2024/1366

24.5.2024

KOMMISSIONENS DELEGEREDE FORORDNING (EU) 2024/1366

af 11. marts 2024

om supplerende regler til Europa-Parlamentets og Rådets forordning (EU) 2019/943 for så vidt angår fastsættelse af netregler om sektorspecifikke regler for cybersikkerhedsmæssige aspekter af grænseoverskridende elektricitetsstrømme

(EØS-relevant tekst)

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

under henvisning til Europa-Parlamentets og Rådets forordning (EU) 2019/943 af 5. juni 2019 om det indre marked for elektricitet ([1]), særlig artikel 59, stk. 2, litra e), og

ud fra følgende betragtninger:

(1) Cybersikkerhedsrisikostyring er afgørende for at opretholde elforsyningssikkerheden og sikre et højt cybersikkerhedsniveau i elsektoren.

(2) Digitalisering og cybersikkerhed er en forudsætning for at kunne udbyde væsentlige tjenester og er derfor af strategisk betydning for kritisk energiinfrastruktur.

(3) Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 ([2]) fastsætter foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen. Europa-Parlamentets og Rådets forordning (EU) 2019/941 ([3]) supplerer direktiv (EU) 2022/2555 ved at sikre, at cybersikkerhedshændelser i elsektoren bliver korrekt kategoriseret som en risiko, og at de foranstaltninger, der træffes for at håndtere dem, er ordentligt afspejlet i risikoberedskabsplanerne. Forordning (EU) 2019/943 supplerer direktiv (EU) 2022/2555 og forordning (EU) 2019/941 ved at fastsætte specifikke regler for elsektoren på EU-plan. Derudover supplerer denne delegerede forordning bestemmelserne i direktiv (EU) 2022/2555 om elsektoren, når der er tale om grænseoverskridende elektricitetsstrømme.

(4) I forbindelse med indbyrdes forbundne digitaliserede elektricitetssystemer kan forebyggelse og styring af elkriser, der er relateret til cyberangreb, ikke betragtes som en udelukkende national opgave. Mere effektive og mindre omkostningstunge foranstaltninger gennem regionalt samarbejde og EU-samarbejde bør udarbejdes for at udnytte det fulde potentiale. Der er derfor behov for en fælles regelramme og bedre koordinerede procedurer for at sikre, at medlemsstaterne og andre aktører kan samarbejde effektivt på tværs af grænserne i en ånd af øget gennemsigtighed, tillid og solidaritet mellem medlemsstaterne og kompetente myndigheder med ansvar for elektricitet og cybersikkerhed.

(5) Cybersikkerhedsrisikostyring inden for denne forordnings anvendelsesområde kræver en struktureret proces, der bl.a. omfatter kortlægning af risici, som grænseoverskridende elektricitetsstrømme er udsat for som følge af cyberangreb, dermed forbundne driftsmæssige procedurer samt tilsvarende cybersikkerhedskontroller og verifikationsmekanismer. Da tidshorisonten for hele processen er flere år, bør hvert trin i den bidrage til et højt fælles cybersikkerhedsniveau i sektoren og afbødning af cybersikkerhedsrisici. Alle deltagere i processen bør gøre deres bedste for at udarbejde og nå til enighed om metoderne så hurtigt som muligt uden unødigt ophold og under alle omstændigheder inden fristerne i denne forordning.

([1]) EUT L 158 af 14.6.2019, s. 54.

([2]) 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) (EUT L 333 af 27.12.2022, s. 80).

([3]) Europa-Parlamentets og Rådets forordning (EU) 2019/941 af 5. juni 2019 om risikoberedskab i elsektoren og om ophævelse af direktiv 2005/89/EF (EUT L 158 af 14.6.2019, s. 1).

(6) Cybersikkerhedsrisikovurderingerne på EU-plan, medlemsstatsniveau, regionalt plan og enhedsniveau i denne forordning kan begrænses til dem, der følger af cyberangreb som defineret i Europa-Parlamentets og Rådets forordning (EU) 2022/2554 ([4]), og som derfor ikke omfatter f.eks. fysiske angreb, naturkatastrofer og afbrydelser som følge af tab af faciliteter eller menneskelige ressourcer. Risici på EU-plan og regionale risici i forbindelse med fysiske angreb eller naturkatastrofer på elområdet er allerede omfattet af anden eksisterende EU-lovgivning, herunder artikel 5 i forordning (EU) 2019/941, eller Kommissionens forordning (EU) 2017/1485 ([5]) om fastsættelse af retningslinjer for drift af elektricitetstransmissionssystemer. På samme måde har Europa-Parlamentets og Rådets direktiv (EU) 2022/2557 ([6]) om kritiske enheders modstandsdygtighed til formål at mindske kritiske enheders sårbarheder og styrke deres fysiske modstandsdygtighed og omfatter alle relevante naturlige og menneskeskabte risici, der kan påvirke leveringen af væsentlige tjenester, herunder ulykker, naturkatastrofer, folkesundhedskriser såsom pandemier samt hybride trusler eller andre antagonistiske trusler, herunder terrorhandlinger, kriminel infiltration og sabotage.

(7) Begrebet »enheder med stor indvirkning eller kritisk indvirkning« i denne forordning er afgørende for at afgrænse omfanget af enheder, der er underlagt forpligtelserne i denne forordning. Den risikobaserede tilgang i de forskellige bestemmelser har til formål at udpege de processer, supplerende aktiver og drivende enheder, der påvirker grænseoverskridende elektricitetsstrømme. Afhængigt af graden af indvirkning af eventuelle cyberangreb i disses drift af grænseoverskridende elektricitetsstrømme kan de betragtes som havende »stor indvirkning« eller »kritisk indvirkning«. I artikel 3 i direktiv (EU) 2022/2555 fastsættes begreberne væsentlige og vigtige enheder og kriterierne for at udpege enheder, der tilhører disse kategorier. Selv om mange af dem på samme tid vil blive betragtet og udpeget som »væsentlige« som omhandlet i artikel 3 i direktiv (EU) 2022/2555 og som havende stor indvirkning eller kritisk indvirkning i henhold til denne forordnings artikel 24, henviser kriterierne i denne forordning kun til deres rolle i og indvirkning på de elektricitetsprocesser, der påvirker grænseoverskridende elektricitetsstrømme, uden hensyntagen til kriterierne i artikel 3 i direktiv (EU) 2022/2555.

(8) De enheder inden for denne forordnings anvendelsesområde, som betragtes som havende stor indvirkning eller kritisk indvirkning i henhold til artikel 24 i denne forordning, og som er underlagt bestemmelserne deri, omfatter hovedsagelig enheder, der har direkte indvirkning på grænseoverskridende elektricitetsstrømme i EU.

(9) I denne forordning gøres brug af eksisterende mekanismer og instrumenter fra anden lovgivning for at sikre effektivitet og undgå overlapning i forbindelse med opnåelsen af målene.

(10) Ved anvendelsen af denne forordning bør medlemsstaterne, relevante myndigheder og systemoperatørerne tage hensyn til vedtagne europæiske standarder og tekniske specifikationer fra de europæiske standardiseringsorganisationer og handle i overensstemmelse med EU-lovgivningen med hensyn til omsætning og ibrugtagning af produkter, som er omfattet af den pågældende EU-lovgivning.

([4]) Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og om ændring af forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011 (EUT L 333 af 27.12.2022, s. 1).

([5]) Kommissionens forordning (EU) 2017/1485 af 2. august 2017 om fastsættelse af retningslinjer for drift af elektricitetstransmissionssystemer (EUT L 220 af 25.8.2017, s. 1).

([6]) 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 (EUT L 333 af 27.12.2022, s. 164).

(11) Med henblik på at afbøde cybersikkerhedsrisici, bør der udarbejdes et detaljeret regelsæt for aktiviteter udført af og samarbejdet mellem relevante interessenter, hvis aktiviteter vedrører cybersikkerhedsmæssige aspekter af grænseoverskridende elektricitetsstrømme, for at sikre systemsikkerheden. Disse organisatoriske og tekniske regler bør sikre, at de fleste elektricitetshændelser, hvis grundlæggende årsager er relateret til cybersikkerhed, håndteres effektivt på driftsmæssigt plan. Det er nødvendigt at fastsætte, hvad disse interessenter bør gøre for at forebygge sådanne kriser, og hvilke foranstaltninger de kan træffe, hvis systemdriftsreglerne alene ikke længere er tilstrækkelige. Der bør derfor udarbejdes fælles regler for at forebygge, forberede sig på og håndtere samtidige elkriser, hvis grundlæggende årsager er relateret til cybersikkerhed. Dette skaber større gennemsigtighed i forberedelsesfasen og i samtidige elkriser og sikrer, at der træffes foranstaltninger på en koordineret og effektiv måde sammen med de af medlemsstaternes myndigheder, der er kompetente inden for cybersikkerhed. Medlemsstaterne og de relevante enheder bør forpligtes til i en ånd af solidaritet at samarbejde på regionalt plan og, hvor det er relevant, bilateralt. Dette samarbejde og disse regler har til formål at opnå et bedre og mindre omkostningstungt cybersikkerhedsberedskab i overensstemmelse med målene i direktiv (EU) 2022/2555. Det indre elektricitetsmarked bør ligeledes styrkes ved at øge tilliden i medlemsstaterne, navnlig ved at afbøde risikoen for utidig indskrænkning af grænseoverskridende elektricitetsstrømme og således mindske risikoen for negative afsmittende virkninger for tilgrænsende medlemsstater.

(12) Elforsyningssikkerhed forudsætter effektivt samarbejde mellem medlemsstaterne, Unionens institutioner, organer, kontorer og agenturer og relevante interessenter. Distributionssystemoperatører og transmissionssystemoperatører spiller en central rolle i at sikre et sikkert, pålideligt og effektivt elektricitetssystem i overensstemmelse med artikel 31 og 40 i Europa-Parlamentets og Rådets direktiv (EU) 2019/944 ([7]). De forskellige regulerende myndigheder og andre relevante kompetente nationale myndigheder spiller også en vigtig rolle med hensyn til at sikre og overvåge cybersikkerheden i elforsyningen som led i de opgaver, de er blevet tildelt i henhold til direktiv (EU) 2019/944 og (EU) 2022/2555. Medlemsstaterne bør udpege en eksisterende eller ny enhed som deres kompetente myndighed med henblik på gennemførelsen af denne forordning for at sikre gennemsigtig og inklusiv deltagelse af alle involverede aktører, effektiv forberedelse og korrekt gennemførelse af forordningen, samarbejde mellem de forskellige relevante interessenter og kompetente myndigheder inden for elektricitet og cybersikkerhed samt lette forebyggelsen og den efterfølgende evaluering af elkriser, hvis grundlæggende årsager er relateret til cybersikkerhed, og informationsudveksling i forbindelse hermed.

(13) Hvis en enhed med stor indvirkning eller kritisk indvirkning udbyder tjenester i mere end én medlemsstat eller har hjemsted, andet forretningssted eller en repræsentant i en medlemsstat, og enhedens net- og informationssystemer er beliggende i en anden eller flere andre medlemsstater, bør disse medlemsstater opfordre deres respektive kompetente myndigheder til at gøre deres bedste for at samarbejde med og bistå hinanden efter behov.

(14) Medlemsstaterne bør sikre, at de kompetente myndigheder har de nødvendige beføjelser med hensyn til enheder med stor indvirkning og enheder med kritisk indvirkning, for at fremme overholdelse af denne forordning. Disse beføjelser bør gøre det muligt for de kompetente myndigheder at foretage inspektioner på stedet og tilsyn eksternt. Dette kan omfatte stikprøvekontrol, regelmæssige revisioner, målrettede sikkerhedsrevisioner på grundlag af risikovurderinger eller tilgængelige risikorelaterede oplysninger og sikkerhedsscanninger baseret på objektive, ikkediskriminerende, rimelige og gennemsigtige risikovurderingskriterier, og som omfatter anmodning om oplysninger, der er nødvendige for at vurdere de cybersikkerhedsforanstaltninger, som enheden har truffet. Disse oplysninger bør omfatte dokumenterede cybersikkerhedspolitikker, adgangsdata, dokumenter eller enhver oplysning, som er nødvendig for at udføre tilsynsopgaverne, samt dokumentation for gennemførelse af cybersikkerhedspolitikker såsom resultaterne af sikkerhedsrevisioner udført af en kvalificeret revisor og den respektive underliggende dokumentation.

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

(15) For at undgå huller mellem eller overlapning af de cybersikkerhedsrisikostyringsforpligtelser, som enheder med stor indvirkning eller kritisk indvirkning pålægges, bør nationale myndigheder i henhold til direktiv (EU) 2022/2555 og kompetente myndigheder i henhold til denne forordning samarbejde om gennemførelsen af foranstaltninger til cybersikkerhedsrisikostyring samt tilsynet med overholdelsen af disse foranstaltninger på nationalt plan. En enheds overholdelse af de krav til cybersikkerhedsrisikostyring, som fastsættes i denne forordning, kan af de kompetente myndigheder i henhold til direktiv (EU) 2022/2555 anses for at sikre overholdelse af de tilsvarende krav i nævnte direktiv eller omvendt.

(16) En fælles tilgang til forebyggelse og styring af samtidige elkriser kræver en fælles forståelse blandt medlemsstaterne med hensyn til, hvad der udgør en samtidig elkrise, og hvornår et cyberangreb i den forbindelse er en vigtig faktor. Navnlig bør koordinering mellem medlemsstaterne og relevante enheder lettes med henblik på håndtering af en situation, hvor der som følge af et cyberangreb kan være risiko eller overhængende fare for betydelig elektricitetsmangel, eller for at det er umuligt at levere elektricitet til kunderne.

(17) I betragtning (1) i Europa-Parlamentets og Rådets forordning (EU) 2019/881 ([8]) anerkendes den afgørende rolle, som net- og informationssystemer og elektroniske kommunikationsnet og -tjenester spiller med hensyn til at sørge for, at økonomien fungerer inden for vigtige sektorer, f.eks. energi, mens det i betragtning (44) forklares, at Den Europæiske Unions Agentur for Cybersikkerhed (»ENISA«) bør etablere kontakt med Den Europæiske Unions Agentur for Samarbejde mellem Energireguleringsmyndigheder (»ACER«).

(18) Ved forordning (EU) 2019/943 tildeles transmissionssystemoperatører (»TSO'er«) og distributionssystemoperatører (»DSO'er«) specifikke ansvarsområder med hensyn til cybersikkerhed. Deres europæiske sammenslutninger, nemlig det europæiske netværk af TSO'er for elektricitet (»ENTSO for elektricitet«) og den europæiske enhed for DSO'er (»EU DSO-enhed«) har i henhold til artikel 30 og 55 i nævnte forordning til opgave at fremme cybersikkerheden i samarbejde med relevante myndigheder og regulerede enheder.

(19) En fælles tilgang til forebyggelse og styring af samtidige elkriser, hvis grundlæggende årsager er relateret til cybersikkerhed, kræver også, at relevante interessenter anvender harmoniserede metoder og definitioner til kortlægning af risici, der vedrører cybersikkerheden i forbindelse med elforsyning. Dette kræver også, at det er muligt at foretage en effektiv sammenligning af, hvor godt de og de tilgrænsende interessenter klarer sig på dette område. Det er derfor nødvendigt at fastlægge procedurer, roller og ansvarsområder for udarbejdelse og ajourføring af risikostyringsmetoder, hændelsesklassificeringsskalaer og cybersikkerhedsforanstaltninger, der er tilpasset de cybersikkerhedsrisici, som påvirker de grænseoverskridende elektricitetsstrømme.

