren og Energinet kan med hjemmel i den foreslåede bestemmelse kræve alle oplysninger, som skønnes nødvendige for deres virksomhed efter loven, eller til afgørelse af om et forhold er omfattet af lovens bestemmelser, herunder regnskaber, regnskabsmateriale, udskrift af bøger, andre forretningspapirer, elektronisk lagrede data m.m. Med den foreslåede bestemmelse kan ministeren og Energinet også kræve sammenstilling af eksisterende data, således det gøres tilgængelig og forståelig og således anvendelig ift. den opgave der skal varetages. Endelig kan den foreslåede bestemmelse også bruges til at kræve generering af nye oplysninger hos virksomheden, såfremt virksomheden ikke allerede har gjort sig bekendt med egne forhold. Her tænkes således på situationer, hvor virksomheden f.eks. ikke allerede måtte være bekendt med hvor meget salg, kapacitet, produktion etc. virksomheden har/har haft, som er data der er nødvendigt for at klima-, energi- og forsyningsministeren kan determinere om virksomheden er omfattet af loven eller ej.

Det følger af den foreslåede § 35, *stk. 2*, at Klima-, energi- og forsyningsministeren fastsætter regler om, at virksomheder skal registrere sig og hvilke oplysningerne virksomheder i den forbindelse skal oplyse, herunder at virksomhederne skal oplyse følgende; 1) virksomhedens navn, 2) Adresse og ajourførte kontaktoplysninger, herunder e-mailadresser, IP-intervaller og telefonnumre, 3) den relevante sektor og delsektor, som virksomheden er omfattet af, 4) de medlemsstater i Den Europæiske Union, hvor virksomheden leverer tjenester.

Bestemmelsen gennemfører NIS 2-direkitvets artikel 3, stk. 3 og 4, hvorefter medlemsstaterne senest den 17. april 2025 udarbejder 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. Med henblik på udarbejdelsen af listes pålægger medlemsstaterne enhederne, at indgive mindst følgende oplysninger til de kompetente myndigheder; a) enhedens navn, b) 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 omhandlede enheder skal i tilfælde af ændringer af de oplysninger, de har indgivet, straks give underretning herom og under alle omstændigheder senest to uger efter datoen for ændringen.

Efter den foreslåede bestemmelse, vil klima-, energi- og forsyningsministeren fastsætte regler for, hvilke virksomheder der skal registrere sig og hvordan registreringen skal foregå.

Ministeren kan på baggrund af bestemmelsen fastsætte den nærmere dato, for hvornår virksomheder senest skal indgive oplysninger efter bestemmelsen og regler udsted i medfør af bestemmelsen. Virksomheder, der omfattes af denne lov, efter den fastsatte dato, vil skulle indgive oplysninger efter en nærmere angiven frist.

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.

Ministeren kan derudover, for at sikre, at oplysningerne er tilstrækkeligt ajourførte, fastsatte en frist for, hvornår virksomheder skal oplyse om ændringer af oplysninger. Ministeren vil fastsætte en frist for virksomheder, for underretning om ændringer i oplysninger.

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.

Klima-, energi- og forsyningsministeren vil derfor som minimum fastsætte en frist på to uger, for nye virksomheder at indgive oplysninger. Ministeren vil desuden som minimum fastsætte en frist på to uger, for underretning om ændringer i oplysninger til brug for registrering af virksomheden.

Klima-, energi- og forsyningsministeren kan fastsætte en kortere frist, for virksomheder på baggrund af deres betydning for energiforsyningen. Ministeren kan dermed fastsætte en differentieret frist for virksomhederne, på baggrund af kritikalitet. Denne differentierede frist, vil som udgangspunkt kun gælde for den underretning, som virksomhederne skal foretage om ændringer i allerede indmeldte oplysninger.

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 energivirksomhederne, som er omfattet af lovens anvendelsesområde. Det forudsættes, at virksomheder, 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, herunder Klima-, Energi- og Forsyningsministeriet 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 virksomheder, som opfylder kravene for væsentlige og vigtige enheder for hver sektor og delsektor.

Til § 36 [Kapitel 12]

Det følger af elforsyningslovens § 87, stk. 1, nr. 7, at medmindre højere straf er forskyldt efter anden lovgivning, straffes den med bøde, der undlader at efterkomme påbud eller forbud efter loven, herunder påbud om at berigtige et ulovligt forhold. Desuden kan der efter elforsyningslovens § 88, stk. 1, i regler udstedt i henhold til loven, fastsættes bødestraf. I bekendtgørelse om beredskab i naturgassektorens § 35, stk. 1, er der fastsat nærmere regler for bødestraf.

Det følger af gasforsyningslovens § 49, stk. 1, nr. 6, at medmindre højere straf er forskyldt efter anden lovgivning, straffes med bøde den, der undlader at efterkomme påbud eller forbud efter loven, herunder påbud om at berigtige et ulovligt forhold. Desuden kan der efter gasforsyningslovens § 50, stk. 1, i regler udstedt i henhold til loven, fastsættes bødestraf. I bekendtgørelse om beredskab i elsektorens § 35, stk. 1, er der fastsat nærmere regler for bødestraf.

Efter olieberedskabslovens § 23, stk. 1, nr. 5, gælder det at medmindre højere straf er forskyldt efter anden lovgivning, straffes med bøde den, der undlader at efterkomme påbud efter loven eller regler udstedt i medfør af loven. Af olieberedskabslovens § 23, stk. 2, følger det at der kan fastsættes bødestraf for overtrædelse af bestemmelserne i reglerne eller vilkår fastsat i henhold til reglerne og for manglende overholdelse af påbud meddelt i henhold til reglerne. Bekendtgørelse om beredskab for oliesektorens § 22, er der fastsat nærmere regler for bødestraf.

For nærmere gennemgang af sanktioner i de forskellige delsektorer henvises der i øvrigt til de almindelige bemærkninger i afsnit 3.7.1.

Det foreslås i § 36, *stk. 1,* at den der; 1) overtræder §§ 6-10, § 11, stk. 2, §§ 12 og 13, 2) undlader at efterkomme en afgørelse efter § 23, stk. 1, nr. 1 eller 2, 3) undlader at efterkomme påbud efter § 21 og § 22, stk. 2, 4) undlader at efterkomme krav efter § 14, stk. 2 eller § 19, stk. 2, nr. 5-7, 5) hindrer myndighederne i at føre kontrol efter bestemmelserne i 20, stk. 2, nr. 1-4, 6) meddeler klima-, energi- og forsyningsministeren eller Energiklagenævnet urigtige eller vildledende oplysninger eller efter anmodning undlader at afgive oplysninger, straffes med bøde.

Den foreslåede bestemmelse vil gennemføre artikel 36, stk. 1, i NIS 2-direktivet. Artikel 36, stk. 1, forpligter medlemsstaterne til at fastsætte regler om sanktioner, der skal anvendes i tilfælde af overtrædelser af de nationale foranstaltninger, der er vedtaget i medfør af NIS 2-direktivet og til at træffe alle nødvendige foranstaltninger for at sikre, at de gennemføres. Sanktionerne skal være effektive, stå i rimeligt forhold til overtrædelsen og have afskrækkende virkning.

Den foreslåede bestemmelse vil endvidere gennemføre NIS 2-direktivets artikel 34, hvoraf det følger, at medlemsstaterne sikrer, at de administrative bøder, der pålægges væsentlige og vigtige enheder i henhold til artiklen, for så vidt angår overtrædelser af direktivet, er effektive, står i rimeligt forhold til overtrædelsen og har afskrækkende virkning, under hensyntagen til omstændighederne i hver enkelt sag.

Efter artikel 34, stk. 2, kan administrative bøder pålægges i tillæg til en hvilken som helst af foranstaltningerne omhandlet i artikel 32, stk. 4, litra a-h, artikel 32, stk. 5, og artikel 33, stk. 4, litra a-g.

Efter NIS 2-direktrivets 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 NIS 2-direkitvets 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 af NIS 2-direktivets 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.

Den foreslåede bestemmelse vil herudover – 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.

Den foreslåede bestemmelse gennemfører desuden artikel 22, 1. og 2. pkt., i CER-direktivet, hvoraf følger, at 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.

Det forudsættes at det alene er de bestemmelser der specifikt henvises til, som vil have særlige betydning for så vidt angår udmålingen af bøders størrelse. Det samme gælder eventuel udmåling af bøder til fysiske personer, hvor det dog i overensstemmelse med NIS 2-direktivets præambelbetragtning nr. 130, 2. pkt., forudsættes, at der lægges vægt på det generelle indkomstniveau og personens økonomiske stilling.

For virksomheder svarende til væsentlige enheder efter NIS 2-direktivet, forudsættes det i overensstemmelse med NIS 2-direktivets artikel 34, stk. 4, at bødens størrelse for virksomheders overtrædelse af bestemmelserne i §§ 6-10, § 11, stk. 2, §§ 12 og 13, § 14, stk. 2, § 19, stk. 2, nr. 1-7, §§ 21 og 22, 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.

For virksomheder svarende til vigtige enheder efter NIS 2-direktivet, forudsættes det i overensstemmelse med NIS 2-direktivets artikel 34, stk. 5, at bødens størrelse for virksomheders overtrædelse af bestemmelserne i §§ 6-10, § 11, stk. 2, §§ 12 og 13, § 14, stk. 2, § 19, stk. 2, nr. 1-7, §§ 21 og 22,

maksimalt vil udgøre et beløb svarende til 7.000.000 euro eller 1,4 pct.af den væsentlige enheds samlede globale årsomsætning i det foregående regnskabsår alt efter, hvad der er højest.

Det forudsættes i overensstemmelse med CER-direktivets artikel 22 og 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 og §§ 15-16, 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 og CER-direktivets artikel 22, være effektiv, stå i et rimeligt forhold til overtrædelsen og have afskrækkende virkning under hensyntagen til omstændighederne i den konkrete sag.

Bøde vil i overensstemmelse med NIS 2-direktivets artikel 34, stk. 2, kunne pålægges i tillæg til håndhævelsesforanstaltningerne i de foreslåede §§ 20, 22 og 23.

Der lægges med loven ikke op til at omfatte virksomheder baseret på antal ansatte og virksomhedens årlige omsætning eller bruttofortjeneste. Det skyldes, at denne afgrænsning ikke inddrager virksomhedernes forsyningsmæssige størrelse og kritikalitet, og at kun få energivirksomheder vil blive omfattet. Eksempelvis kan koncernkonstruktioner med datterselskaber indebære, at energivirksomheder med stor kritikalitet kan have få ansatte. I stedet lægges der op til for begge direktiver at følge den nuværende afgrænsningsmodel i energisektoren, som er den model, der bl.a. er blevet brugt ved implementering af NIS1-direktivet i energisektoren. Herved er det forsyningsstørrelsen, der primært er afgørende for, om virksomheden omfattes af beredskabsregulering, da forsyningsstørrelsen afspejler virksomhedens kritikalitet for energiforsyningen. Det vurderes, at denne afgrænsning stadig lever op til direktiverne.

Den foreslåede bestemmelse svarer indholdsmæssigt til NIS 2-direktivets artikel 35, stk. 2, for så vidt angår væsentlige enheder. Bestemmelsen fastsætter desuden bødestraf for overtrædelser af bestemmelser, som implementerer CER-direktivet, og går dermed videre end minimumskravene i CER-direktivets artikel 22. Bestemmelsen skal derudover forstås og anvendes i overensstemmelse med direktivernes forudsætninger.

Om valg af ansvarssubjekt henvises til afsnit 3.5.2.3 i lovforslagets almindelige bemærkninger.

Det foreslås i § 36, *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) vil kunne ifalde strafansvar for overtrædelse af denne lov efter reglerne i straffelovens kapitel 5.

Det foreslås i § 36, *stk. 3*, at hvor der er pålagt en bøde for overtrædelse af 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 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.

Den foreslåede bestemmelse svarer indholdsmæssigt til NIS 2-direktivets artikel 35, stk. 2, og skal således forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Klima- Energi- og Forsyningsministeriet vil fortsat kunne anvende håndhævelsesforanstaltninger i medfør af denne lov, uagtet at der måtte være pålagt en bøde for overtrædelse af databeskyttelseslovgivningen.

Det foreslås i § 36, *stk. 4*, at der i forskrifter, der udstedes i henhold til loven, kan fastsættes straf af bøde for overtrædelse af bestemmelser i forskrifterne.

Bestemmelsen vil indeholde hjemmel til fastsættelse af straffebestemmelser i forskrifter, som vil skulle medvirke til at sikre overholdelse af reglerne, der forventes udmøntet ved administrativ regulering i form af bekendtgørelser.

Til § 37 [Kapitel 13]

Det foreslås, at loven skal træde i kraft den 1. januar 2025.