(20) Medlemsstaterne er gennem den kompetente myndighed, der er udpeget i henhold til denne forordning, ansvarlige for at udpege de enheder, der opfylder kriterierne for at kunne betragtes som enheder med stor indvirkning eller kritisk indvirkning. For at fjerne forskelle mellem medlemsstaterne i denne henseende og garantere retssikkerhed for så vidt angår foranstaltningerne til cybersikkerhedsrisikostyring og rapporteringsforpligtelserne for alle relevante enheder bør der fastsættes kriterier for, hvilke enheder der er omfattet af denne forordnings anvendelsesområde. Disse kriterier bør defineres og ajourføres regelmæssigt gennem udarbejdelse og vedtagelse af vilkårene, betingelserne og metoderne i denne forordning.

(21) Bestemmelserne i denne forordning bør ikke berøre EU-lovgivning om specifikke regler for certificering af informations- og kommunikationsteknologiske (»IKT«) produkter, tjenester og processer, og bør navnlig ikke berøre forordning (EU) 2019/881 med hensyn til rammen for etablering af europæiske cybersikkerhedscertificeringsordninger. I forbindelse med denne forordning bør IKT-produkter også omfatte teknisk udstyr og software, der gør det muligt at interagere direkte med det elektrotekniske net, navnlig industrielle kontrolsystemer, der kan anvendes til energitransmission, energidistribution og energiproduktion samt indsamling og overførsel af oplysninger. Bestemmelserne bør sikre, at de IKT-produkter, IKT-tjenester og IKT-processer, der skal indkøbes, opfylder de relevante sikkerhedsmål i artikel 51 i forordning (EU) 2019/881.

([8]) Europa-Parlamentets og Rådets forordning (EU) 2019/881 af 17. april 2019 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed), om cybersikkerhedscertificering af informations- og kommunikationsteknologi og om ophævelse af forordning (EU) nr. 526/2013 (forordningen om cybersikkerhed) (EUT L 151 af 7.6.2019, s. 15).

(22) Nylige cyberangreb viser, at enheder i stigende grad bliver mål for angreb på forsyningskæder. Disse angreb på forsyningskæder har ikke kun indvirkning på de enkelte enheder i anvendelsesområdet, men kan også have kaskadevirkninger for større angreb på enheder, som de er forbundet med i elnettet. Der er derfor tilføjet bestemmelser og henstillinger, som har til formål at afbøde cybersikkerhedsrisici i forbindelse med processer, der er knyttet til forsyningskæden, og som påvirker grænseoverskridende elektricitetsstrømme, navnlig udbud.

(23) Da udnyttelsen af sårbarheder i net- og informationssystemer kan forårsage betydelige energiforstyrrelser og være til skade for økonomien og forbrugerne, bør disse sårbarheder hurtigt afdækkes og afhjælpes med henblik på at mindske risiciene. For at lette en effektiv gennemførelse af denne forordning bør relevante enheder og kompetente myndigheder samarbejde om at udføre og afprøve aktiviteter, der anses for at være passende til formålet, herunder udveksling af oplysninger om cybertrusler, cyberangreb, sårbarheder, værktøjer og metoder, taktikker, teknikker og procedurer, beredskab i forbindelse med styring af cybersikkerhedskriser og andre aktiviteter. Da teknologien er under konstant udvikling, og da digitaliseringen af elsektoren sker med hastige skridt, bør gennemførelsen af de vedtagne bestemmelser ikke være til skade for innovationen eller udgøre en hindring for adgangen til elektricitetsmarkedet og den efterfølgende anvendelse af innovative løsninger, som bidrager til et effektivt og bæredygtigt elektricitetssystem.

(24) De oplysninger, der indsamles med henblik på overvågning af gennemførelsen af denne forordning, bør være rimeligt begrænset ud fra need-to-know-princippet. Fristerne for interessenterne til at forelægge disse oplysninger bør være realistiske og effektive. Dobbeltunderretning bør undgås.

(25) Beskyttelse af cybersikkerheden stopper ikke ved Unionens grænser. Et sikkert system kræver inddragelse af tilgrænsende tredjelande. Unionen og dens medlemsstater bør bestræbe sig på at støtte de tilgrænsende tredjelande, hvis elinfrastruktur er tilsluttet det europæiske net, i at anvende tilsvarende cybersikkerhedsregler som fastsat i denne forordning.

(26) ENTSO for elektricitet, EU DSO-enheden og de kompetente myndigheder bør begynde at udarbejde ikkebindende retningslinjer umiddelbart efter denne forordnings ikrafttræden for at forbedre sikkerhedskoordineringen tidligt og afprøve fremtidige bindende vilkår, betingelser og metoder. Disse retningslinjer vil fungere som grundlag for udarbejdelsen af fremtidige vilkår, betingelser og metoder. Parallelt hermed bør de kompetente myndigheder frivilligt udpege enheder som potentielle enheder med stor indvirkning eller kritisk indvirkning for at opfylde forpligtelserne.

(27) Denne forordning er udarbejdet i tæt samarbejde med ACER, ENISA, ENTSO for elektricitet, EU DSO-enheden og andre interessenter med henblik på at vedtage effektive, balancerede og forholdsmæssigt afpassede regler på en gennemsigtig måde, der giver mulighed for medbestemmelse.

(28) Denne forordning supplerer og styrker krisestyringsforanstaltningerne i EU's krisereaktionsramme for cybersikkerhed som fastsat i Kommissionens henstilling (EU) 2017/1584 ([9]). Et cyberangreb kan desuden forårsage, bidrage til eller falde sammen med en elkrise som defineret i artikel 2, nr. 9, i forordning (EU) 2019/941, hvilket vil have en indvirkning på grænseoverskridende elektricitetsstrømme. Denne elkrise kan føre til en samtidig elkrise som defineret i artikel 2, nr. 10), i forordning (EU) 2019/941. En sådan hændelse kan også have indvirkning på andre sektorer, der er afhængige af elforsyningssikkerheden. Hvis en sådan hændelse eskalerer til en omfattende cybersikkerhedshændelse i henhold til artikel 16 i direktiv (EU) 2022/2555, bør bestemmelserne i nævnte artikel om oprettelse af Det Europæiske Netværk af Forbindelsesorganisationer for Cyberkriser (»EU-CyCLONe«) finde anvendelse. Med hensyn til krisestyring på EU-plan bør de relevante parter støtte sig til EU's integrerede ordninger for politisk kriserespons (»IPCR-ordninger«) i henhold til Rådets gennemførelsesafgørelse (EU) 2018/1993 ([10]).

(29) Denne forordning berører ikke medlemsstaternes kompetence til at træffe de nødvendige foranstaltninger for at sikre beskyttelsen af deres væsentlige sikkerhedsinteresser, opretholde den offentlige orden og sikkerhed samt tillade efterforskning, afsløring og retsforfølgelse af strafbare handlinger i overensstemmelse med EU-retten. I henhold til artikel 346 i TEUF er ingen medlemsstat forpligtet til at meddele oplysninger, hvis udbredelse efter dens opfattelse ville stride mod dens væsentlige sikkerhedsinteresser.

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

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

(30) Selv om denne forordning i princippet finder anvendelse på enheder, der beskæftiger sig med produktion af elektricitet fra kernekraftværker, kan nogle af disse aktiviteter være knyttet til den nationale sikkerhed.

(31) EU-retten om databeskyttelse og privatlivets fred bør finde anvendelse på enhver behandling af personoplysninger i henhold til denne forordning. Navnlig berører denne forordning ikke Europa-Parlamentets og Rådets forordning (EU) 2016/679 ([11]), Europa-Parlamentets og Rådets direktiv 2002/58/EF ([12]) og Europa-Parlamentets og Rådets forordning (EU) 2018/1725 ([13]). Denne forordning bør derfor ikke berøre bl.a. de opgaver og beføjelser, som påhviler de myndigheder, der har kompetence til at overvåge overholdelsen af gældende EU-ret om databeskyttelse og om privatlivets fred.

(32) I betragtning af betydningen af internationalt samarbejde om cybersikkerhed bør de kompetente myndigheder, der er ansvarlige for at udføre de opgaver, de pålægges i henhold til denne forordning, og som er udpeget af medlemsstaterne, deltage i internationale samarbejdsnetværk. Med henblik på at udføre deres opgaver bør de kompetente myndigheder derfor kunne udveksle oplysninger, herunder personoplysninger, med tredjelandes kompetente myndigheder, forudsat at betingelserne i henhold til EU's databeskyttelseslovgivning for overførsel af personoplysninger til tredjelande, bl.a. betingelserne i artikel 49 i forordning (EU) 2016/679, er opfyldt.

(33) Behandling af personoplysninger foretaget af enheder med stor indvirkning eller kritisk indvirkning vil i det omfang, det er nødvendigt og står i et rimeligt forhold til målet om at garantere sikkerheden i forbindelse med aktiver, kunne anses for at være lovlig, når en sådan behandling overholder en retlig forpligtelse, som påhviler den dataansvarlige, i overensstemmelse med betingelserne i artikel 6, stk. 1, litra c), og artikel 6, stk. 3, i forordning (EU) 2016/679. Behandling af personoplysninger kan også være nødvendig for, at enheder med stor indvirkning eller kritisk indvirkning samt udbydere af sikkerhedsteknologier og -tjenester, der handler på de nævnte enheders vegne, kan forfølge legitime interesser i henhold til artikel 6, stk. 1, litra f), i forordning (EU) 2016/679, herunder når en sådan behandling er nødvendig for ordninger for deling af cybersikkerhedsrelaterede oplysninger eller frivillig underretning om relevante oplysninger i overensstemmelse med nærværende forordning. Foranstaltninger vedrørende forebyggelse, afsløring, identifikation, inddæmning og analyse af samt reaktion på cyberangreb, foranstaltninger til at øge bevidstheden vedrørende specifikke cybertrusler, udveksling af oplysninger i forbindelse med afhjælpning af sårbarheder og koordineret offentliggørelse af sårbarheder, frivillig udveksling af oplysninger om disse cyberangreb samt cybertrusler og sårbarheder, kompromitteringsindikatorer, taktikker, teknikker og procedurer, cybersikkerhedsadvarsler og konfigurationsværktøjer kan kræve behandling af visse kategorier af personoplysninger såsom IP-adresser, uniform resources locators (URL'er), domænenavne, e-mailadresser og, hvor disse afslører personlige oplysninger, tidsstempler. De kompetente myndigheders, de centrale kontaktpunkters og CSIRT'ernes behandling af personoplysninger kan udgøre en retlig forpligtelse eller anses for at være nødvendig for udførelsen af en opgave i samfundets interesse eller henhørende under offentlig myndighedsudøvelse, som den ansvarlige har fået pålagt, i henhold til artikel 6, stk. 1, litra c) eller e), og artikel 6, stk. 3, i forordning (EU) 2016/679, eller for forfølgelsen af de legitime interesser, som enheder med stor indvirkning eller kritisk indvirkning har, som omhandlet i artikel 6, stk. 1, litra f), i forordning (EU) 2016/679. Desuden kan der i national ret fastsættes regler, der gør det muligt for de kompetente myndigheder, de centrale kontaktpunkter og CSIRT'erne, i det omfang det er nødvendigt og forholdsmæssigt for at garantere sikkerheden i net- og informationssystemer hos enheder med stor indvirkning eller kritisk indvirkning, at behandle særlige kategorier af personoplysninger i overensstemmelse med artikel 9 i forordning (EU) 2016/679, navnlig ved at fastsætte passende og specifikke foranstaltninger til beskyttelse af fysiske personers grundlæggende rettigheder og interesser, herunder tekniske begrænsninger for videreanvendelse af sådanne data og anvendelse af sikkerheds- og privatlivsbevarende foranstaltninger på det aktuelle teknologiske stade såsom pseudonymisering eller kryptering, hvor anonymisering i væsentlig grad kan påvirke det forfulgte formål.

([11]) Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (EUT L 119 af 4.5.2016, s. 1).

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

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

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

(35) Den Europæiske Tilsynsførende for Databeskyttelse er blevet hørt i overensstemmelse med artikel 42, stk. 1, i forordning (EU) 2018/1725 og afgav en udtalelse den 17. november 2023 —

VEDTAGET DENNE FORORDNING:

KAPITEL I

ALMINDELIGE BESTEMMELSER

Artikel 1

Genstand

Ved denne forordning indføres netregler, hvormed der fastsættes sektorspecifikke regler for cybersikkerhedsmæssige aspekter af grænseoverskridende elektricitetsstrømme, herunder regler om fælles minimumskrav, planlægning, overvågning, rapportering og krisestyring.

Artikel 2

Anvendelsesområde

1. Denne forordning finder anvendelse på cybersikkerhedsmæssige aspekter af grænseoverskridende elektricitetsstrømme i følgende enheders aktiviteter, hvis de udpeges som enheder med stor indvirkning eller kritisk indvirkning i overensstemmelse med artikel 24:

a) elektricitetsvirksomheder som defineret i artikel 2, nr. 57), i direktiv (EU) 2019/944

b) udpegede elektricitetsmarkedsoperatører (NEMO'er) som defineret i artikel 2, nr. 8), i forordning (EU) 2019/943

c) organiserede markedspladser eller »organiserede markeder« som defineret i artikel 2, nr. 4), i Kommissionens gennemførelsesforordning (EU) nr. 1348/2014 ([14]), der arrangerer transaktioner med produkter, der er relevante for grænseoverskridende elektricitetsstrømme

d) kritisk IKT-tjenesteudbyder som omhandlet i artikel 3, nr. 9), i denne forordning

e) ENTSO for elektricitet som oprettet i henhold til artikel 28 i forordning (EU) 2019/943

f) EU DSO-enheden som oprettet i henhold til artikel 52 i forordning (EU) 2019/943

g) balanceansvarlige aktører som defineret i artikel 2, nr. 14), i forordning (EU) 2019/943

h) operatører af ladestationer som omhandlet i bilag I til direktiv (EU) 2022/2555

i) regionale koordinationscentre som oprettet i henhold til artikel 35 i forordning (EU) 2019/943

j) udbydere af administrerede sikkerhedstjenester som defineret i artikel 6, nr. 40), i direktiv (EU) 2022/2555

k) enhver anden enhed eller tredjepart, som har fået delegeret eller tildelt ansvar i henhold til denne forordning.

2. Følgende myndigheder er inden for rammerne af deres nuværende mandat ansvarlige for at udføre de opgaver, de pålægges ved denne forordning:

a) Den Europæiske Unions Agentur for Samarbejde mellem Energireguleringsmyndigheder (»ACER«) som oprettet ved Europa-Parlamentets og Rådets forordning (EU) 2019/942 ([15])

b) nationale kompetente myndigheder, der er ansvarlige for at udføre de opgaver, de pålægges i henhold til denne forordning, og som medlemsstaterne har udpeget i henhold til artikel 4, eller »kompetent myndighed«

c) nationale regulerende myndigheder, som hver medlemsstat har udpeget i henhold til artikel 57, stk. 1, i direktiv (EU) 2019/944

([14]) Kommissionens gennemførelsesforordning (EU) nr. 1348/2014 af 17. december 2014 om dataindberetning til gennemførelse af artikel 8, stk. 2, og artikel 8, stk. 6, i Europa-Parlamentets og Rådets forordning (EU) nr. 1227/2011 om integritet og gennemsigtighed på engrosenergimarkederne (EUT L 363 af 18.12.2014, s. 121).

([15]) Europa-Parlamentets og Rådets forordning (EU) 2019/942 af 5. juni 2019 om oprettelse af Den Europæiske Unions Agentur for Samarbejde mellem Energireguleringsmyndigheder (EUT L 158 af 14.6.2019, s. 22).

d) myndigheder, der er kompetente inden for risikoberedskab, og som er udpeget i henhold til artikel 3 i forordning (EU) 2019/941

e) enheder, der håndterer IT-sikkerhedshændelser (»CSIRT'er«), som udpeget eller oprettet i henhold til artikel 10 i direktiv (EU) 2022/2555

f) kompetente myndigheder med ansvar for cybersikkerhed som udpeget eller oprettet i henhold til artikel 8 i direktiv (EU) 2022/2555

g) Den Europæiske Unions Agentur for Cybersikkerhed, som er oprettet i henhold til forordning (EU) 2019/881

h) enhver anden myndighed eller tredjepart, som har fået delegeret eller tildelt ansvar i henhold til artikel 4, stk. 3.