Til § 38 [Kapitel 14]

Det følger af § 16 i olieberedskabsloven, at lagringspligtige virksomheder skal foretage den nødvendige planlægning og træffe de nødvendige foranstaltninger for at sikre forsyningen af råolie og olieprodukter i beredskabssituationer og andre ekstraordinære situationer. Det følger endvidere af § 16, stk. 2, at den centrale lagerenhed skal varetage de overordnede, koordinerende planlægningsmæssige og operative opgaver vedrørende det beredskab, der er anført i stk. 1. Klima-, energi- og forsyningsministeren kan fastsætte regler om varetagelse af de i stk. 1 nævnte opgaver samt om vare-

tagelse af de overordnede, koordinerende planlægningsmæssige og operative opgaver vedrørende beredskabet, jf. § 16, stk. 3, i olieberedskabsloven.

Det foreslås, at § 16 ophæves.

Bestemmelsen foreslås ophævet af hensyn til, at det er vurderet mere hensigtsmæssigt at samle bestemmelserne om beredskab i energisektoren i nærværende lovforslag, i stedet for at der findes regler herom i de forskellige forsyningslove.

Ændringen vil således medføre, at hjemmelsgrundlaget for beredskab i energisektoren fremadrettet vil være samlet i én lov, hvilket vil give et samlet overblik over beredskabsreguleringen for de omfattede virksomheder, hvoraf en del er multiforsyningsvirksomheder eller har aktiviteter i flere delsektorer. Ændringen vil dermed gøre det lettere for virksomhederne at navigere i den regulering, som de er underlagt med hensyn til beredskab.

Til § 39 [Kapitel 14]

Til nr. 1

Det følger af § 51 d, i elforsyningsloven, at virksomheder med elproduktionsbevilling efter § 10, stk. 1, eller med tilladelse til elproduktion fra anlæg med en kapacitet på over 25 MW efter § 29 i lov om fremme af vedvarende energi eller § 11, netvirksomheder og virksomheder, der yder balancering af elsystemet, betaler halvårligt et beløb til Klima-, Energi- og Forsyningsministeriet til dækning af omkostninger til tilsyn med virksomhederne efter regler udstedt i medfør af § 85 b, stk. 4, og § 85 c, stk. 6

Det foreslås, at § 51 d ophæves.

Bestemmelsen foreslås ophævet af hensyn til, at det er vurderet mere hensigtsmæssigt at samle bestemmelserne om beredskab i energisektoren i nærværende lovforslag, i stedet for at der findes regler herom i de forskellige forsyningslove.

Ændringen vil således medføre, at hjemmelsgrundlaget for beredskab i energisektoren fremadrettet vil være samlet i én lov, hvilket vil give et samlet overblik over beredskabsreguleringen for de omfattede virksomheder,

hvoraf en del er multiforsyningsvirksomheder eller har aktiviteter i flere delsektorer. Ændringen vil dermed gøre det lettere for virksomhederne at navigere i den regulering, som de er underlagt med hensyn til beredskab.

Til nr. 2

I konsekvens af den foreslåede samling af bestemmelser om beredskab, herunder en samling af de nødvendige bemyndigelser for klima-, energi- og forsyningsministeren til at kunne fastsætte regler om beredskab i en bekendtgørelse, i en ny lov om styrket beredskab i energisektoren og hvormed de relevante beredskabsbestemmelser i forsyningslovene, herunder elforsyningsloven foreslås ophævet, foreslås det, at beredskab slettes i overskriften i kapitel 12.

Der henvises til lovforslagets § 39, nr. 1, og bemærkningerne hertil.

Til nr. 3

Det følger af elforsyningsloven § 85b, stk. 1, at virksomheder, som er bevillingspligtige efter §§ 10 og 19 eller har tilladelse til elproduktion fra anlæg med en kapacitet på over 25 MW efter § 29 i lov om fremme af vedvarende energi eller § 11, samt elforsyningsvirksomhed, der varetages af Energinet eller denne virksomheds helejede datterselskaber i medfør af § 2, stk. 2 og 3, i lov om Energinet, skal foretage nødvendig planlægning og træffe nødvendige foranstaltninger for at sikre elforsyningen i beredskabssituationer og andre ekstraordinære situationer.

Energinet skal varetage de overordnede, koordinerende planlægningsmæssige og operative opgaver vedrørende det i stk. 1 nævnte beredskab, jf. elforsyningsloven § 85 b, stk. 2.

Klima-, energi- og forsyningsministeren kan fastsætte regler om varetagelse af de i § 85 b, stk. 1 og 2 nævnte opgaver, jf. § 85b, stk. 3 lov om elforsyning, ligesom Klima-, energi- og forsyningsministeren i medfør af 85b, stk. 4 i lov om elforsyning kan fastsætte regler om udførelse af tilsyn med det beredskabsarbejde, der udføres efter stk. 1 og 2, herunder om virksomhedernes fremsendelse af materiale som grundlag for tilsynet, om tilsynets beføjelser i forhold til virksomhederne og om klageadgang.

Det følger endvidere af elforsyningsloven § 85c, stk. 1, at samme virksomheder skal opretholde et it-beredskab, herunder planlægge og træffe nødvendige foranstaltninger for at sikre beskyttelsen af kritiske it-systemer, der er af betydning for elforsyningen.

Klima-, energi- og forsyningsministeren fastsætter nærmere regler for it-beredskab, jf. § 85 c, stk. 1, herunder regler om; 1) organisering af virksomhedens it-beredskab og evne til at modtage advarsler om trusler mod it-sikkerheden, 2) planlægning og beredskabsarbejde, som virksomhederne skal udføre for at modvirke trusler mod it-sikkerheden, herunder virksomhedernes pligt til at videregive oplysninger til Energinet og relevante myndigheder, 3) virksomhedernes risikostyring, herunder inddragelse af andre virksomheder i risikovurderinger, 4) tilmelding til en it-sikkerhedstjeneste, der yder varsler og informationer om it-sikkerhedstrusler, 5) Energinets varetagelse af overordnede, koordinerende planlægningsmæssige og operative opgaver vedrørende it-beredskab, jf. stk. 1, og 6) krav til indholdet og planlægningen af en it-revision ved en uafhængig revisor, jf. stk. 2.

Klima-, energi- og forsyningsministeren fastsætter desuden nærmere regler for udførelsen af tilsyn med virksomheders it-beredskab, jf. § 85 c, stk. 1.

Det foreslås, at § 85b og § 85c ophæves.