3. Denne forordning finder også anvendelse på alle enheder, som ikke er etableret i Unionen, men som leverer tjenester til enheder i Unionen, forudsat at de er blevet udpeget som enheder med stor indvirkning eller kritisk indvirkning af de kompetente myndigheder i overensstemmelse med artikel 24, stk. 2.

4. Denne forordning berører ikke medlemsstaternes ansvar for at beskytte den nationale sikkerhed eller deres beføjelse til at beskytte andre væsentlige statslige funktioner, herunder sikring af statens territoriale integritet og opretholdelse af lov og orden.

5. Denne forordning berører ikke medlemsstaternes ansvar for at beskytte den nationale sikkerhed med hensyn til aktiviteter vedrørende produktion af elektricitet fra kernekraftværker, herunder aktiviteter inden for den nukleare værdikæde, i overensstemmelse med traktaterne.

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

Artikel 3

Definitioner

I denne forordning forstås ved:

(1) »aktiv«: enhver materiel eller immateriel oplysning, software eller hardware i net- og informationssystemerne, som har værdi for en person, en organisation eller en myndighed

(2) »myndighed, der er kompetent inden for risikoberedskab«: den kompetente myndighed, der er udpeget i henhold til artikel 3 i forordning (EU) 2019/941

(3) »enhed, der håndterer IT-sikkerhedshændelser«: en enhed, der er ansvarlig for håndtering af risici og hændelser i overensstemmelse med artikel 10 i direktiv (EU) 2022/2555

(4) »aktiv med kritisk indvirkning«: et aktiv, der er nødvendigt for at gennemføre en proces med kritisk indvirkning

(5) »enhed med kritisk indvirkning«: en enhed, der gennemfører en proces med kritisk indvirkning, og som er udpeget af de kompetente myndigheder i overensstemmelse med artikel 24

(6) »område med kritisk indvirkning«: et område afgrænset af en enhed som omhandlet i artikel 2, stk. 1, som omfatter alle aktiver med kritisk indvirkning, og hvor adgangen til disse aktiver kan kontrolleres, og som definerer anvendelsesområdet for de udvidede cybersikkerhedskontroller

(7) »proces med kritisk indvirkning«: en forretningsproces, som gennemføres af en enhed, for hvilken indekserne for indvirkning på cybersikkerheden i forbindelse med elektricitetsstrømme overstiger tærsklen for kritisk indvirkning

(8) »tærskel for kritisk indvirkning«: indeksværdierne for indvirkning på cybersikkerheden i forbindelse med elektricitetsstrømme som omhandlet i artikel 19, stk. 3, litra b), over hvilke et cyberangreb på en forretningsproces vil forårsage kritiske forstyrrelser af grænseoverskridende elektricitetsstrømme

(9) »kritisk IKT-tjenesteudbyder«: en enhed, som udbyder en IKT-tjeneste eller IKT-proces, som er nødvendig for en proces med kritisk eller stor indvirkning, der påvirker cybersikkerhedsmæssige aspekter af grænseoverskridende elektricitetsstrømme, og som, hvis den bringes i fare, kan forårsage et cyberangreb med indvirkninger, der overstiger tærsklen for kritisk eller stor indvirkning

(10) »grænseoverskridende elektricitetsstrøm«: en grænseoverskridende strøm som defineret i artikel 2, nr. 3), i forordning (EU) 2019/943

(11) »cyberangreb«: en hændelse som defineret i artikel 3, nr. 14), i forordning (EU) 2022/2554

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

(13) »cybersikkerhedskontrol«: handlinger eller procedurer, der gennemføres med henblik på at undgå, opdage, modvirke eller minimere cybersikkerhedsrisici

(14) »cybersikkerhedshændelse«: en hændelse som defineret i artikel 6, nr. 6), i direktiv (EU) 2022/2555

(15) »cybersikkerhedsstyringssystem«: politikker, procedurer, retningslinjer og tilknyttede ressourcer og aktiviteter, som en enhed forvalter kollektivt med det formål at beskytte sine informationsaktiver mod cybertrusler, og hvormed sikkerheden i en organisations netværks- og informationssystemer systematisk kan etableres, gennemføres, drives, overvåges, gennemgås, vedligeholdes og forbedres

(16) »cybersikkerhedsoperationscenter«: en til formålet indrettet central, hvor et teknisk hold bestående af én eller flere eksperter ved hjælp af IT-systemer til cybersikkerhed udfører sikkerhedsrelaterede opgaver (cybersikkerhedsoperationscentertjenester, »CSOC-tjenester«) såsom håndtering af cyberangreb og sikkerhedskonfigurationsfejl, sikkerhedsovervågning, logfilanalyse og afsløring af cyberangreb

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

(18) »cybersikkerhedsmæssig sårbarhedsstyring«: afdækning og håndtering af sårbarheder

(19) »enhed«: en enhed som defineret i artikel 6, nr. 38), i direktiv (EU) 2022/2555

(20) »tidlig varsling«: de oplysninger, der er nødvendige for at angive, om den væsentlige hændelse formodes at være forårsaget af ulovlige eller ondsindede handlinger, eller om den kan have en grænseoverskridende indvirkning

(21) »indeks for indvirkning på cybersikkerheden i forbindelse med elektricitetsstrømme« (»ECII«): et indeks eller en klassificeringsskala, hvor de mulige konsekvenser af cyberangreb for forretningsprocesser, der indgår i grænseoverskridende elektricitetsstrømme, rangeres

(22) »europæisk cybersikkerhedscertificeringsordning«: en ordning som defineret i artikel 2, nr. 9), i forordning (EU) 2019/881

(23) »enhed med stor indvirkning«: en enhed, der gennemfører en proces med stor indvirkning, og som er udpeget af de kompetente myndigheder i overensstemmelse med artikel 24

(24) »proces med stor indvirkning«: enhver forretningsproces, som gennemføres af en enhed, for hvilken indekserne for indvirkning på cybersikkerheden i forbindelse med elektricitetsstrømme overstiger tærsklen for stor indvirkning

(25) »aktiv med stor indvirkning«: et aktiv, der er nødvendigt for at gennemføre en proces med stor indvirkning

(26) »tærskel for stor indvirkning«: indeksværdierne for indvirkning på cybersikkerheden i forbindelse med elektricitetsstrømme som omhandlet i artikel 19, stk. 3, litra b), over hvilke et vellykket cyberangreb på en proces vil forårsage omfattende forstyrrelser af grænseoverskridende elektricitetsstrømme

(27) »område med stor indvirkning«: et område afgrænset af de i artikel 2, stk. 1, opstillede enheder, som omfatter alle aktiver med stor indvirkning, og hvor adgangen til disse aktiver kan kontrolleres, og som definerer anvendelsesområdet for minimumscybersikkerhedskontrollerne

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

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

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

(31) »legacy-system«: et legacy-IKT-system som defineret i artikel 3, nr. 3), i forordning (EU) 2022/2554

(32) »nationalt centralt kontaktpunkt«: det centrale kontaktpunkt, som hver medlemsstat har udpeget eller oprettet i henhold til artikel 8, stk. 3, i direktiv (EU) 2022/2555

(33) »NIS-cyberkrisestyringsmyndigheder«: de myndigheder, der er udpeget eller oprettet i henhold til artikel 9, stk. 1, i direktiv (EU) 2022/2555

(34) »ophavsmand«: en enhed, som initierer udveksling, deling eller lagring af oplysninger

(35) »udbudsspecifikationer«: de specifikationer, som enheder fastlægger med henblik på indkøb af nye eller ajourførte IKT-produkter, IKT-processer eller IKT-tjenester

(36) »repræsentant«: en fysisk eller juridisk person, der er etableret i Unionen, og som udtrykkeligt er udpeget til at handle på vegne af en enhed med stor indvirkning eller kritisk indvirkning, der ikke er etableret i Unionen, men som leverer tjenester til enheder i Unionen, og som en kompetent myndighed eller en CSIRT kan rette henvendelse til i stedet for selve enheden med stor indvirkning eller kritisk indvirkning for så vidt angår den pågældende enheds forpligtelser i henhold til denne forordning

(37) »risiko«: risiko som defineret i artikel 6, nr. 9), i direktiv (EU) 2022/2555

(38) »risikoindvirkningsmatrix«: en matrix, der anvendes i forbindelse med risikovurdering med henblik på at bestemme risikoindvirkningsniveauet for hver risiko, der vurderes

(39) »samtidig elkrise«: en elkrise som defineret i artikel 2, nr. 10), i forordning (EU) 2019/941

(40) »centralt kontaktpunkt på enhedsniveau«: et centralt kontaktpunkt på enhedsniveau som udpeget i henhold til artikel 38, stk. 1, litra c)

(41) »interessent«: enhver part, som har interesse i den vellykkede og fortsatte drift af en organisation eller proces, såsom medarbejdere, direktører, aktionærer, tilsynsmyndigheder, sammenslutninger, leverandører og kunder

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

(43) »systemdriftsområde«: systemdriftsområder som defineret i bilag I til ACER's afgørelse 05-2022 om afgrænsning af systemdriftsområder, der er fastsat i overensstemmelse med artikel 36 i forordning (EU) 2019/943

(44) »systemoperatører«: »distributionssystemoperatør« (DSO) og »transmissionssystemoperatør« (TSO) som defineret i artikel 2, nr. 29) og 35), i direktiv (EU) 2019/944

(45) »proces med kritisk indvirkning på EU-plan«: enhver proces i elsektoren, som evt. involverer flere enheder, for hvilken den mulige virkning af et cyberangreb kan anses for at være kritisk i cybersikkerhedsrisikovurderingen på EU-plan

(46) »proces med stor indvirkning på EU-plan«: enhver proces i elsektoren, som evt. involverer flere enheder, for hvilken den mulige virkning af et cyberangreb kan anses for at være stor i cybersikkerhedsrisikovurderingen på EU-plan

(47) »aktivt udnyttet sårbarhed, der ikke er blevet afhjulpet«: en sårbarhed, der endnu ikke er blevet offentliggjort og afhjulpet, og hvor der er pålidelig dokumentation for, at en aktør har installeret ondsindet kode på et system uden tilladelse fra systemejeren

(48) »sårbarhed«: sårbarhed som defineret i artikel 6, nr. 15), i direktiv (EU) 2022/2555.

Artikel 4

Kompetent myndighed

1. Hver medlemsstat udpeger hurtigst muligt og under alle omstændigheder senest den **13. december 2024** en national offentlig myndighed på regeringsplan eller en national regulerende myndighed, der er ansvarlig for at udføre de opgaver, den pålægges i denne forordning (»kompetent myndighed«). Indtil den kompetente myndighed er blevet pålagt at udføre opgaverne i denne forordning, udfører den regulerende myndighed, som hver medlemsstat har udpeget i henhold til artikel 57, stk. 1, i direktiv (EU) 2019/944, den kompetente myndigheds opgaver i overensstemmelse med denne forordning.

2. Medlemsstaterne underretter uden ophold Kommissionen, ACER, ENISA, NIS-samarbejdsgruppen som oprettet i henhold til artikel 14 i direktiv (EU) 2022/2555 og Elektricitetskoordinationsgruppen som oprettet i henhold til artikel 1 i Kommissionens afgørelse af 15. november 2012 ([17]) og meddeler dem navn og kontaktoplysninger på deres kompetente myndighed som udpeget i henhold til denne artikels stk. 1 og eventuelle senere ændringer heraf.

([16]) Europa-Parlamentets og Rådets forordning (EU) Nr. 1025/2021 af 25. oktober 2012 om europæisk standardisering, om ændring af Rådets direktiv 89/686/EØF og 93/15/EØF og Europa-Parlamentets og Rådets direktiv 94/9/EF, 94/25/EF, 95/16/EF, 97/23/EF, 98/34/EF, 2004/22/EF, 2007/23/EF, 2009/23/EF og 2009/105/EF og om ophævelse af Rådets beslutning 87/95/EØF og Europa-Parlamentets og Rådets afgørelse nr. 1673/2006/EF (EUT L 316 af 14.11.2012, s. 12).

([17]) Kommissionens afgørelse af 15. november 2012 om oprettelse af Elektricitetskoordinationsgruppen (2012/C 353/02) (EUT C 353 af 17.11.2012, s. 2).

3. Medlemsstaterne kan give deres kompetente myndighed tilladelse til at uddelegere de opgaver, den pålægges i denne forordning, til andre nationale myndigheder med undtagelse af opgaverne i artikel 5. Hver kompetent myndighed overvåger, hvorledes de myndigheder, den har uddelegeret opgaver til, anvender denne forordning. Den kompetente myndighed meddeler navn på de myndigheder, som en opgave er blevet uddelegeret til, deres kontaktoplysninger og pålagte opgaver samt eventuelle senere ændringer heraf til Kommissionen, ACER, Elektricitetskoordinationsgruppen, ENISA og NIS-samarbejdsgruppen.

Artikel 5

Samarbejde mellem relevante myndigheder og organer på nationalt plan

De kompetente myndigheder koordinerer og sikrer et passende samarbejde mellem de kompetente myndigheder med ansvar for cybersikkerhed, cyberkrisestyringsmyndighederne, de nationale regulerende myndigheder, de myndigheder, der er kompetente inden for risikoberedskab, og CSIRT'erne med henblik på opfyldelse af de relevante forpligtelser i denne forordning. De kompetente myndigheder koordinerer også med andre organer eller myndigheder, som hver medlemsstat har udpeget, med henblik på at sikre effektive procedurer og undgå overlapning af opgaver og forpligtelser. De kompetente myndigheder skal kunne instruere de pågældende nationale regulerende myndigheder i at anmode ACER om en udtalelse i henhold til artikel 8, stk. 3.

Artikel 6

Vilkår og betingelser eller metoder samt planer

1. TSO'erne udarbejder i samarbejde med EU DSO-enheden forslag til vilkår og betingelser eller metoder i henhold til stk. 2 eller til planer i henhold til stk. 3.

2. Følgende vilkår og betingelser eller metoder samt ændringer heraf godkendes af alle kompetente myndigheder:

a) metoder til cybersikkerhedsrisikovurdering i henhold til artikel 18, stk. 1

b) den omfattende rapport om cybersikkerhedsrisikovurderingen i forbindelse med grænseoverskridende elektricitetsstrømme i henhold til artikel 23

c) minimumscybersikkerhedskontrollerne og de udvidede cybersikkerhedskontroller i henhold til artikel 29, kortlægning af cybersikkerhedskontroller i forbindelse med elektricitetsstrømme i forhold til standarder i henhold til artikel 34, herunder minimumscybersikkerhedskontroller og udvidede cybersikkerhedskontroller i forsyningskæden i henhold til artikel 33

d) en cybersikkerhedsmæssig henstilling i forbindelse med udbud i henhold til artikel 35

e) metoden til skalaklassificering af cyberangreb i henhold til artikel 37, stk. 8.

3. Forslagene til planer for afbødning af cybersikkerhedsrisici på regionalt plan i henhold til artikel 22 godkendes af alle kompetente myndigheder i det pågældende systemdriftsområde.

4. Forslagene til vilkår og betingelser eller metoder som omhandlet i stk. 2 eller til planer som omhandlet i stk. 3 skal omfatte et forslag til tidsplan for deres gennemførelse og en beskrivelse af deres forventede indvirkning på målene for denne forordning.