Bestemmelsen foreslås ophævet af hensyn til, at det er vurderet mere hensigtsmæssigt at samle bestemmelserne om beredskab i energisektoren i nærværende lovforslag, i stedet for at der findes regler herom i de forskellige forsyningslove.

Ændringen vil således medføre, at hjemmelsgrundlaget for beredskab i energisektoren fremadrettet vil være samlet i én lov, hvilket vil give et samlet overblik over beredskabsreguleringen for de omfattede virksomheder, hvoraf en del er multiforsyningsvirksomheder eller har aktiviteter i flere delsektorer. Ændringen vil dermed gøre det lettere for virksomhederne at navigere i den regulering, som de er underlagt med hensyn til beredskab.

Der henvises til lovforslagets almindelige bemærkninger i afsnit 2.

Til § 40 [Kapitel 14]

Til § nr. 1

I konsekvens af den foreslåede samling af bestemmelser om beredskab, herunder en samling af de nødvendige bemyndigelser for klima-, energi- og forsyningsministeren til at kunne fastsætte regler om beredskab i en bekendtgørelse, i en ny lov om styrket beredskab i energisektoren og hvormed de relevante beredskabsbestemmelser i forsyningslovene, herunder gasforsyningsloven foreslås ophævet, foreslås det, at beredskab slettes i overskriften før § 15 a ophæves.

Til nr. 2

Det følger af § 15 a, stk. 1 i lov om gasforsyning, at selskaber, der er bevillingspligtige efter § 10, samt Energinet og denne virksomheds helejede datterselskaber, der varetager gasvirksomhed i medfør af § 2, stk. 2 og 3, i lov om Energinet skal foretage nødvendig planlægning og træffe de nødvendige foranstaltninger for at sikre gasforsyningen i beredskabssituationer og andre ekstraordinære situationer. Af samme bestemmelse følger det, at Klima-, energi- og forsyningsministeren kan bestemme, at opstrømsanlæg og bygasnet tilsvarende skal foretage sådan planlægning og træffe sådanne foranstaltninger.

I medfør af § 15 a, stk. 2 1 i lov om gasforsyning skal Energinet varetage de overordnede, koordinerende planlægningsmæssige og operative opgaver vedrørende det i stk. 1 nævnte beredskab.

§ 15 a, stk. 3 og 4 indeholder bemyndigelsesbestemmelser til at Klima-, energi- og forsyningsministeren kan fastsætte regler om henholdsvis varetagelse af beredskabsopgaverne i stk. 1 og 2 samt kan fastsætte regler om udførelse af tilsyn med det beredskabsarbejde, der udføres efter stk. 1 og 2.

Lov om gasforsyning indeholder i § 15 b, stk. 1 en tilsvarende en tilsvarende bestemmelse for IT-beredskab. Det følger blandt andet, at lov om gasforsyning, at selskaber, der er bevillingspligtige efter § 10, samt Energinet og dennes helejede datterselskaber, der varetager gasforsyningsvirksomhed i henhold til § 2, stk. 2 og 3, i lov om Energinet, skal opretholde et it-beredskab, herunder planlægge og træffe nødvendige foranstaltninger for at sikre beskyttelsen af kritiske it-systemer, der er af væsentlig betydning for gasforsyningen.

Det foreslås, at § 15 a og § 15 b ophæves.

Bestemmelserne foreslås ophævet af hensyn til, at det er vurderet mere hensigtsmæssigt at samle bestemmelserne om beredskab i energisektoren i nærværende lovforslag, i stedet for at der findes regler herom i de forskellige forsyningslove.

Ændringen vil således medføre, at hjemmelsgrundlaget for beredskab i energisektoren fremadrettet vil være samlet i én lov, hvilket vil give et samlet overblik over beredskabsreguleringen for de omfattede virksomheder, hvoraf en del er multiforsyningsvirksomheder eller har aktiviteter i flere delsektorer. Ændringen vil dermed gøre det lettere for virksomhederne at navigere i den regulering, som de er underlagt med hensyn til beredskab.

Til nr. 3.

Det følger af § 30, a, stk. 5 i lov om gasforsyning, at Energinet og denne virksomheds helejede datterselskaber i medfør af § 2, stk. 2 og 3, i lov om Energinet, der driver lagervirksomhed, og selskaber, der driver distributionsvirksomhed efter bevilling, betaler halvårligt et beløb til Klima-, Energi- og Forsyningsministeriet til dækning af omkostninger til tilsyn med selskaberne efter regler udstedt i medfør af § 15 a, stk. 4, og § 15 b, stk. 6.

I medfør af § 30 a, stk. 6 i lov om gasforsyning, kan klima-, energi- og forsyningsministeren fastsætter størrelsen af beløbet efter stk. 5, herunder fordelingen af omkostningerne på kategorier af selskaber.

Det foreslås, at *§ 30 a, stk. 5 og 6* ophæves.

Stk. 6 og 7 bliver herefter stk. 5 og 6.

Den foreslåede ændring vil medføre, at virksomheder omfattet af gasforsyningslovens af § 30, a ikke vil blive opkrævet et halvårligt gebyr efter elforsyningsloven til dækning af Klima-, Energi- og Forsyningsministeriets omkostninger til tilsyn med virksomhedernes organisatoriske beredskab, fysiske sikring og cybersikkerhed, samt til dækning af de omkostninger, der er til administration af ordningen.

Klima-, Energi- og Forsyningsministeriets vil derimod fremadrettet opkræve et halvårligt gebyr hos virksomhederne til dækningen af tilsvarende opgaver efter nærværende lovforslags § 18, stk. 1, hvorved der sker en vi-

dereførelse af den eksisterende gebyrordning for tilsynet med gasvirksomhedernes organisatoriske beredskab, fysiske sikring og cybersikkerhed og dækning af de omkostninger, der er til administration af ordningen.

Ophævelsen af § 30 a, stk. 5 og 6 vil derfor ikke medføre nogle ændringer i praksis på området, da den erstattes af nærværende lovforslags § 18, stk. 1

Til § 41 [Kapitel 14]

Til nr. 1

Anvendelsesområdet for prisreguleringen i lov om varmeforsyning fremgår af § 20, stk. 1. Bestemmelsen finder anvendelse på virksomheder, der leverer opvarmet vand, damp eller gas bortset fra naturgas til det indenlandske marked med det formål at levere energi til bygningers opvarmning og forsyning med varmt vand. [Det drejer sig blandt andet om kollektive varmeforsyningsanlæg, jf. § 2, i lov om varmeforsyning.]

Bestemmelsen i § 20, stk. 1, indeholder princippet om nødvendige omkostninger. Princippet indebærer, at de varmeforsyningsvirksomheder, der er omfattet af bestemmelsen, kan opkræve de nødvendige omkostninger, der er forbundet med levering af det opvarmede vand m.m. til rumvarmeformål. De omkostninger, der må indregnes i priserne, skal ud over at være nødvendige, også efter deres art være indregningsberettigede.

Det foreslås i *§ 20, stk. 1, 1. pkt.* at indsætte en henvisning til omkostninger til beredskab efter lov om styrket beredskab i energisektoren.

Den foreslåede ændring vil medføre, at varmeforsyningsvirksomheder omfattet af § 20, stk. 1, som udgangspunkt vil kunne indregne omkostninger til beredskab som en nødvendig omkostning i sine varmepriser.

Varmeforsyningsvirksomhedernes omkostninger til beredskab vil fortsat skulle være nødvendige efter § 20, stk. 1. Derudover må prisen ikke være urimelig, jf. § 21, stk. 4, i lov om varmeforsyning. En varmeforsyningsvirksomheds omkostninger til beredskab vil således fortsat være underlagt Forsyningstilsynets tilsyn og indgrebsbeføjelse efter § 21, stk. 4.

Det er ikke hensigten med lovforslaget derudover at ændre den måde, som Forsyningstilsynet i dag fører tilsyn i medfør af § 21, stk. 4, i varmeforsyningsloven. Forsyningstilsynet vil derfor skulle føre sit sædvanlige tilsyn på omkostninger til beredskab.

Der henvises til lovforslagets almindelige bemærkninger i afsnit 3.8.

Til nr. 2

Det følger af § 29 a i lov om varmeforsyning, at virksomheder, som driver anlæg til produktion og fremføring af bygas, skal foretage nødvendig planlægning og træffe de nødvendige foranstaltninger for at sikre bygasforsyningen i beredskabssituationer og andre ekstraordinære situationer. Klima, energi- og forsyningsministeren kan fastsætte regler om varetagelse af de i stk. 1 nævnte opgaver samt om varetagelse af de overordnede, koordinerende planlægningsmæssige og operative opgaver vedrørende beredskabet, jf. § 29 a, stk. 2, i lov om varmeforsyning.

Det foreslås, at *§ 29 a* ophæves.

Den foreslåede ændring er en konsekvens af den foreslåede samling af bestemmelser om beredskab, herunder en samling af de nødvendige bemyndigelser for klima-, energi- og forsyningsministeren til at kunne fastsætte regler om beredskab i en bekendtgørelse, i en ny lov om [styrket] beredskab i energisektoren. Det er vurderet mere hensigtsmæssigt at samle bestemmelserne i en ny hovedlov i stedet for, at der – som nu- findes regler herom i de forskellige forsyningslove. Det vil derfor være nødvendigt at ophæve bestemmelsen i lov om varmeforsyning.

Til § 42 [Kapitel 14]

Det følger af § 17 a, stk. 1 i lov om anvendelse af Danmarks undergrund, at rettighedshavere med tilladelse til efterforskning og indvinding af kulbrinter eller tilladelse til etablering og drift af rørledningsanlæg i forbindelse med indvinding af kulbrinter skal planlægge med hensyn til opretholdelse og videreførelse af forsyningen af kulbrinter til samfundet i tilfælde af krisesituationer, herunder udarbejde beredskabsplaner og gennemføre nødvendige foranstaltninger til sikring af egne anlæg, rørledninger, kritiske systemer og data m.v. Dette gælder også ejere af tilstødende olie- og naturgasrørledningsanlæg, separationsfaciliteter og terminalanlæg for råolie, jf.

§ 1 i lov om etablering og benyttelse af en rørledning til transport af råolie og kondensat og §§ 3 a og 4 i lov om kontinentalsoklen og visse rørledningsanlæg på søterritoriet. Rettighedshavere og ejere skal koordinere dette beredskab med beredskab efter anden lovgivning.

I medfør af § 17 a, stk. 2 i lov om anvendelse af Danmarks undergrund, hvis rettighedshaveren eller ejeren består af en eller flere fysiske eller juridiske personer i forening, gælder stk. 1 for hver enkelt af disse.

Det følger af § 17 a, stk. 3 i lov om anvendelse af Danmarks undergrund, at klima-, energi- og forsyningsministeren kan fastsætte nærmere regler om varetagelse af de opgaver, som er anført i stk. 1, herunder om fremsendelse af oplysninger af relevans for dette arbejde til ministeren, og nærmere regler om gennemførelse af EU-regler.

Med bemyndigelsen er der tilvejebragt hjemmel til at fastsætte regler om bl.a. følgende forhold af betydning for samfundets energiforsyning:

– Virksomhedernes beredskabsplanlægning. Det er hensigten at fastsætte regler om den beredskabsplanlægning, som skal foretages af virksomhederne. Denne beredskabsplanlægning omfatter især forhold om udarbejdelse af risiko- og sårbarhedsvurderinger, udarbejdelse af beredskabsplaner, afholdelse af øvelser om de væsentligste dele af beredskabsplanerne, evaluering af hændelser af betydning for dette beredskab samt medvirken i myndighedernes beredskab på energiområdet.

– Virksomhedernes fremsendelse af oplysninger til myndighederne. Det er hensigten at fastsætte regler herom, idet sådanne oplysninger, primært om kritiske situationer samt deres udvikling og håndtering, er centrale for myndighedernes beredskab efter den nationale beredskabsplan. Tilsvarende er det centralt, at virksomhederne på en effektiv måde kan modtage oplysninger herom fra myndighederne.

– Identifikation af kritisk infrastruktur. Det er hensigten at fastsætte regler herom, idet en central del af beredskabsarbejdet er identifikation af anlæg, rørledninger, kritiske systemer og data m.v., som har kritisk betydning for samfundets energiforsyning.

– Sikring af kritisk infrastruktur. Det er hensigten at fastsætte regler om sikring af kritisk infrastruktur over for naturgivne og menneskabte hændelser som led i beredskabsarbejdet.

– Virksomhedernes arbejde om cyber- og informationssikkerhed. Det er hensigten at fastsætte regler om virksomhedernes arbejde med beskyttelse af deres centrale aktiviteter over for cyber-trusler samt deres beskyttelse af kritiske informationer, både på digital form og på anden form.

Hjemlen anvendes også til gennemførelse af EU-regler om beredskab af betydning for de nævnte forsyningsmæssige forhold.