5. EU DSO-enheden kan afgive en begrundet udtalelse til de berørte TSO'er indtil tre uger før fristen for forelæggelse af forslaget til vilkår og betingelser eller metoder eller til planer til de kompetente myndigheder. De TSO'er, der er ansvarlige for forslaget til vilkår og betingelser eller metoder eller til planer, tager hensyn til den begrundede udtalelse fra EU DSO-enheden forud for forelæggelsen for de kompetente myndigheder med henblik på deres godkendelse. Hvis der ikke er taget hensyn til EU DSO-enhedens udtalelse, redegør TSO'erne for årsagen hertil.

6. I den fælles udarbejdelse af vilkår, betingelser og metoder eller planer arbejder de deltagende TSO'er tæt sammen. I samråd med ENTSO for elektricitet og i samarbejde med EU DSO-enheden underretter TSO'erne regelmæssigt de kompetente myndigheder og ACER om fremskridtene med at udarbejde vilkår og betingelser eller metoder eller planer.

Artikel 7

Afstemningsregler i TSO'erne

1. Hvis TSO'er, der skal træffe afgørelse om forslag til vilkår og betingelser eller metoder, ikke kan nå til enighed, træffer de afgørelse ved kvalificeret flertal. Et kvalificeret flertal for sådanne forslag opgøres således:

a) TSO'er, der repræsenterer mindst 55 % af medlemsstaterne, og

b) TSO'er, der repræsenterer medlemsstater med tilsammen mindst 65 % af Unionens befolkning.

2. Et blokerende mindretal for så vidt angår afgørelser om forslag til vilkår og betingelser eller metoder som omhandlet i artikel 6, stk. 2, skal omfatte TSO'er, der repræsenterer mindst fire medlemsstater; er der ikke et sådant mindretal, anses det kvalificerede flertal for opnået.

3. Hvis TSO'erne i et systemdriftsområde skal træffe afgørelse om forslag til planer som omhandlet i artikel 6, stk. 2, og ikke kan nå til enighed, og hvis de berørte systemdriftsområder består af mere end fem medlemsstater, træffer TSO'erne afgørelse ved kvalificeret flertal. Et kvalificeret flertal for forslag som omhandlet i artikel 6, stk. 2, kræver følgende flertal:

a) TSO'er, der repræsenterer mindst 72 % af de berørte medlemsstater, og

b) TSO'er, der repræsenterer medlemsstater med tilsammen mindst 65 % af befolkningen i det berørte område.

4. Såfremt der ikke opnås et blokerende mindretal for så vidt angår afgørelser om planerne, som i givet fald skal bestå af mindst et antal TSO'er, der repræsenterer mindst 35 % af befolkningen i de deltagende medlemsstater og mindst én yderligere berørt medlemsstat, anses det kvalificerede flertal for opnået.

5. For så vidt angår TSO-afgørelser om forslag til vilkår og betingelser eller metoder i henhold til artikel stk. 6, stk. 2, tildeles medlemsstaterne én stemme hver. Hvis der er mere end én TSO i en medlemsstat, fordeler medlemsstaten stemmerettighederne mellem TSO'erne.

6. Hvis TSO'erne i samarbejde med EU DSO-enheden ikke forelægger et første forslag eller et ændret forslag til vilkår og betingelser eller metoder eller til planer for de relevante kompetente myndigheder inden fristerne i denne forordning, forelægger de i stedet de relevante udkast til vilkår og betingelser eller metoder eller til planer for de relevante kompetente myndigheder. De redegør for, hvorfor de ikke er nået til enighed. De kompetente myndigheder træffer i fællesskab passende foranstaltninger til vedtagelse af de krævede vilkår og betingelser eller metoder eller planer. Dette kan f.eks. gøres ved at anmode om ændringer af udkastene i henhold til dette stykke, revidere og færdiggøre disse udkast eller, hvis der ikke er forelagt noget udkast, fastlægge og godkende de krævede vilkår og betingelser eller metoder eller planer.

Artikel 8

Forelæggelse af forslag for de kompetente myndigheder

1. TSO'erne forelægger forslagene til vilkår og betingelser eller metoder eller til planer for de relevante myndigheder med henblik på godkendelse inden fristerne i artikel 18, 23, 29, 33, 34, 35 og 37. De kompetente myndigheder kan under særlige omstændigheder i fællesskab forlænge disse frister, navnlig hvis en frist ikke kan overholdes på grund af omstændigheder, der ligger uden for TSO'ernes eller EU DSO-enhedens kontrol.

2. Forslag til vilkår og betingelser eller metoder eller til planer i henhold til stk. 1 forelægges for ACER til orientering, samtidig med at de forelægges for de kompetente myndigheder.

3. Efter fælles anmodning fra de nationale regulerende myndigheder afgiver ACER udtalelse om forslaget til vilkår og betingelser eller metoder eller til planer senest seks måneder efter modtagelsen af forslagene til vilkår og betingelser eller metoder eller til planer og underretter de nationale regulerende myndigheder og de kompetente myndigheder om udtalelsen. De nationale regulerende myndigheder, de kompetente myndigheder med ansvar for cybersikkerhed og alle andre myndigheder, der er udpeget som kompetente myndigheder, koordinerer med hinanden, inden de nationale regulerende myndigheder anmoder ACER om en udtalelse. ACER kan medtage anbefalinger i deres udtalelse. ACER hører ENISA, før det afgiver udtalelse om forslagene, der er omhandlet i artikel 6, stk. 2.

4. De kompetente myndigheder hører hinanden, arbejder tæt sammen og koordinerer med hinanden med henblik på at nå til enighed om de foreslåede vilkår og betingelser, metoder eller planer. Før de godkender vilkårene og betingelserne eller metoderne eller planerne, reviderer og færdiggør de forslagene, hvis det er nødvendigt, efter høring af ENTSO for elektricitet og EU DSO-enheden med henblik på at sikre, at forslagene er i overensstemmelse med denne forordning og bidrager til et højt fælles cybersikkerhedsniveau i hele Unionen.

5. De kompetente myndigheder træffer afgørelse om vilkårene og betingelserne eller metoderne eller om planerne, senest seks måneder efter at den pågældende kompetente myndighed eller, hvis det er relevant, den sidste af de pågældende myndigheder har modtaget vilkårene og betingelserne eller metoderne eller planerne.

6. Hvis ACER afgiver en udtalelse, tager de relevante kompetente myndigheder hensyn til denne udtalelse og træffer deres afgørelser senest seks måneder efter modtagelsen af ACER's udtalelse.

7. Hvis de kompetente myndigheder i fællesskab kræver en ændring af de foreslåede vilkår og betingelser eller metoder eller planer, udarbejder TSO'erne i samarbejde med EU DSO-enheden et forslag til en sådan ændring af vilkårene og betingelserne eller metoderne eller planerne med henblik på godkendelse. TSO'erne forelægger det ændrede forslag til godkendelse senest to måneder efter de kompetente myndigheders anmodning. De kompetente myndigheder træffer afgørelse om de ændrede vilkår og betingelser eller metoder eller planer senest to måneder efter forelæggelsen.

8. Hvis de kompetente myndigheder ikke har kunnet nå til enighed inden fristen i stk. 5 eller 7, meddeler de Kommissionen herom. Kommissionen kan træffe passende foranstaltninger til at gøre det muligt at vedtage de krævede vilkår og betingelser eller metoder eller planer.

9. I samråd med ENTSO for elektricitet offentliggør TSO'erne og EU DSO-enheden vilkårene og betingelserne eller metoderne eller planerne på deres websteder, efter de relevante kompetente myndigheder har godkendt dem, medmindre oplysningerne betragtes som fortrolige i overensstemmelse med artikel 47.

10. De kompetente myndigheder kan i fællesskab anmode TSO'erne og EU DSO-enheden om forslag til ændringer af de godkendte vilkår og betingelser eller metoder eller planer og fastsætte en frist for forelæggelse af disse forslag. TSO'erne kan også på eget initiativ i samarbejde med EU DSO-enheden foreslå ændringer til de kompetente myndigheder. Forslagene til ændring af vilkårene og betingelserne eller metoderne eller af planerne udarbejdes og godkendes i overensstemmelse med proceduren i denne artikel.

11. Mindst hvert tredje år efter den første vedtagelse af de pågældende vilkår og betingelser eller metoder eller de pågældende vedtagne planer vurderer TSO'erne i samarbejde med EU DSO-enheden, hvor effektive de vedtagne vilkår og betingelser eller metoder eller planer er, og underretter uden unødigt ophold de kompetente myndigheder og ACER om resultaterne af gennemgangen.

Artikel 9

Høringer

1. TSO'erne hører med bistand fra ENTSO for elektricitet og i samarbejde med EU DSO-enheden interessenterne, herunder ACER, ENISA og den kompetente myndighed i hver medlemsstat, om udkastene til forslag til vilkår og betingelser eller metoder som omhandlet i artikel 6, stk. 2, eller til planer som omhandlet i artikel 6, stk. 3. Høringen varer mindst én måned.

2. De forslag til vilkår og betingelser eller metoder som omhandlet i artikel 6, stk. 2, som TSO'erne har forelagt i samarbejde med EU DSO-enheden, offentliggøres og sendes til høring på EU-plan. De forslag til planer som omhandlet i artikel 6, stk. 3, som de relevante TSO'er har forelagt i samarbejde med EU DSO-enheden på regionalt plan, offentliggøres og sendes til høring som minimum på regionalt plan.

3. TSO'erne og EU DSO-enheden, som er ansvarlig for forslaget til vilkår og betingelser eller metoder eller til planer, tager med bistand fra ENTSO for elektricitet behørigt hensyn til de synspunkter, som interessenterne fremsætter i forbindelse med de høringer, der gennemføres i henhold til stk. 1, inden forslaget forelægges for myndighederne med henblik på deres godkendelse. I alle tilfælde udarbejdes en velfunderet begrundelse for at tage hensyn til eller undlade at tage hensyn til synspunkter, der blevet fremsat i forbindelse med høringen, og denne vedlægges forslaget og offentliggøres inden for rimelig tid inden eller samtidig med forslaget til vilkår og betingelser eller metoder.

Artikel 10

Inddragelse af interessenter

ACER tilrettelægger i tæt samarbejde med ENTSO for elektricitet og EU DSO-enheden inddragelse af interessenter, herunder regelmæssige møder med interessenterne med henblik på at afdække problemer og foreslå forbedringer i forbindelse med gennemførelsen af denne forordning.

Artikel 11

Dækning af omkostninger

1. De omkostninger, som TSO'er og DSO'er, der er underlagt regulering af nettariffer, bærer, og som følger af de forpligtelser, der er fastsat i denne forordning, herunder de omkostninger, som ENTSO for elektricitet og EU DSO-enheden bærer, vurderes af hver medlemsstats relevante regulerende myndighed.

2. Omkostninger, der vurderes som rimelige, lønsomme og forholdsmæssige, dækkes ved hjælp af nettariffer eller andre passende mekanismer som fastsat af den relevante nationale regulerende myndighed.

3. Hvis de relevante nationale regulerende myndigheder anmoder om det, tilvejebringer TSO'er og DSO'er som omhandlet i stk. 1 inden for en rimelig frist, som fastsættes af den nationale regulerende myndighed, de oplysninger, der er nødvendige for at lette vurderingen af de påløbne omkostninger.

Artikel 12

Overvågning

1. ACER overvåger gennemførelsen af denne forordning i overensstemmelse med artikel 32, stk. 1, i forordning (EU) 2019/943 og artikel 4, stk. 2, i forordning (EU) 2019/942. I forbindelse med denne overvågning kan ACER samarbejde med ENISA og anmode om bistand fra ENTSO for elektricitet og EU DSO-enheden. ACER orienterer regelmæssigt Elektricitetskoordinationsgruppen og NIS-samarbejdsgruppen om gennemførelsen af denne forordning.

2. ACER offentliggør en rapport mindst hvert tredje år efter denne forordnings ikrafttræden med henblik på at

a) gennemgå status for gennemførelsen af de gældende foranstaltninger til cybersikkerhedsrisikostyring med hensyn til enhederne med stor indvirkning og enhederne med kritisk indvirkning

b) afdække, om der er behov for yderligere regler om fælles krav, planlægning, overvågning, rapportering og krisestyring for at forebygge risici i elsektoren og

c) kortlægge områder, hvor der med henblik på revision af denne forordning kan ske forbedringer, eller afdække uopdagede områder og nye prioriteter, der kan opstå som følge af den teknologiske udvikling.

3. Senest den **13. juni 2025** kan ACER i samarbejde med ENISA og efter høring af ENTSO for elektricitet og EU DSO-enheden udstede retningslinjer for de relevante oplysninger, som skal meddeles ACER med henblik på overvågning, samt for proceduren for og hyppigheden af indsamlingen på grundlag af resultatindikatorerne som fastsat i overensstemmelse med stk. 5.

4. De kompetente myndigheder kan få adgang til de relevante oplysninger, som ACER er i besiddelse af og har indsamlet i overensstemmelse med denne artikel.

5. ACER udsteder i samarbejde med ENISA og med støtte fra ENTSO for elektricitet og EU DSO-enheden ikkebindende resultatindikatorer for vurdering af driftsmæssig pålidelighed i forbindelse med cybersikkerhedsmæssige aspekter af grænseoverskridende elektricitetsstrømme.

6. De enheder, der er omhandlet i artikel 2, stk. 1, i denne forordning forelægger ACER de oplysninger, som er nødvendige for, at ACER kan udføre opgaverne i stk. 2.

Artikel 13

Benchmarking

1. Senest den **13. juni 2025** udarbejder ACER i samarbejde med ENISA en ikkebindende vejledning til cybersikkerheds-benchmarking. Formålet med vejledningen er over for de nationale regulerende myndigheder at redegøre for principperne for benchmarking af den cybersikkerhedskontrol, der gennemføres i henhold til denne artikels stk. 2, under hensyntagen til omkostningerne ved at gennemføre kontrollen, og hvor effektive processerne, produkterne, tjenesterne, systemerne og løsningerne er i gennemførelsen af kontrollen. ACER tager hensyn til eksisterende benchmarkingrapporter i udarbejdelsen af den ikkebindende vejledning til cybersikkerhedsbenchmarking. ACER forelægger den ikkebindende vejledning til cybersikkerhedsbenchmarking for de nationale regulerende myndigheder til deres orientering.

2. Senest 12 måneder efter udarbejdelsen af benchmarkingvejledningen i henhold til stk. 1 udfører de nationale regulerende myndigheder en benchmarkinganalyse med henblik på at vurdere, om de nuværende investeringer i cybersikkerhed:

a) afbøder de risici, der har en indvirkning på grænseoverskridende elektricitetsstrømme

b) giver de ønskede resultater og effektivitetsgevinster med hensyn til videreudvikling af elektricitetssystemerne

c) er effektive og indarbejdet i det overordnede indkøb af aktiver og tjenesteydelser.

3. I forbindelse med benchmarkinganalysen kan de nationale regulerende myndigheder tage hensyn til ACER's ikkebindende vejledning til cybersikkerhedsbenchmarking og vurderer navnlig:

a) de gennemsnitlige cybersikkerhedsmæssige omkostninger i forbindelse med afbødning af risici, der har en indvirkning på grænseoverskridende elektricitetsstrømme, navnlig med hensyn til enheder med stor indvirkning og kritisk indvirkning

b) i samarbejde med ENTSO for elektricitet og EU DSO-enheden, de gennemsnitlige priser på cybersikkerhedstjenester, -systemer og -produkter, der i høj grad bidrager til forbedring og vedligeholdelse af foranstaltningerne til cybersikkerhedsrisikostyring i de forskellige systemdriftsområder

c) tilstedeværelsen af cybersikkerhedstjenester, -systemer og -løsninger, der egner sig til gennemførelse af denne forordning, samt graden af sammenligneligheden af deres omkostninger og funktioner, idet der udpeges mulige foranstaltninger, som er nødvendige for at fremme omkostningseffektiviteten, navnlig i tilfælde hvor der er behov for investeringer i cybersikkerhedsteknologi.