Reglerne i medfør af stk. 3 udarbejdes i samarbejde med oliebranchen.

Med lovforslaget foreslås § 17 a ophævet.

Bestemmelsen foreslås ophævet af hensyn til, at det er vurderet mere hensigtsmæssigt at samle bestemmelserne om beredskab i energisektoren i nærværende lovforslag, i stedet for at der findes regler herom i de forskellige forsyningslove.

Ændringen vil således medføre, at hjemmelsgrundlaget for beredskab i energisektoren fremadrettet vil være samlet i én lov, hvilket vil give et samlet overblik over beredskabsreguleringen for de omfattede virksomheder, hvoraf en del er multiforsyningsvirksomheder eller har aktiviteter i flere delsektorer. Ændringen vil dermed gøre det lettere for virksomhederne at navigere i den regulering, som de er underlagt med hensyn til beredskab.

Til § 43 [Kapitel 14]

Det følger af § 2, stk. 2, at Energinet varetager en sammenhængende og helhedsorienteret planlægning efter reglerne i denne lov, lov om elforsyning, lov om fremme af vedvarende energi og lov om gasforsyning og driver systemansvarlig virksomhed, eltransmissionsvirksomhed og gastransmissionsvirksomhed.

Energinets opgavevaretagelse på beredskabsområdet er nærmere fastlagt i beredskabsbekendtgørelserne nr. 821 2446 og 2647, hvorefter Energinet blandt andet varetager de overordnede, koordinerende planlægningsmæssige og operative opgaver vedrørende beredskabssituationerne i el- og gassektoren.

Det foreslås i *§ 20, stk. 1, 1. pkt.* at indsætte en henvisning til lov om styrket beredskab i energisektoren.

Bestemmelsen foreslås ændret i konsekvens af bestemmelserne om beredskab i energisektoren samles i nærværende lovforslag, i stedet for at der findes regler herom i de forskellige forsyningslove.

Det forventes de gældende regler angående Energinets opgavevaretagelse i medfør af beredskabsbekendtgørelserne for elsektoren og naturgassektoren videreføres for el- og gassektoren, dog med tilføjelse af brintsektoren såfremt der måtte etableres et brinttransmissionssystem i Danmark, samt tilføjelse af de nye aktører, der vil omfattes af beredskabsreguleringen i delsektorerne for el-, gas. Disse aktører er hovedsageligt dikteret af NIS2 og CER-direktivernes bilag om disses anvendelsesområde.

Til § 44 [Kapitel 15]

Det foreslås, at loven ikke skal gælde for Færøerne og Grønland.

Bilag 1

Lovforslaget sammenholdt med gældende lov

Gældende formulering	Lovforslaget
	§ 38 I olieberedskabslov jf. lov nr. 354 af 24. april 2012, foretages følgende ændringer:
§ 16. Lagringspligtige virksomheder skal foretage den nødvendige planlægning og træffe de nødvendige foranstaltninger for at sikre forsyningen af råolie og olieprodukter i beredskabssituationer og andre ekstraordinære situationer. *Stk. 2.* Den centrale lagerenhed skal varetage de overordnede, koordinerende planlægningsmæssige og operative opgaver vedrørende det beredskab, der er anført i stk. 1. *Stk. 3.* Klima-, energi- og bygningsministeren kan fastsætte nærmere regler om virksomhedernes beredskabsplanlægning efter stk. 1 og den centrale lagerenheds overordnede, koordinerende planlægningsmæssige og operative beredskabsopgaver efter stk. 2.	**1.** *§ 16,* ophæves.

	§ 39 I lov om elforsyning jf. lovbekendtgørelse nr. 1248 af 24. oktober 2023, foretages følgende ændringer:
§ 51 d. Virksomheder med elproduktionsbevilling efter § 10, stk. 1, eller med tilladelse til elproduktion fra anlæg med en kapacitet på over 25 MW efter § 29 i lov om fremme af vedvarende energi eller § 11, netvirksomheder og virksomheder, der yder balancering af elsystemet, betaler halvårligt et beløb til Klima-, Energi- og Forsyningsministeriet til dækning af omkostninger til tilsyn med virksomhederne efter regler udstedt i medfør af § 85 b, stk. 4, og § 85 c, stk. 6. *Stk. 2.* Klima-, energi- og forsyningsministeren fastsætter regler om størrelsen af beløb efter stk. 1, herunder om fordelingen af omkostningerne på kategorier af virksomheder. Klima-, energi- og forsyningsministeren kan fastsætte nærmere regler om betaling og opkrævning af beløb efter stk. 1.	**1.** *§ 51 d*, ophæves.

Kapitel 12 *Beredskab, fortrolighed, kontrol, oplysningspligt og påbud*	
§ 85 b. Virksomheder, som er bevillingspligtige efter §§ 10 og 19 eller har tilladelse til elproduktion fra anlæg med en kapacitet på over 25 MW efter § 29 i lov om fremme af vedvarende energi eller § 11, samt elforsyningsvirksomhed, der varetages af Energinet eller denne virksomheds helejede datterselskaber i medfør af § 2, stk. 2 og 3, i lov om Energinet, skal foretage nødvendig planlægning og træffe nødvendige foranstaltninger for at sikre elforsyningen i beredskabssituationer og andre ekstraordinære situationer. *Stk. 2.* Energinet skal varetage de overordnede, koordinerende planlægningsmæssige og operative opgaver vedrørende det i stk. 1 nævnte beredskab. *Stk. 3.* Klima-, energi- og forsyningsministeren kan fastsætte regler om varetagelse af de i stk. 1 og 2 nævnte opgaver. *Stk. 4.* Klima-, energi- og forsyningsministeren kan fastsætte regler om udførelse af tilsyn med det	**2.** *Overskriften* til kapitel 12 affattes således: »Kapitel 12 *Fortrolighed, kontrol, oplysningspligt og påbud*«

beredskabsarbejde, der udføres efter stk. 1 og 2, herunder om virksomhedernes fremsendelse af materiale som grundlag for tilsynet, om tilsynets beføjelser i forhold til virksomhederne og om klageadgang. **§ 85 c.** Virksomheder, som er bevillingspligtige efter §§ 10 og 19 eller har tilladelse til elproduktion fra anlæg med en kapacitet på over 25 MW efter § 29 i lov om fremme af vedvarende energi eller § 11, Energinet og dennes helejede datterselskaber samt virksomheder, der yder balancering af elsystemet, skal opretholde et it-beredskab, herunder planlægge og træffe nødvendige foranstaltninger for at sikre beskyttelsen af kritiske it-systemer, der er af betydning for elforsyningen. *Stk. 2.* Klima-, energi- og forsyningsministeren kan ved manglende opfyldelse af et påbud efter § 85 d om at overholde stk. 1 påbyde virksomheder at foretage en it-revision af kritiske systemer ved en uafhængig revisor godkendt af tilsynsmyndigheden. *Stk. 3.* Klima-, energi- og forsyningsministeren kan påbyde virksomheder at gennemføre tiltag, som på baggrund af en it-revision, jf. stk. 2, skønnes nødvendige for at opretholde et it-beredskab, jf. stk. 1.	**3.** *§§ 85 b og 85 c,* ophæves.

Stk. 4. Informationer, herunder vurderinger, planer og data, vedrørende sikkerhedsforhold for kritiske it-systemer i virksomheder omfattet af stk. 1 er fortrolige, hvis oplysningerne er væsentlige af hensyn til driften af virksomheden eller det sammenhængende elsystem. *Stk. 5.* Klima-, energi- og forsyningsministeren fastsætter nærmere regler for it-beredskab, jf. stk. 1, herunder regler om 1) organisering af virksomhedens it-beredskab og evne til at modtage advarsler om trusler mod it-sikkerheden, 2) planlægning og beredskabsarbejde, som virksomhederne skal udføre for at modvirke trusler mod it-sikkerheden, herunder virksomhedernes pligt til at videregive oplysninger til Energinet og relevante myndigheder, 3) virksomhedernes risikostyring, herunder inddragelse af andre virksomheder i risikovurderinger, 4) tilmelding til en it-sikkerhedstjeneste, der yder varsler og informationer om it-sikkerhedstrusler, 5) Energinets varetagelse af overordnede, koordinerende planlægningsmæssige og operative opgaver vedrørende it-beredskab, jf. stk. 1, og	

6) krav til indholdet og planlægningen af en it-revision ved en uafhængig revisor, jf. stk. 2. *Stk. 6.* Klima-, energi- og forsyningsministeren fastsætter regler for udførelse af tilsyn med virksomheders it-beredskab, jf. stk. 1.	
	§ 40 I lov om gasforsyning jf. lovbekendtgørelse nr. 1100 af 16. august 2023, foretages følgende ændringer:
Beredskab **§ 15 a.** Selskaber, der er bevillingspligtige efter § 10, samt Energinet og denne virksomheds helejede datterselskaber, der varetager gasvirksomhed i medfør af § 2, stk. 2 og 3, i lov om Energinet skal foretage nødvendig planlægning og træffe de nødvendige foranstaltninger for at sikre gasforsyningen i beredskabssituationer og andre ekstraordinære situationer. Klima-, energi- og forsyningsministeren kan bestemme, at opstrømsanlæg	**1.** *Overskriften* før § 15 a ophæves.

og bygasnet tilsvarende skal foretage sådan planlægning og træffe sådanne foranstaltninger. *Stk. 2.* Energinet skal varetage de overordnede, koordinerende planlægningsmæssige og operative opgaver vedrørende det i stk. 1 nævnte beredskab. *Stk. 3.* Klima-, energi- og forsyningsministeren kan fastsætte regler om varetagelse af de i stk. 1 og 2 nævnte opgaver, herunder om udveksling af nødvendige data i de i stk. 1 nævnte situationer og for at undgå sådanne situationer. *Stk. 4.* Klima-, energi- og forsyningsministeren kan fastsætte regler om udførelse af tilsyn med det beredskabsarbejde, der udføres efter stk. 1 og 2, herunder om selskabernes fremsendelse af materiale som grundlag for tilsynet, om tilsynets beføjelser i forhold til selskaberne og om klageadgang. **§ 15 b.** Selskaber, der er bevillingspligtige efter § 10, samt Energinet og dennes helejede datterselskaber, der varetager gasforsyningsvirksomhed i henhold til § 2, stk. 2 og 3, i lov om Energinet, skal opretholde et it-beredskab, herunder planlægge og træffe nødvendige foranstaltninger for at sikre beskyttelsen af kritiske it-systemer, der er af væsentlig betydning for gasforsyningen.	**2.** *§§ 15 a* og *15 b*, ophæves.

Stk. 2. Klima-, energi- og forsyningsministeren kan ved manglende opfyldelse af et påbud efter § 47 b om at overholde stk. 1 påbyde virksomheder at foretage en it-revision af kritiske it-systemer ved en uafhængig revisor godkendt af tilsynsmyndigheden. *Stk. 3.* Klima-, energi- og forsyningsministeren kan påbyde virksomheder at gennemføre tiltag, som på baggrund af en it-revision, jf. stk. 2, skønnes nødvendige for at opretholde et it-beredskab, jf. stk. 1. *Stk. 4.* Informationer, herunder vurderinger, planer og data, vedrørende sikkerhedsforhold for forsyningskritiske it-systemer i virksomheder, som er omfattet af stk. 1, er fortrolige, hvis oplysningerne er væsentlige af hensyn til driften af virksomheden eller gassystemet. *Stk. 5.* Klima-, energi- og forsyningsministeren fastsætter nærmere regler for it-beredskab, jf. stk. 1, herunder regler om 1) organisering af virksomhedens it-beredskab og evne til at modtage advarsler om trusler mod it-sikkerheden, 2) planlægning og beredskabsarbejde, som virksomhederne skal udføre for at modvirke trusler mod it-sikkerheden, herunder virksom-	

hedernes pligt til at videregive oplysninger til Energinet og til klima-, energi- og forsyningsministeren, 3) virksomhedernes risikostyring, herunder inddragelse af andre virksomheder i risikovurderinger, 4) tilmelding til en tjeneste, der yder varsler og informationer om it-sikkerhedstrusler, 5) Energinets varetagelse af overordnede, koordinerende planlægningsmæssige og operative opgaver vedrørende it-beredskabet, jf. stk. 1, og 6) krav til indholdet og planlægningen af en it-revision ved en uafhængig revisor, jf. stk. 2. *Stk. 6.* Klima-, energi- og forsyningsministeren fastsætter regler for udførelse af tilsyn med det beredskabsarbejde, der udføres efter stk. 1. **§ 30 a.** --- *Stk. 2-4.* --- *Stk. 5.* Energinet og denne virksomheds helejede datterselskaber i medfør af § 2, stk. 2 og 3, i lov om Energinet, der driver lagervirksomhed, og selskaber, der driver distributionsvirksomhed efter bevilling, betaler halvårligt et beløb	**3.** *§ 30 a, stk. 5 og 6,* ophæves. stk. 6 og 7 bliver herefter stk. 5 og 6.