4. Enhver oplysning vedrørende benchmarkinganalysen håndteres og behandles i henhold til dataklassificeringskravene i denne forordning, minimumscybersikkerhedskontrollerne og rapporten om cybersikkerhedsrisikovurderingen i forbindelse med grænseoverskridende elektricitetsstrømme. Benchmarkinganalysen i stk. 2 og 3 offentliggøres ikke.

5. Uden at det berører kravene om fortrolighed i artikel 47 og behovet for at beskytte sikkerheden for enheder, der er omfattet af bestemmelserne i denne forordning, deles den benchmarkinganalyse, der er omhandlet i stk. 2 og 3 i denne artikel, med alle nationale regulerende myndigheder, alle kompetente myndigheder, ACER, ENISA og Kommissionen.

Artikel 14

Aftaler med TSO'er uden for Unionen

1. Senest 18 måneder efter denne forordnings ikrafttræden bestræber TSO'er i et systemdriftsområde, der grænser op til et tredjeland, sig på at indgå aftaler med TSO'er i det tilgrænsende tredjeland, der er i overensstemmelse med relevant EU-ret, og som fastlægger grundlaget for samarbejdet om beskyttelse af cybersikkerhed og samarbejdsordningerne for cybersikkerhed med disse TSO'er.

2. TSO'erne underretter den kompetente myndighed om de aftaler, der er indgået i henhold til stk. 1.

Artikel 15

Retlige repræsentanter

1. Enheder, der ikke er etableret i Unionen, men som leverer tjenester til enheder i Unionen, og som er underrettet om, at de er blevet udpeget som enheder med stor indvirkning eller kritisk indvirkning i overensstemmelse med artikel 24, stk. 6, udpeger skriftligt og senest tre måneder efter underretningen en repræsentant i Unionen og meddeler den underrettende kompetente myndighed herom.

2. Repræsentanten har mandat til at blive kontaktet af en kompetent myndighed eller CSIRT i Unionen ud over eller i stedet for enheden med stor indvirkning eller kritisk indvirkning med henblik på enhedens forpligtelser i henhold til denne forordning. Enheden med stor indvirkning eller kritisk indvirkning giver sin retlige repræsentant de nødvendige beføjelser og tilstrækkelige ressourcer til at sikre, at denne kan arbejde effektivt og rettidigt sammen med de relevante kompetente myndigheder eller CSIRT'er.

3. Repræsentanten skal være etableret i en af de medlemsstater, hvor enheden udbyder sine tjenester. Enheden anses for at høre under jurisdiktionen i den medlemsstat, hvor repræsentanten er etableret. Enheder med stor indvirkning eller kritisk indvirkning meddeler navn, postadresse, e-mailadresse og telefonnummer på deres retlige repræsentant til den kompetente myndighed i den medlemsstat, hvor den retlige repræsentant er bosiddende eller etableret.

4. Den udpegede retlige repræsentant skal kunne drages til ansvar for manglende overholdelse af forpligtelserne i henhold til denne forordning, uden at det berører det ansvar, som selve enheden med stor indvirkning eller kritisk indvirkning har, eller de retlige skridt, der vil kunne indledes over for denne.

5. Hvis der ikke findes en repræsentant i Unionen, der er udpeget i henhold til denne artikel, kan enhver medlemsstat, hvor enheden udbyder tjenester, tage retlige skridt mod enheden for manglende overholdelse af forpligtelserne i henhold til denne forordning.

6. Udpegningen af en retlig repræsentant i Unionen i henhold til stk. 1 udgør ikke en etablering i Unionen.

Artikel 16

Samarbejde mellem ENTSO for elektricitet og EU DSO-enheden

1. ENTSO for elektricitet og EU DSO-enheden samarbejder om at udføre cybersikkerhedsrisikovurderinger i henhold til artikel 19 og artikel 21, navnlig i forbindelse med følgende opgaver:

a) udarbejdelse af metoder til cybersikkerhedsrisikovurdering i henhold til artikel 18, stk. 1

b) udarbejdelse af den omfattende rapport om cybersikkerhedsrisikovurderingen i forbindelse med grænseoverskridende elektricitetsstrømme i henhold til artikel 23

c) udarbejdelse af den fælles ramme for cybersikkerhed i forbindelse med elektricitetsstrømme i henhold til kapitel III

d) udarbejdelse af den cybersikkerhedsmæssige henstilling i forbindelse med udbud i henhold til artikel 35

e) udarbejdelse af metoden til skalaklassificering af cyberangreb i henhold til artikel 37, stk. 8

f) udarbejdelse af det foreløbige indeks for indvirkning på cybersikkerheden i forbindelse med elektricitetsstrømme (»ECII«) i henhold til artikel 48, stk. 1, litra a)

g) udarbejdelse af den konsoliderede foreløbige liste over enheder med stor indvirkning og kritisk indvirkning i henhold til artikel 48, stk. 3

h) udarbejdelse af den foreløbige liste over processer med stor indvirkning og kritisk indvirkning på EU-plan i henhold til artikel 48, stk. 4

i) udarbejdelse af den foreløbige liste over europæiske og internationale standarder og kontroller i henhold til artikel 48, stk. 6

j) udførelse af cybersikkerhedsrisikovurderingen på EU-plan i henhold til artikel 19

k) udførelse af cybersikkerhedsrisikovurderingerne på regionalt plan i henhold til artikel 21

l) udarbejdelse af planerne for afbødning af cybersikkerhedsrisici på regionalt plan i henhold til artikel 22

m) udarbejdelse af vejledning om anvendelse af europæiske cybersikkerhedscertificeringsordninger i forbindelse med IKT-produkter, IKT-tjenester og IKT-processer i overensstemmelse med artikel 36

n) udarbejdelse af retningslinjer for gennemførelsen af denne forordning i samråd med ACER og ENISA.

2. Samarbejdet mellem ENTSO for elektricitet og EU DSO-enheden kan tage form af en arbejdsgruppe vedrørende cybersikkerhedsrisici.

3. ENTSO for elektricitet og EU DSO-enheden orienterer regelmæssigt ACER, ENISA, NIS-samarbejdsgruppen og Elektricitetskoordinationsgruppen om fremskridtene med hensyn til gennemførelsen af cybersikkerhedsrisikovurderingen på EU-plan og cybersikkerhedsrisikovurderingerne på regionalt plan i henhold til artikel 19 og artikel 21.

Artikel 17

Samarbejde mellem ACER og de kompetente myndigheder

ACER overvåger i samarbejde med hver kompetent myndighed følgende:

(1) gennemførelsen af foranstaltninger til cybersikkerhedsrisikostyring i henhold til artikel 12, stk. 2, litra a), samt rapporteringsforpligtelser i henhold til artikel 27 og artikel 39 og

(2) vedtagelsesproceduren og gennemførelsen af vilkår og betingelser og metoder eller planer i henhold til artikel 6, stk. 2 og 3. Samarbejdet mellem ACER, ENISA og hver kompetent myndighed kan tage form af et organ til overvågning af cybersikkerhedsrisici.

KAPITEL II

RISIKOVURDERING OG KORTLÆGNING AF DE RELEVANTE CYBERSIKKERHEDSRISICI

Artikel 18

Metoder til cybersikkerhedsrisikovurdering

1. Senest den **13. marts 2025** forelægger TSO'erne med bistand fra ENTSO for elektricitet, i samarbejde med EU DSO-enheden og efter høring af NIS-samarbejdsgruppen et forslag til metoder til cybersikkerhedsrisikovurdering på EU-plan, på regionalt plan og på medlemsstatsniveau.

2. Metoderne til cybersikkerhedsrisikovurdering på EU-plan, regionalt plan og medlemsstatsplan skal omfatte:

a) en liste over cybertrusler, der skal tages i betragtning, herunder som minimum følgende trusler mod forsyningskæden:

   i) en omfattende og uventet korruption i forsyningskæden

   ii) manglende adgang til IKT-produkter, IKT-tjenester eller IKT-processer i forsyningskæden

iii) cyberangreb, som er indledt af aktører i forsyningskæden

iv) lækage af følsomme oplysninger i forsyningskæden, herunder sporing i forsyningskæden

v) svagheder og bagdøre i IKT-produkter, IKT-tjenester eller IKT-processer, som er indsat af aktører i forsyningskæden

b) kriterierne for at vurdere indvirkningen af cybersikkerhedsrisici som værende stor eller kritisk ved hjælp af fastlagte tærskler for konsekvenser og sandsynlighed

c) en tilgang til analyse af de cybersikkerhedsrisici, der hidrører fra legacy-systemer, kaskadevirkningerne af cyberangreb og realtidselementet af de systemer, som anvendes til drift af nettet

d) en tilgang til analyse af de cybersikkerhedsrisici, der følger af afhængigheden af en enkelt leverandør af IKT-produkter, IKT-tjenester eller IKT-processer.

3. Med metoderne til cybersikkerhedsrisikovurdering på EU-plan, regionalt plan og medlemsstatsplan vurderes cybersikkerhedsrisiciene ved hjælp af den samme risikoindvirkningsmatrix. Formålet med risikoindvirkningsmatrixen er at:

a) måle konsekvenserne af cyberangreb på grundlag af følgende kriterier:

i) belastningstab

ii) reduktion af elektricitetsproduktionen

iii) kapacitetstab i den primære frekvensreserve

iv) tab af kapacitet til at genoprette driften af et elnet uafhængigt af det eksterne transmissionsnet efter en fuldstændig eller delvis nedlukning (»evne til start fra dødt net«)

v) den forventede varighed af en afbrydelse af elforsyningen, som påvirker kunderne, kombineret med afbrydelsens omfang opgjort i antal berørte kunder, og

vi) andre kvantitative eller kvalitative kriterier, der med rimelighed kan fungere som en indikator for et cyberangrebs indvirkning på grænseoverskridende elektricitetsstrømme

b) måle sandsynligheden for en hændelse som hyppigheden af cyberangreb pr. år

4. Metoderne til cybersikkerhedsrisikovurdering på EU-plan skal omfatte beskrivelse af, hvordan ECII-værdierne for tærsklerne for stor indvirkning og kritisk indvirkning fastlægges. ECII gør det muligt for enhederne ved hjælp af kriterierne i stk. 2, litra b), at vurdere indvirkningen af risiciene på deres forretningsproces i forbindelse med de konsekvensanalyser, de udfører i henhold til artikel 26, stk. 4, litra c), nr. i).

5. ENTSO for elektricitet orienterer i samarbejde med EU DSO-enheden Elektricitetskoordinationsgruppen om de forslag til metoder til cybersikkerhedsrisikovurdering, som udarbejdes i henhold til stk. 1.

Artikel 19

Cybersikkerhedsrisikovurdering på EU-plan

1. Senest ni måneder efter godkendelsen af metoderne til cybersikkerhedsrisikovurdering i henhold til artikel 8 og hvert tredje år derefter udfører ENTSO for elektricitet i samarbejde med EU DSO-enheden og i samråd med NIS-samarbejdsgruppen, uden at det berører artikel 22 i direktiv (EU) 2022/2555, en cybersikkerhedsrisikovurdering på EU-plan og udarbejder et udkast til rapport om cybersikkerhedsrisikovurderingen på EU-plan. I den forbindelse anvender de de metoder, der er udarbejdet i henhold til artikel 18 og godkendt i henhold til artikel 8, med henblik på at afdække, analysere og vurdere eventuelle konsekvenser af cyberangreb, der påvirker elektricitetssystemets driftssikkerhed og forstyrrer grænseoverskridende elektricitetsstrømme. I cybersikkerhedsrisikovurderingen på EU-plan tages retlig, finansiel eller omdømmemæssig skade som følge af cyberangreb ikke i betragtning.

2. Rapporten om cybersikkerhedsrisikovurderingen på EU-plan skal indeholde følgende elementer:

a) processerne med stor indvirkning på EU-plan og processerne med kritisk indvirkning på EU-plan

b) en risikoindvirkningsmatrix, som enhederne og de kompetente myndigheder skal benytte til at vurdere den cybersikkerhedsrisiko, der er konstateret i cybersikkerhedsrisikovurderingen på medlemsstatsniveau i henhold til artikel 20 og i cybersikkerhedsrisikovurderingen på enhedsniveau i henhold til artikel 26, stk. 2, litra b).

3. Med hensyn til processerne med stor indvirkning på EU-plan og processerne med kritisk indvirkning på EU-plan skal rapporten om cybersikkerhedsrisikovurderingen på EU-plan indeholde:

a) en vurdering af mulige konsekvenser af et cyberangreb ved hjælp af parametrene i den metode til cybersikkerhedsrisikovurdering, der er udarbejdet i henhold til artikel 18, stk. 2, 3, og 4, og som er godkendt i henhold til artikel 8

b) det ECII og de tærskler for stor indvirkning og kritisk indvirkning, som den kompetente myndighed skal anvende i henhold til artikel 24, stk. 1, og 2, med henblik på at udpege enheder med stor indvirkning eller kritisk indvirkning, som er involverede i processer med stor indvirkning på EU-plan og processer med kritisk indvirkning på EU-plan.

4. ENTSO for elektricitet forelægger i samarbejde med EU DSO-enheden udkastet til rapport om cybersikkerhedsrisikovurderingen med resultaterne af cybersikkerhedsrisikovurderingen på EU-plan for ACER med henblik på en udtalelse. ACER afgiver en udtalelse om udkastet til rapporten senest tre måneder efter modtagelsen heraf. ENTSO for elektricitet og EU DSO-enheden tager størst muligt hensyn til ACER's udtalelse i færdiggørelsen af rapporten.

5. Senest tre måneder efter modtagelsen af ACER's udtalelse formidler ENTSO for elektricitet i samarbejde med EU DSO-enheden den endelige rapport om cybersikkerhedsrisikovurderingen på EU-plan til Kommissionen, ENISA og de kompetente myndigheder.

Artikel 20

Cybersikkerhedsrisikovurdering på medlemsstatsniveau

1. Hver kompetent myndighed foretager en cybersikkerhedsrisikovurdering på medlemsstatsniveau af alle enheder med stor indvirkning og kritisk indvirkning i den pågældende medlemsstat ved hjælp af de metoder, der er udarbejdet i henhold til artikel 18 og godkendt i henhold til artikel 8. I cybersikkerhedsrisikovurderingen på medlemsstatsniveau kortlægges og analyseres de risici for cyberangreb, der påvirker elektricitetssystemets driftssikkerhed og forstyrrer grænseoverskridende elektricitetsstrømme. I cybersikkerhedsrisikovurderingen på medlemsstatsniveau tages retlig, finansiel eller omdømmemæssig skade som følge af cyberangreb ikke i betragtning.

2. Senest 21 måneder efter underretningen af enhederne med stor indvirkning og kritisk indvirkning i henhold til artikel 24, stk. 6, og hvert tredje år efter denne dato, og efter høring af den kompetente myndighed med ansvar for cybersikkerhed, der har ansvaret for elektricitet, forelægger hver kompetent myndighed med støtte fra CSIRT'en en rapport om cybersikkerhedsrisikovurderingen på medlemsstatsniveau for ENTSO for elektricitet og EU DSO-enheden med følgende oplysninger for hver forretningsproces med stor indvirkning og kritisk indvirkning:

a) status for gennemførelsen af minimumscybersikkerhedskontrol og udvidet cybersikkerhedskontrol, jf. artikel 29

b) en liste over alle cyberangreb, der er indberettet i de foregående tre år, jf. artikel 38, stk. 3

c) en sammenfatning af de oplysninger om cybertrusler, der er indberettet i de foregående tre år, jf. artikel 38, stk. 6

d) for hver proces med stor indvirkning eller kritisk indvirkning på EU-plan et skøn over risiciene ved kompromittering af fortroligheden, integriteten og tilgængeligheden af oplysninger og relevante aktiver

e) om nødvendigt en liste over yderligere enheder, der er udpeget som enheder med stor indvirkning eller kritisk indvirkning i henhold til artikel 24, stk. 1, 2, 3 og 5.