til Klima-, Energi- og Forsyningsministeriet til dækning af omkostninger til tilsyn med selskaberne efter regler udstedt i medfør af § 15 a, stk. 4, og § 15 b, stk. 6. *Stk. 6.* Klima-, energi- og forsyningsministeren fastsætter størrelsen af beløbet efter stk. 5, herunder fordelingen af omkostningerne på kategorier af selskaber. *Stk. 7.* Klima-, energi- og forsyningsministeren kan fastsætte regler om betaling og opkrævning af beløb til dækning af omkostningerne efter stk. 1, 2, 5 og 6.	**4.** I *§ 30 a, stk. 7,* der bliver stk. 6, ændres »stk. 1, 2, 5 og 6.« til: »stk. 1 og 2.«æ
	§ 41 I lov om varmeforsyning jf. lovbekendtgørelse nr. 124 af 2. februar 2024, 2068 foretages følgende ændringer:
§ 20. Kollektive varmeforsyningsanlæg, industrivirksomheder, kraftvarmeanlæg med en eleffekt over 25 MW samt geotermiske anlæg m.v. kan i priserne for levering til det indenlandske marked af opvarmet vand, damp eller gas bortset fra naturgas med det formål at	

levere energi til bygningers opvarmning og forsyning med varmt vand indregne nødvendige udgifter til energi, lønninger og andre driftsomkostninger, efterforskning, administration og salg, omkostninger som følge af pålagte offentlige forpligtelser, herunder omkostninger til energispareaktiviteter efter §§ 28 a, 28 b og 29, samt finansieringsudgifter ved fremmedkapital, herunder ved et statsfinansieret lån, og underskud fra tidligere perioder opstået i forbindelse med etablering og væsentlig udbygning af forsyningssystemerne, jf. dog stk. 7-19 og §§ 20 b, 20 c og 20 e. 1. pkt. finder tilsvarende anvendelse på levering af opvarmet vand til andre formål fra et centralt kraft-varme-anlæg, jf. § 10, stk. 6, i lov om elforsyning. 1. pkt. finder ikke anvendelse på virksomheder, der leverer overskudsvarme, hvor anlægget, der udnytter og leverer overskudsvarme, har en kapacitet på under 0,25 MW. *Skt. 2-19.* --- **§ 29 a.** Virksomheder, som driver anlæg til produktion og fremføring af bygas, skal foretage nødvendig planlægning og træffe de nødvendige foranstaltninger for at sikre bygasforsyningen i beredskabssituationer og andre ekstraordinære situationer.	**1.** I *§ 20, stk. 1, 1. pkt.,* indsættes efter »§§ 28 a, 28 b og 29«: »og omkostninger til beredskab efter lov om styrket beredskab i energisektoren,«.

Stk. 2. Klima-, energi- og forsyningsministeren kan fastsætte regler om varetagelse af de i stk. 1 nævnte opgaver samt om varetagelse af de overordnede, koordinerende planlægningsmæssige og operative opgaver vedrørende beredskabet.	**2.** *§ 29 a,* ophæves.

	§ 42 I lov om anvendelse af Danmarks undergrund jf. lovbekendtgørelse 1461 af 29. november 2023, foretages følgende ændringer.
§ 17 a. Rettighedshavere med tilladelse til efterforskning og indvinding af kulbrinter eller tilladelse til etablering og drift af rørledningsanlæg i forbindelse med indvinding af kulbrinter skal planlægge med hensyn til opretholdelse og videreførelse af forsyningen af kulbrinter til samfundet i tilfælde af krisesituationer, herunder udarbejde beredskabsplaner og gennemføre nødvendige foranstaltninger til sikring af egne anlæg, rørledninger, kritiske systemer og data m.v. Dette gælder også ejere af tilstødende olie- og naturgasrørledningsanlæg, separationsfaciliteter og terminalanlæg for råolie, jf. § 1 i lov om etablering og benyttelse af en rørledning til transport af råolie og kondensat og §§ 3 a og 4 i lov om kontinentalsoklen og visse rørledningsanlæg på søterritoriet. Rettighedshavere og ejere skal koordinere dette beredskab med beredskab efter anden lovgivning.	

Stk. 2. Hvis rettighedshaveren eller ejeren består af en eller flere fysiske eller juridiske personer i forening, gælder stk. 1 for hver enkelt af disse. *Stk. 3.* Klima-, energi- og forsyningsministeren kan fastsætte nærmere regler om varetagelse af de opgaver, som er anført i stk. 1, herunder om fremsendelse af oplysninger af relevans for dette arbejde til ministeren, og nærmere regler om gennemførelse af EU-regler.	**1.** *§ 17 a* ophæves.
	§ 43 I lov om energinet jf. lovbekendtgørelse nr. 271 af 09. marts 2023, foretages følgende ændringer.
§ 2. --- *Stk. 1.* --- *Stk. 2.* Energinet varetager en sammenhængende og helhedsorienteret planlægning efter reglerne i denne lov, lov om elforsyning, lov om fremme af vedvarende energi og lov om gasforsyning og driver systemansvarlig virksomhed, eltransmissionsvirksomhed og	

gastransmissionsvirksomhed. Endvidere varetager Energinet administrative opgaver vedrørende miljøvenlig elektricitet i medfør af lov om elforsyning, administrative opgaver vedrørende gas fra vedvarende energikilder i medfør af lov om gasforsyning, administrative opgaver vedrørende miljøvenlig elektricitet i medfør af lov om fremme af vedvarende energi og administrative opgaver i medfør af lov om pilotudbud af pristillæg for elektricitet fremstillet på solcelleanlæg. Energinet kan endvidere varetage gasdistributions-, gaslager- og gasopstrømsrørlednings- og gasopstrømsanlægsvirksomhed. Endvidere kan Energinet varetage opgaver vedrørende CO_2-transportnet og CO_2-lagringslokaliteter. Energinet kan tillige efter pålæg fra klima-, energi- og forsyningsministeren varetage opgaver vedrørende forundersøgelser og koblingsanlæg. Endelig kan Energinet varetage olierørledningsvirksomhed og dertil knyttet separationsvirksomhed. *Stk. 3-6.* ---	**1.** I *§ 2, stk. 2, 1. pkt.,* indsættes efter »reglerne i denne lov«: lov om styrket beredskab «.