3. I rapporten om cybersikkerhedsrisikovurderingen på medlemsstatsniveau tages der hensyn til medlemsstatens risikoberedskabsplan, der er udarbejdet i henhold til artikel 10 i forordning (EU) 2019/941.

4. Oplysningerne i rapporten om cybersikkerhedsrisikovurderingen på medlemsstatsniveau i henhold til stk. 2, litra a)-d), må ikke være knyttet til specifikke enheder eller aktiver. Rapporten om cybersikkerhedsrisikovurderingen på medlemsstatsniveau skal også indeholde en risikovurdering af de midlertidige undtagelser, der er indrømmet af de kompetente myndigheder i medlemsstaterne i henhold til artikel 30.

5. ENTSO for elektricitet og EU DSO-enheden kan anmode de kompetente myndigheder om yderligere oplysninger i forbindelse med de opgaver, der er nævnt i stk. 2, litra a) og c).

6. De kompetente myndigheder sørger for, at de oplysninger, de giver, er nøjagtige og korrekte.

Artikel 21

Cybersikkerhedsrisikovurdering på regionalt plan

1. ENTSO for elektricitet foretager i samarbejde med EU DSO-enheden og i samråd med det relevante regionale koordinationscenter en regional cybersikkerhedsrisikovurdering for hvert systemdriftsområde ved hjælp af de metoder, der er udarbejdet i henhold til artikel 19 og godkendt i henhold til artikel 8, for at kortlægge, analysere og vurdere risiciene for cyberangreb, der påvirker elektricitetssystemets driftssikkerhed og forstyrrer grænseoverskridende elektricitetsstrømme. I cybersikkerhedsrisikovurderingerne på regionalt plan tages retlig, finansiel eller omdømmemæssig skade som følge af cyberangreb ikke i betragtning.

2. Senest 30 måneder efter underretningen af enhederne med stor indvirkning og kritisk indvirkning i henhold til artikel 24, stk. 6, og hvert tredje år herefter udarbejder ENTSO for elektricitet i samarbejde med EU DSO-enheden og i samråd med NIS-samarbejdsgruppen en rapport om cybersikkerhedsrisikovurderingen på regionalt plan for hvert systemdriftsområde.

3. I rapporten om cybersikkerhedsrisikovurderingen på regionalt plan tages der hensyn til de relevante oplysninger i rapporterne om cybersikkerhedsrisikovurderingen på EU-plan og i rapporterne om cybersikkerhedsrisikovurderingen på medlemsstatsniveau.

4. I den regionale cybersikkerhedsrisikovurdering tages de i henhold til artikel 6 i forordning (EU) 2019/941 opstillede regionale elkrisescenarier, der vedrører cybersikkerhed, i betragtning.

Artikel 22

Planer for afbødning af cybersikkerhedsrisici på regionalt plan

1. Senest 36 måneder efter underretningen af enhederne med stor indvirkning og kritisk indvirkning i henhold til artikel 24, stk. 6, og senest den **13. juni 2031** samt hvert tredje år efter denne dato udarbejder TSO'erne med bistand fra ENTSO for elektricitet, i samarbejde med EU DSO-enheden og i samråd med de regionale koordinationscentre og NIS-samarbejdsgruppen en regional plan for afbødning af cybersikkerhedsrisici for hvert systemdriftsområde.

2. Planerne for afbødning af cybersikkerhedsrisici på regionalt plan skal omfatte:

a) de minimumscybersikkerhedskontroller og udvidede cybersikkerhedskontroller, som enheder med stor indvirkning og kritisk indvirkning skal anvende i systemdriftsområdet

b) de resterende cybersikkerhedsrisici i systemdriftsområderne efter anvendelse af de kontroller, der er omhandlet i litra a).

3. ENTSO for elektricitet forelægger planerne for afbødning af risici på regionalt plan for de relevante transmissionssystemoperatører, de kompetente myndigheder og Elektricitetskoordinationsgruppen. Elektricitetskoordinationsgruppen kan anbefale ændringer.

4. TSO'erne ajourfører med bistand fra ENTSO for elektricitet, i samarbejde med EU DSO-enheden og i samråd med NIS-samarbejdsgruppen planerne for afbødning af risici på nationalt plan hvert tredje år, medmindre omstændighederne berettiger hyppigere ajourføringer.

Artikel 23

Omfattende rapport om cybersikkerhedsrisikovurderingen i forbindelse med grænseoverskridende elektricitetsstrømme

1. Senest 40 måneder efter underretningen af enhederne med stor indvirkning og kritisk indvirkning i henhold til artikel 24, stk. 6, og hvert tredje år herefter forelægger TSO'erne med bistand fra ENTSO for elektricitet, i samarbejde med EU DSO-enheden og i samråd med NIS-samarbejdsgruppen en rapport om resultatet af vurderingen af cybersikkerhedsrisici i forbindelse med grænseoverskridende elektricitetsstrømme (»den omfattende rapport om cybersikkerhedsrisikovurderingen i forbindelse med grænseoverskridende elektricitetsstrømme«).

2. Den omfattende rapport om cybersikkerhedsrisikovurderingen i forbindelse med grænseoverskridende elektricitetsstrømme baseres på rapporten om cybersikkerhedsrisikovurderingen på EU-plan, rapporterne om cybersikkerhedsrisikovurderingen på medlemsstatsniveau og rapporterne om cybersikkerhedsrisikovurderingen på regionalt plan og skal indeholde følgende oplysninger:

a) listen over processer med stor indvirkning og kritisk indvirkning på EU-plan, der er udpeget i rapporten om cybersikkerhedsrisikovurderingen på EU-plan i overensstemmelse med artikel 19, stk. 2, litra a), herunder vurderingen af sandsynligheden for og indvirkningen af cybersikkerhedsrisici, der er vurderet i forbindelse med rapporterne om cybersikkerhedsrisikovurderingen på regionalt plan i henhold til artikel 21, stk. 2, og artikel 19, stk. 3, litra a)

b) aktuelle cybertrusler, med særligt fokus på nye trusler og risici, som elektricitetssystemet er udsat for

c) cyberangreb i den foregående periode på EU-plan, med et kritisk overblik over, hvordan disse cyberangreb kan have påvirket grænseoverskridende elektricitetsstrømme

d) den overordnede status for gennemførelsen af cybersikkerhedsforanstaltningerne

e) status for gennemførelsen af informationsstrømmene, jf. artikel 37 og 38

f) en liste over oplysninger eller specifikke kriterier for klassificering af oplysninger i overensstemmelse med artikel 46

g) konstaterede og fremhævede risici, der kan opstå som følge af usikker styring af forsyningskæder

h) resultater af og akkumulerede erfaringer fra regionale og tværregionale cybersikkerhedsøvelser, der er tilrettelagt i henhold til artikel 44

i) en analyse af udviklingen af de overordnede grænseoverskridende cybersikkerhedsrisici i elsektoren siden de seneste regionale cybersikkerhedsrisikovurderinger

j) alle andre oplysninger, der kan være nyttige med henblik på mulige forbedringer af denne forordning eller behovet for en revision af denne forordning eller dens værktøjer, og

k) aggregerede og anonymiserede oplysninger om undtagelser, der er indrømmet i henhold til artikel 30, stk. 3.

3. De i artikel 2, stk. 1, opførte enheder kan bidrage til udarbejdelsen af den omfattende rapport om cybersikkerhedsrisikovurderingen i forbindelse med grænseoverskridende elektricitetsstrømme under overholdelse af fortroligheden af oplysninger i overensstemmelse med artikel 47. TSO'erne hører med bistand fra ENTSO for elektricitet og i samarbejde med EU DSO-enheden disse enheder på et tidligt tidspunkt.

4. Den omfattende rapport om cybersikkerhedsrisikovurderingen i forbindelse med grænseoverskridende elektricitetsstrømme er omfattet af reglerne om beskyttelse af udveksling af oplysninger i henhold til artikel 46. Uden at det berører artikel 10, stk. 4, og artikel 47, stk. 4, offentliggør ENTSO for elektricitet og EU DSO-enheden en offentlig udgave af rapporten, som ikke må indeholde oplysninger, der kan være til skade for enheder, der er opført i artikel 2, stk. 1. Den offentlige udgave af rapporten offentliggøres kun efter aftale med NIS-samarbejdsgruppen og Elektricitetskoordinationsgruppen. ENTSO for elektricitet er i samarbejde med EU DSO-enheden ansvarlig for sammenfatningen og offentliggørelsen af den offentlige udgave af rapporten.

Artikel 24

Udpegelse af enheder med stor indvirkning og kritisk indvirkning

1. Hver kompetent myndighed udpeger ved hjælp af ECII og tærsklerne for stor indvirkning og kritisk indvirkning i rapporten om cybersikkerhedsrisikovurderingen på EU-plan, jf. artikel 19, stk. 3, litra b), enheder med stor indvirkning og kritisk indvirkning i sin medlemsstat, som er involverede i processer med stor indvirkning og kritisk indvirkning på EU-plan. De kompetente myndigheder kan anmode en enhed i deres medlemsstat om oplysninger med henblik på at fastlægge ECII-værdierne for den pågældende enhed. Hvis det fastlagte ECII for en enhed ligger over tærsklen for stor indvirkning eller kritisk indvirkning, opføres den udpegede enhed i rapporten om cybersikkerhedsrisikovurderingen på medlemsstatsniveau, jf. artikel 20, stk. 2.

2. Hver kompetent myndighed udpeger ved hjælp af ECII og tærsklerne for stor indvirkning og kritisk indvirkning i rapporten om cybersikkerhedsrisikovurderingen på EU-plan, jf. artikel 19, stk. 3, litra b), enheder med stor indvirkning og kritisk indvirkning, som ikke er etablerede i Unionen, for så vidt som de er aktive i Unionen. Den kompetente myndighed kan anmode en enhed, der ikke er etableret i Unionen, om oplysninger med henblik på at fastlægge ECII-værdierne for den pågældende enhed.

3. Hver kompetent myndighed kan udpege yderligere enheder i sin medlemsstat som enheder med stor indvirkning eller kritisk indvirkning, hvis følgende kriterier er opfyldt:

a) enheden er en del af en gruppe af enheder, som er i betydelig risiko for at blive berørt på samme tid i tilfælde af et cyberangreb

b) det aggregerede ECII for gruppen af enheder ligger over tærsklen for stor indvirkning eller kritisk indvirkning.

4. Hvis en kompetent myndighed udpeger yderligere enheder i overensstemmelse med stk. 3, anses alle processer i disse enheder, for hvilke det aggregerede ECII for gruppen ligger over tærsklen for stor indvirkning, for at være processer med stor indvirkning, og alle processer i disse enheder, for hvilke det aggregerede ECII for gruppen ligger over tærsklerne for kritisk indvirkning, anses for at være processer med kritisk indvirkning.

5. Hvis en kompetent myndighed udpeger enheder som omhandlet i stk. 3, litra a), i mere end én medlemsstat, underretter den de øvrige kompetente myndigheder, ENTSO for elektricitet og EU DSO-enheden herom. På grundlag af de modtagne oplysninger fra alle kompetente myndigheder forelægger ENTSO for elektricitet i samarbejde med EU DSO-enheden de kompetente myndigheder en analyse af de aggregeringer af enheder i mere end én medlemsstat, som kan forårsage en afbrydelse fra flere steder af de grænseoverskridende elektricitetsstrømme og resultere i et cyberangreb. Hvis en gruppe af enheder i flere medlemsstater udpeges som en aggregering, for hvilken ECII ligger over tærsklen for stor indvirkning eller kritisk indvirkning, udpeger alle berørte kompetente myndigheder enhederne i gruppen som enheder med stor indvirkning eller kritisk indvirkning for deres respektive medlemsstat på grundlag af det aggregerede ECII for gruppen af enheder, og de udpegede enheder opføres i rapporten om cybersikkerhedsrisikovurderingen på EU-plan.

6. Hver kompetent myndighed underretter senest ni måneder efter at være blevet underrettet af ENTSO for elektricitet og EU DSO-enheden om rapporten om cybersikkerhedsrisikovurderingen på EU-plan i henhold til artikel 19, stk. 5, og under alle omstændigheder senest den **13. juni 2028** enhederne på listen om, at de er blevet udpeget som en enhed med stor indvirkning eller kritisk indvirkning i den pågældende medlemsstat.

7. Når en tjenesteudbyder rapporteres til en kompetent myndighed som værende en kritisk IKT-tjenesteudbyder i henhold til artikel 27, litra c), underretter den kompetente myndighed de kompetente myndigheder i de medlemsstater, på hvis område hjemstedet eller repræsentanten er beliggende, herom. Sidstnævnte kompetente myndighed underretter tjenesteudbyderen om, at denne er blevet udpeget som kritisk tjenesteudbyder.

Artikel 25

Nationale kontrolordninger

1. De kompetente myndigheder kan indføre en national kontrolordning for at verificere, at enheder med kritisk indvirkning, der er udpeget i henhold til artikel 24, stk. 1, har gennemført de nationale love, der indgår i den kortlægningsmatrix, der er omhandlet i artikel 34. Den nationale kontrolordning kan baseres på en inspektion udført af den kompetente myndighed, uafhængige sikkerhedsrevisioner eller gensidige peerevalueringer foretaget af enheder med kritisk indvirkning i samme medlemsstat under tilsyn af den kompetente myndighed.

2. Hvis en kompetent myndighed beslutter at indføre en national kontrolordning, sikrer den kompetente myndighed, at kontrollen udføres i overensstemmelse med følgende krav:

a) enhver part, der foretager peerevalueringen, revisionen eller inspektionen, skal være uafhængig af den enhed med kritisk indvirkning, der er genstand for kontrollen, og må ikke have interessekonflikter

b) det personale, der foretager peerevalueringen, revisionen eller inspektionen, skal have påviselig viden om:

   i) cybersikkerhed i elsektoren

   ii) cybersikkerhedsstyringssystemer

   iii) principperne for revision

   iv) cybersikkerhedsrisikovurdering

   v) den fælles ramme for cybersikkerhed i forbindelse med elektricitetsstrømme

   vi) de nationale love og administrative bestemmelser og de europæiske og internationale standarder, der er omfattet af kontrollen

   vii) de processer med kritisk indvirkning, der er omfattet af kontrollen

c) den part, der foretager peerevalueringen, revisionen eller inspektionen, skal have tilstrækkelig tid til at udføre disse aktiviteter

d) den part, der foretager peerevalueringen, revisionen eller inspektionen, skal træffe passende foranstaltninger til at beskytte de oplysninger, der indsamles under kontrollen, efter deres fortrolighedsgrad og

e) peerevalueringer, revisioner eller inspektioner skal gennemføres mindst én gang om året og skal mindst hvert tredje år omfatte den fulde rækkevidde af kontrollen.

3. Hvis en kompetent myndighed beslutter at indføre en national kontrolordning, aflægger den årligt rapport til ACER om, hvor ofte den har foretaget inspektioner under den pågældende ordning.

Artikel 26

Cybersikkerhedsrisikostyring på enhedsniveau

1. Hver enhed med stor indvirkning eller kritisk indvirkning som udpeget af de kompetente myndigheder i henhold til artikel 24, stk. 1, foretager cybersikkerhedsrisikostyring for alle sine aktiver i sine områder med stor indvirkning og kritisk indvirkning. Hver enhed med stor indvirkning eller kritisk indvirkning gennemfører hvert tredje år en risikostyring, der omfatter faserne i stk. 2.

2. Hver enhed med stor indvirkning eller kritisk indvirkning baserer sin cybersikkerhedsrisikostyring på en tilgang, der har til formål at beskytte deres net- og informationssystemer, og som består af følgende faser:

a) bestemmelse af kontekst

b) vurdering af cybersikkerhedsrisici på enhedsniveau

c) behandling af cybersikkerhedsrisici

d) accept af cybersikkerhedsrisici.

3. I fasen med bestemmelse af kontekst fastsætter hver enhed med stor indvirkning eller kritisk indvirkning:

a) omfanget af cybersikkerhedsrisikovurderingen, herunder de processer med stor indvirkning og kritisk indvirkning, som ENTSO for elektricitet og EU DSO-enheden har udpeget, og andre processer, der kan være mål for cyberangreb med stor indvirkning eller kritisk indvirkning på grænseoverskridende elektricitetsstrømme, og

b) kriterierne for risikovurdering og risikoaccept i overensstemmelse med den risikoindvirkningsmatrix, som enhederne og de kompetente myndigheder skal benytte til at vurdere cybersikkerhedsrisiciene i de metoder til cybersikkerhedsrisikovurdering på EU-plan, regionalt plan og på medlemsstatsniveau, der er udarbejdet af ENTSO for elektricitet og EU DSO-enheden, jf. artikel 19, stk. 2.

4. I fasen med vurdering af cybersikkerhedsrisici gør hver enhed med stor indvirkning eller kritisk indvirkning følgende:

a) kortlægger cybersikkerhedsrisici ved at tage følgende i betragtning:

   i) alle aktiver, der understøtter processer med stor indvirkning eller kritisk indvirkning på EU-plan, med en vurdering af den mulige indvirkning på grænseoverskridende elektricitetsstrømme, i tilfælde af at aktivet bringes i fare

   ii) mulige cybertrusler under hensyntagen til de cybertrusler, der er konstateret i den seneste omfattende rapport om cybersikkerhedsrisikovurderingen i forbindelse med grænseoverskridende elektricitetsstrømme, jf. artikel 23, og trusler mod forsyningskæder

   iii) sårbarheder, herunder sårbarheder i legacy-systemer

   iv) mulige cyberangrebsscenarier, herunder cyberangreb, der påvirker elektricitetssystemets driftssikkerhed og forstyrrer grænseoverskridende elektricitetsstrømme

   v) relevante risikovurderinger og vurderinger, der er foretaget på EU-plan, herunder koordinerede risikovurderinger af kritiske forsyningskæder i henhold til artikel 22 i direktiv (EU) 2022/2555, og

   vi) eksisterende gennemførte kontroller.

b) analyserer sandsynligheden for og konsekvenserne af de cybersikkerhedsrisici, der er konstateret efter litra a), og fastlægger cybersikkerhedsrisikoniveauet ved hjælp af den risikoindvirkningsmatrix, som anvendes til at vurdere cybersikkerhedsrisici i metoderne til cybersikkerhedsrisikovurdering på EU-plan, regionalt plan og på medlemsstatsniveau, og som er udarbejdet af TSO'erne med bistand fra ENTSO for elektricitet og i samarbejde med EU DSO-enheden, jf. artikel 19, stk. 2

c) klassificerer aktiver efter de mulige konsekvenser i tilfælde af, at cybersikkerheden bringes i fare, og afgrænser området med stor indvirkning og kritisk indvirkning ved hjælp af følgende trin:

   i) udførelse af en konsekvensanalyse ved hjælp af ECII for alle processer, der er omfattet af cybersikkerhedsrisikovurderingen

   ii) klassificering af processer som processer med stor indvirkning eller kritisk indvirkning, hvis ECII for processen ligger over tærsklen for henholdsvis stor indvirkning eller kritisk indvirkning

   iii) bestemmelse af alle aktiver med stor indvirkning og kritisk indvirkning som de aktiver, der er nødvendige for processerne med henholdsvis stor indvirkning og kritisk indvirkning

   iv) afgrænsning af områder med stor indvirkning og kritisk indvirkning, som omfatter alle aktiver med henholdsvis stor indvirkning og kritisk indvirkning, så adgangen til områderne kan kontrolleres

d) vurderer cybersikkerhedsrisici ved at prioritere dem ud fra de kriterier for risikovurdering og risikoaccept, der er omhandlet i stk. 3, litra b).

5. I fasen med behandling af cybersikkerhedsrisici udarbejder hver enhed med stor indvirkning eller kritisk indvirkning en risikoafbødningsplan på enhedsniveau ved at udvælge de muligheder for risikobehandling, der er egnede til at styre risiciene og afdække residualrisici.

6. I fasen med accept af cybersikkerhedsrisici beslutter hver enhed med stor indvirkning eller kritisk indvirkning, om residualrisikoen skal accepteres på grundlag af de kriterier for risikoaccept, der er omhandlet i stk. 3, litra b).

7. Hver enhed med stor indvirkning eller kritisk indvirkning registrerer de aktiver, der er omhandlet i stk. 1, i en fortegnelse over aktiver. Denne fortegnelse over aktiver indgår ikke i risikovurderingsrapporten.

8. Den kompetente myndighed kan undersøge aktiverne i fortegnelsen i forbindelse med inspektioner.

Artikel 27

Rapportering om risikovurdering på enhedsniveau

Hver enhed med stor indvirkning eller kritisk indvirkning forelægger senest 12 måneder efter underretningen af enhederne med stor indvirkning og kritisk indvirkning i henhold til artikel 24, stk. 6, og hvert tredje år herefter den kompetente myndighed en rapport med følgende oplysninger:

(1) en liste over de kontroller, der er udvalgt til risikoafbødningsplanen på enhedsniveau i henhold til artikel 26, stk. 5, med den aktuelle gennemførelsesstatus for hver kontrol

(2) for hver proces med stor indvirkning eller kritisk indvirkning på EU-plan et skøn over risiciene ved kompromittering af fortroligheden, integriteten og tilgængeligheden af oplysninger og relevante aktiver. Skønnet over denne risiko gives i overensstemmelse med den risikoindvirkningsmatrix, der er omhandlet i artikel 19, stk. 2

(3) en liste over kritiske IKT-tjenesteudbydere for deres processer med kritisk indvirkning.

KAPITEL III

FÆLLES RAMME FOR CYBERSIKKERHED I FORBINDELSE MED ELEKTRICITETSSTRØMME

Artikel 28

Sammensætning, funktion og revision af den fælles ramme for cybersikkerhed i forbindelse med elektricitetsstrømme

1. Den fælles ramme for cybersikkerhed i forbindelse med elektricitetsstrømme består af følgende kontroller og cybersikkerhedsstyringssystem:

a) minimumscybersikkerhedskontroller udviklet i overensstemmelse med artikel 29

b) udvidede cybersikkerhedskontroller udviklet i overensstemmelse med artikel 29

c) den i overensstemmelse med artikel 34 udarbejdede kortlægningsmatrix, hvori de i litra a) og b) omhandlede kontroller kortlægges i forhold til udvalgte europæiske og internationale standarder og nationale love og administrative bestemmelser

d) det cybersikkerhedsstyringssystem, der er indført i henhold til artikel 32.

2. Alle enheder med stor indvirkning anvender de minimumscybersikkerhedskontroller, der er nævnt stk. 1, litra a), inden for deres område med stor indvirkning.

3. Alle enheder med kritisk indvirkning anvender de udvidede cybersikkerhedskontroller, der er nævnt stk. 1, litra b), inden for deres område med kritisk indvirkning.

4. Senest syv måneder efter forelæggelsen af det første udkast til rapport om cybersikkerhedsrisikovurderingen på EU-plan i henhold til artikel 19, stk. 4, suppleres den fælles ramme for cybersikkerhed i forbindelse med elektricitetsstrømme, der er omhandlet i stk. 1, med de minimumscybersikkerhedskontroller og udvidede cybersikkerhedskontroller i forsyningskæden, der er udviklet i henhold til artikel 33.

Artikel 29

Minimumscybersikkerhedskontrol og udvidet cybersikkerhedskontrol

1. Senest syv måneder efter forelæggelsen af det første udkast til rapport om cybersikkerhedsrisikovurderingen på EU-plan i henhold til artikel 19, stk. 4, udarbejder TSO'erne med bistand fra ENTSO for elektricitet og i samarbejde med EU DSO-enheden et forslag til minimumscybersikkerhedskontrol og udvidet cybersikkerhedskontrol.

2. Senest 6 måneder efter udarbejdelsen af hver rapport om cybersikkerhedsrisikovurderingen på regionalt plan i henhold til artikel 21, stk. 2, foreslår TSO'erne med bistand fra ENTSO for elektricitet og i samarbejde med EU DSO-enheden de kompetente myndigheder ændringer af minimumscybersikkerhedskontrollerne og de udvidede cybersikkerhedskontroller. Forslaget stilles i overensstemmelse med artikel 8, stk. 10, og der tages hensyn til de risici, der er konstateret i den regionale risikovurdering.

3. Minimumscybersikkerhedskontrollerne og de udvidede cybersikkerhedskontroller skal kunne verificeres ved at være omfattet af en national kontrolordning i overensstemmelse med proceduren i artikel 31 eller ved at blive underkastet uafhængige sikkerhedsrevisioner, der udføres af tredjepart i overensstemmelse med kravene i artikel 25, stk. 2.

4. I de første minimumscybersikkerhedskontroller og udvidede cybersikkerhedskontroller, der udvikles efter stk. 1, tages der udgangspunkt i de risici, der er konstateret i rapporten om cybersikkerhedsrisikovurderingen på EU-plan, jf. artikel 19, stk. 5. I de ændrede minimumscybersikkerhedskontroller og udvidede cybersikkerhedskontroller, der udvikles efter stk. 2, tages der udgangspunkt rapporten om cybersikkerhedsrisikovurderingen på regionalt plan, jf. artikel 21, stk. 2.

5. Minimumscybersikkerhedskontrollen omfatter kontroller til beskyttelse af oplysninger, der udveksles i overensstemmelse med artikel 46.

6. Senest 12 måneder efter godkendelsen af minimumscybersikkerhedskontrollerne og de udvidede cybersikkerhedskontroller i overensstemmelse med artikel 8, stk. 5, eller efter hver opdatering i overensstemmelse med artikel 8, stk. 10, anvender de enheder, der er opført i artikel 2, stk. 1, og som er udpeget som enheder med kritisk indvirkning eller stor indvirkning i henhold til artikel 24, i udarbejdelsen af risikoafbødningsplanen på enhedsniveau i henhold til artikel 26, stk. 5, minimumscybersikkerhedskontrollerne inden for området med stor indvirkning og de udvidede cybersikkerhedskontroller inden for området med kritisk indvirkning.

Artikel 30

Undtagelser fra minimumscybersikkerhedskontrollen og den udvidede cybersikkerhedskontrol

1. De i artikel 2, stk. 1, opførte enheder kan anmode den respektive kompetente myndighed om at indrømme en undtagelse fra deres forpligtelse til at anvende de minimumscybersikkerhedskontroller og udvidede cybersikkerhedskontroller, der er omhandlet i artikel 29, stk. 6. Den kompetente myndighed kan indrømme en sådan undtagelse af en af følgende grunde:

a) under ekstraordinære omstændigheder, hvor enheden kan påvise, at omkostningerne ved at gennemføre de relevante cybersikkerhedskontroller i væsentlig grad overstiger fordelene. ACER og ENTSO for elektricitet i samarbejde med DSO-enheden kan i fællesskab udarbejde en vejledning til vurdering af omkostningerne ved cybersikkerhedskontrollerne for at hjælpe enhederne

b) enheden fremlægger en risikobehandlingsplan på enhedsniveau, der afbøder cybersikkerhedsrisiciene ved hjælp af alternative kontroller til et niveau, der er acceptabelt i overensstemmelse med de kriterier for risikoaccept, der er omhandlet i artikel 26, stk. 3, litra b).

2. Senest tre måneder efter modtagelsen af anmodningen i stk. 1 træffer hver kompetent myndighed afgørelse om, hvorvidt der skal indrømmes en undtagelse fra minimumscybersikkerhedskontrollen og den udvidede cybersikkerhedskontrol. Der indrømmes undtagelser fra minimumscybersikkerhedskontrollen eller den udvidede cybersikkerhedskontrol for en periode på højst tre år med mulighed for forlængelse.

3. For indrømmede undtagelser bør der medtages aggregerede og anonymiserede oplysninger som et bilag til den omfattende rapport om cybersikkerhedsrisikovurderingen i forbindelse med grænseoverskridende elektricitetsstrømme i artikel 23. ENTSO for elektricitet og EU DSO-enheden ajourfører i fællesskab listen, hvis det er nødvendigt.

Artikel 31

Kontrol af den fælles ramme for cybersikkerhed i forbindelse med elektricitetsstrømme

1. Senest 24 måneder efter vedtagelsen af de kontroller, der er omhandlet i artikel 28, stk. 1, litra a), b) og c), og indførelsen af det cybersikkerhedsstyringssystem, der er omhandlet i nævnte artikels litra d), skal hver enhed med kritisk indvirkning, der er udpeget i henhold til artikel 24, stk. 1, efter anmodning fra den kompetente myndighed kunne påvise efterlevelse af cybersikkerhedsstyringssystemet og minimumscybersikkerhedskontrollen eller den udvidede cybersikkerhedskontrol.

2. Hver enhed med kritisk indvirkning opfylder forpligtelsen i stk. 1 ved at underkaste sig uafhængige sikkerhedsrevisioner, der udføres af tredjepart i overensstemmelse med kravene i artikel 25, stk. 2, eller ved at være omfattet af en national kontrolordning i overensstemmelse med artikel 25, stk. 1.

3. Kontrollen af, om en enhed med kritisk indvirkning efterlever cybersikkerhedsstyringssystemet og minimumscybersikkerhedskontrollen eller den udvidede cybersikkerhedskontrol, omfatter alle aktiver inden for enheden med kritisk indvirknings område med kritisk indvirkning.

4. Kontrollen af, om en enhed med kritisk indvirkning efterlever cybersikkerhedsstyringssystemet og minimumscybersikkerhedskontrollen eller den udvidede cybersikkerhedskontrol, gentages med regelmæssige mellemrum, senest 36 måneder efter afslutningen af den første kontrol og hvert tredje år herefter.

5. Hver enhed med kritisk indvirkning, der er udpeget i henhold til artikel 24, påviser sin efterlevelse af de kontroller, der er omhandlet i artikel 28, stk. 1, litra a), b) og c), og indførelsen af et cybersikkerhedsstyringssystem som omhandlet i nævnte artikels litra d) ved at aflægge rapport om resultatet af overensstemmelseskontrollen til den kompetente myndighed.

Artikel 32

Cybersikkerhedsstyringssystem

1. Hver enhed med stor indvirkning eller kritisk indvirkning indfører et cybersikkerhedsstyringssystem senest 24 måneder efter at være blevet underrettet af den kompetente myndighed om udpegelsen som enhed med stor indvirkning eller kritisk indvirkning i henhold til artikel 24, stk. 6, og reviderer systemet hvert tredje år herefter med henblik på at:

a) fastsætte omfanget af cybersikkerhedsstyringssystemet under hensyntagen til grænseflader og afhængigheder af andre enheder

b) sikre, at hele enhedens øverste ledelse er informeret om relevante retlige forpligtelser og aktivt bidrager til at gennemføre cybersikkerhedsstyringssystemet gennem rettidige beslutninger og hurtige reaktioner

c) sikre, at de nødvendige ressourcer til cybersikkerhedsstyringssystemet er til rådighed

d) udarbejde en cybersikkerhedspolitik, der dokumenteres og formidles inden for enheden og til parter, der er berørt af sikkerhedsrisiciene

e) tildele og formidle ansvar for roller, der er relevante med henblik på cybersikkerhed

f) varetage cybersikkerhedsrisikostyring på enhedsniveau som fastsat i artikel 26

g) fastlægge, hvilke ressourcer der er nødvendige for at gennemføre, vedligeholde og løbende forbedre cybersikkerhedsstyringssystemet, og tilvejebringe disse, under hensyntagen til den nødvendige kompetence inden for og bevidsthed om cybersikkerhedsressourcer

h) fastlægge, hvilken intern og ekstern kommunikation der er relevant i forbindelse med cybersikkerhed

i) oprette, ajourføre og kontrollere dokumenterede oplysninger vedrørende cybersikkerhedsstyringssystemet

j) vurdere cybersikkerhedsstyringssystemets ydeevne og effektivitet

k) gennemføre interne revisioner med planlagte mellemrum for at sikre, at cybersikkerhedsstyringssystemet er gennemført og vedligeholdes på effektiv vis

l) revidere gennemførelsen af cybersikkerhedsstyringssystemet med planlagte mellemrum og kontrollere og korrigere ressourcernes og aktiviteternes manglende overensstemmelse med politikker, procedurer og retningslinjer i cybersikkerhedsstyringssystemet.

2. Anvendelsesområdet for cybersikkerhedsstyringssystemet omfatter alle aktiver inden for området med stor indvirkning og kritisk indvirkning for enheden med stor indvirkning eller kritisk indvirkning.

3. De kompetente myndigheder tilskynder, uden at påtvinge eller forskelsbehandle til fordel for brug af en bestemt type teknologi, til anvendelse af europæiske eller internationale standarder og specifikationer, der vedrører styringssystemer og er relevante for sikkerheden i net- og informationssystemer.

Artikel 33

Minimumscybersikkerhedskontrol og udvidet cybersikkerhedskontrol i forsyningskæden

1. Senest syv måneder efter forelæggelsen af det første udkast til rapport om cybersikkerhedsrisikovurderingen på EU-plan i henhold til artikel 19, stk. 4, udarbejder TSO'erne med bistand fra ENTSO for elektricitet og i samarbejde med EU DSO-enheden et forslag til minimumscybersikkerhedskontrol og udvidet cybersikkerhedskontrol i forsyningskæden, som afbøder de risici i forsyningskæden, der er konstateret i cybersikkerhedsrisikovurderinngerne på EU-plan, og supplerer den minimumscybersikkerhedskontrol og udvidede cybersikkerhedskontrol, der er udviklet i henhold til artikel 29. Minimumscybersikkerhedskontrollen og den udvidede cybersikkerhedskontrol i forsyningskæden udvikles sammen med minimumscybersikkerhedskontrollen og den udvidede cybersikkerhedskontrol i artikel 29. Minimumscybersikkerheds-kontrollen og den udvidede cybersikkerhedskontrol i forsyningskæden omfatter hele livscyklussen for alle IKT-produkter, IKT-tjenester og IKT-processer inden for området med stor indvirkning eller kritisk indvirkning for en enhed med stor indvirkning eller kritisk indvirkning. NIS-samarbejdsgruppen høres i forbindelse med udarbejdelsen af forslaget om minimumscybersikkerhedskontrol og udvidet cybersikkerhedskontrol i forsyningskæden.

2. Minimumscybersikkerhedskontrollen i forsyningskæden består af kontroller for enheder med stor indvirkning eller kritisk indvirkning, som:

a) omfatter henstillinger om indkøb af IKT-produkter, IKT-tjenester og IKT-processer, som indeholder henvisninger til cybersikkerhedsspecifikationer og som minimum omfatter:

   i) baggrundstjek af personalet hos den leverandør, der er involveret i forsyningskæden, og som beskæftiger sig med følsomme oplysninger eller med adgang til enhedens aktiver med stor indvirkning eller kritisk indvirkning. Baggrundstjekket kan omfatte kontrol af en enheds personales eller kontrahenters identitet og baggrund i overensstemmelse med national ret og nationale procedurer samt relevant og gældende EU-ret, herunder forordning (EU) 2016/679 og Europa-Parlamentets og Rådets direktiv (EU) 2016/680 ([18]). Baggrundstjek skal være forholdsmæssige og strengt begrænsede til, hvad der er nødvendigt. De foretages udelukkende med henblik på at vurdere en potentiel sikkerhedsrisiko, som den berørte enhed er udsat for. De skal stå i et rimeligt forhold til de forretningsmæssige krav, klassificeringen af de oplysninger, der skal tilgås, og de opfattede risici og kan udføres af enheden selv, af en ekstern virksomhed, der foretager en screening, eller gennem en statslig clearing

   ii) procedurer for sikker og kontrolleret udformning, udvikling og produktion af IKT-produkter, IKT-tjenester og IKT-processer, fremme af udformning og udvikling af IKT-produkter, IKT-tjenester og IKT-processer, herunder passende tekniske foranstaltninger til cybersikkerhed

   iii) udformning af net- og informationssystemer, hvor der ikke er tillid til enheder, selv når de befinder sig inden for et sikkert område og kræver verifikation af alle modtagne anmodninger, og princippet om minimumsrettigheder anvendes

   iv) leverandørens adgang til enhedens aktiver

([18]) Europa-Parlamentets og Rådets direktiv (EU) 2016/680 af 27. april 2016 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 (EUT L 119 af 4.5.2016, s. 89).

v) leverandørens kontraktlige forpligtelser til at beskytte og begrænse adgangen til enhedens følsomme oplysninger

vi) de grundlæggende cybersikkerhedsmæssige udbudsspecifikationer ved tildeling af kontrakter til leverandørens underleverandører

vii) sporbarheden af anvendelsen af cybersikkerhedsspecifikationerne fra udvikling og produktion til levering af IKT-produkter, IKT-tjenester og IKT-processer

viii) støtte til sikkerhedsopdateringer i hele levetiden for IKT-produkter, IKT-tjenester og IKT-processer

ix) retten til at revidere cybersikkerheden i leverandørens udformnings-, udviklings- og produktionsprocesser og

x) en vurdering af leverandørens risikoprofil

b) kræver, at enhederne tager hensyn til de henstillinger i forbindelse med udbud, der er omhandlet i litra a), når de indgår kontrakter med leverandører, samarbejdspartnere og andre parter i forsyningskæden, hvilket omfatter almindelig levering af IKT-produkter, IKT-tjenester og IKT-processer samt uplanlagte begivenheder og omstændigheder såsom opsigelse eller overførsel af kontrakter i tilfælde af forsømmelighed fra kontraktpartnerens side

c) kræver, at enhederne tager hensyn til resultaterne af de relevante koordinerede sikkerhedsrisikovurderinger af kritiske forsyningskæder, der er foretaget i henhold til artikel 22, stk. 1, i direktiv (EU) 2022/2555

d) omfatter kriterier for udvælgelse af og indgåelse af kontrakter med leverandører, der kan opfylde de i litra a) omhandlede cybersikkerhedsspecifikationer og har et cybersikkerhedsniveau, der modsvarer cybersikkerhedsrisiciene ved det IKT-produkt, den IKT-tjeneste eller de IKT-processer, som leverandøren leverer

e) omfatter kriterier for diversificering af forsyningskilderne for IKT-produkter, IKT-tjenester og IKT-processer og mindskning af risikoen for leverandørfastlåsning

f) omfatter kriterier for regelmæssig overvågning, gennemgang eller revision af cybersikkerhedsspecifikationerne for leverandørens interne driftsprocesser i hele livscyklussen for hvert IKT-produkt, hver IKT-tjeneste og hver IKT-proces.

3. Hvad angår cybersikkerhedsspecifikationerne i den i stk. 2, litra a), omhandlede cybersikkerhedsmæssige henstilling i forbindelse med udbud anvender enheder med stor indvirkning eller kritisk indvirkning i overensstemmelse med artikel 35, stk. 4, udbudsprincipperne i henhold til Europa-Parlamentets og Rådets direktiv 2014/24/EU ([19]) eller fastsætter deres egne specifikationer på grundlag af resultaterne af cybersikkerhedsrisikovurderingen på enhedsniveau.

4. Den udvidede cybersikkerhedskontrol i forsyningskæden omfatter kontroller for enheder med kritisk indvirkning for i forbindelse med indkøb at verificere, at IKT-produkter, IKT-tjenester og IKT-processer, der vil blive anvendt som aktiver med kritisk indvirkning, lever op til cybersikkerhedsspecifikationerne. IKT-produktet, IKT-tjenesten eller IKT-processen kontrolleres enten gennem en europæisk cybersikkerhedscertificeringsordning, jf. artikel 31, eller gennem kontrolaktiviteter, der er udvalgt og tilrettelagt af enheden. Kontrolaktiviteternes dybde og omfang skal være tilstrækkelige til at give sikkerhed for, at IKT-produktet, IKT-tjenesten eller IKT-processen kan anvendes til at afbøde de risici, der er konstateret i risikovurderingen på enhedsniveau. Enheden med kritisk indvirkning dokumenterer de skridt, der er taget for at begrænse de konstaterede risici.

5. Minimumscybersikkerhedskontrollen og den udvidede cybersikkerhedskontrol i forsyningskæden finder anvendelse på indkøb af relevante IKT-produkter, IKT-tjenester og IKT-processer. Minimumscybersikkerhedskontrollen og den udvidede cybersikkerhedskontrol i forsyningskæden finder anvendelse på udbudsprocedurer i enheder, der er udpeget som enheder med kritisk indvirkning eller stor indvirkning i henhold til artikel 24, som begynder seks måneder efter vedtagelsen eller opdateringen af de i artikel 29 omhandlede minimumscybersikkerhedskontroller og udvidede cybersikkerhedskontroller.

([19]) Europa-Parlamentets og Rådets direktiv 2014/24/EU af 26. februar 2014 om offentlige udbud og om ophævelse af direktiv 2004/18/EF (EUT L 94 af 28.3.2014, s. 65).

6. Senest seks måneder efter udarbejdelsen af hver rapport om cybersikkerhedsrisikovurderingen på regionalt plan i henhold til artikel 21, stk. 2, foreslår TSO'erne med bistand fra ENTSO for elektricitet og i samarbejde med EU DSO-enheden de kompetente myndigheder ændringer af minimumscybersikkerhedskontrollerne og de udvidede cybersikkerhedskontroller i forsyningskæden. Forslaget stilles i overensstemmelse med artikel 8, stk. 10, og der tages hensyn til de risici, der er konstateret i den regionale risikovurdering.

Artikel 34

Matrix til kortlægning af cybersikkerhedskontroller i forbindelse med elektricitetsstrømme i forhold til standarder

1. Senest syv måneder efter forelæggelsen af det første udkast til rapport om cybersikkerhedsrisikovurderingen på EU-plan i henhold til artikel 19, stk. 4, udarbejder TSO'erne med bistand fra ENTSO for elektricitet, i samarbejde med EU DSO-enheden og i samråd med ENISA et forslag til en matrix til kortlægning af de kontroller, der er omhandlet i artikel 28, stk. 1, litra a) og b), i forhold til udvalgte europæiske og internationale standarder samt relevante tekniske specifikationer (»kortlægningsmatrixen«). ENTSO for elektricitet og EU DSO-enheden dokumenterer ækvivalensen mellem de forskellige kontroller og de kontroller, der er omhandlet i artikel 28, stk. 1, litra a) og b).

2. De kompetente myndigheder kan forelægge ENTSO for elektricitet og EU DSO-enheden en kortlægning af de kontroller, der er omhandlet i artikel 28, stk. 1, litra a) og b), med en henvisning til de relaterede nationale love og administrative bestemmelser, herunder medlemsstaternes relevante nationale standarder, jf. artikel 25 i direktiv (EU) 2022/2555. Hvis en medlemsstats kompetente myndighed foretager en sådan kortlægning, indarbejder ENTSO for elektricitet og EU DSO-enheden denne nationale kortlægning i kortlægningsmatrixen.

3. Senest seks måneder efter udarbejdelsen af hver rapport om cybersikkerhedsrisikovurderingen på regionalt plan i henhold til artikel 21, stk. 2, foreslår TSO'erne med bistand fra ENTSO for elektricitet, i samarbejde med EU DSO-enheden og i samråd med ENISA de kompetente myndigheder ændringer af kortlægningsmatrixen. Forslaget stilles i overensstemmelse med artikel 8, stk. 10, og der tages hensyn til de risici, der er konstateret i den regionale risikovurdering.

KAPITEL IV

CYBERSIKKERHEDSMÆSSIGE HENSTILLINGER I FORBINDELSE MED UDBUD

Artikel 35

Cybersikkerhedsmæssige henstillinger i forbindelse med udbud

1. TSO'erne udarbejder med bistand fra ENTSO for elektricitet og i samarbejde med EU DSO-enheden i et arbejdsprogram, der skal fastlægges og ajourføres, hver gang der vedtages en rapport om cybersikkerhedsrisikovurderingen på regionalt plan, en række ikkebindende cybersikkerhedsmæssige henstillinger i forbindelse med udbud, som enheder med stor indvirkning eller kritisk indvirkning kan anvende som grundlag for indkøb af IKT-produkter, IKT-tjenester og IKT-processer i områderne med stor indvirkning og kritisk indvirkning. Arbejdsprogrammet skal omfatte følgende:

a) en beskrivelse og klassificering af de typer IKT-produkter, IKT-tjenester og IKT-processer, der anvendes af enheder med stor indvirkning og kritisk indvirkning i området med stor indvirkning og kritisk indvirkning

b) en liste over, for hvilke typer IKT-produkter, IKT-tjenester og IKT-processer der skal udarbejdes et sæt ikkebindende cybersikkerhedsmæssige henstillinger på grundlag af de relevante rapporter om cybersikkerhedsrisikovurderingen på regionalt plan og prioriteterne for enheder med stor indvirkning og kritisk indvirkning.

2. Senest seks måneder efter vedtagelsen eller ajourføringen af rapporten om cybersikkerhedsrisikovurderingen på regionalt plan forelægger ENTSO for elektricitet i samarbejde med EU DSO-enheden ACER et sammendrag af arbejdsprogrammet.

3. TSO'erne bestræber sig med bistand fra ENTSO for elektricitet og i samarbejde med EU DSO-enheden på at sikre, at de ikkebindende cybersikkerhedsmæssige henstillinger i forbindelse med udbud, der er udarbejdet på grundlag af den relevante regionale cybersikkerhedsrisikovurdering, er ens eller sammenlignelige på tværs af systemdriftsområder. De cybersikkerhedsmæssige henstillinger i forbindelse med udbud omfatter som minimum de specifikationer, der er omhandlet i artikel 33, stk. 2, litra a). Hvor det er muligt, udvælges specifikationerne på grundlag af europæiske og internationale standarder.

4. TSO'erne sikrer med bistand fra ENTSO for elektricitet og i samarbejde med EU DSO-enheden, at de cybersikkerhedsmæssige henstillinger i forbindelse med udbud:

a) overholder udbudsprincipperne i henhold til direktiv 2014/24/EU og

b) er forenelige med og tager hensyn til de seneste tilgængelige europæiske cybersikkerhedscertificeringsordninger, der er relevante for IKT-produktet, IKT-tjenesten eller IKT-processen.

Artikel 36

Vejledning om anvendelse af europæiske cybersikkerhedscertificeringsordninger i forbindelse med indkøb af IKT-produkter, IKT-tjenester og IKT-processer

1. De ikkebindende cybersikkerhedsmæssige henstillinger i forbindelse med udbud, der er udarbejdet i henhold til artikel 35, kan omfatte sektorspecifik vejledning om anvendelse af europæiske cybersikkerhedscertificeringsordninger, når der findes en passende ordning for en bestemt type IKT-produkt, IKT-tjeneste eller IKT-proces, som anvendes af enheder med kritisk indvirkning, uden at dette berører rammen for etablering af europæiske cybersikkerhedscertificeringsordninger i henhold til artikel 46 i forordning (EU) 2019/881.

2. TSO'erne arbejder med bistand fra ENTSO for elektricitet og i samarbejde med EU DSO-enheden tæt sammen med ENISA om at tilvejebringe den sektorspecifikke vejledning, der indgår i de ikkebindende cybersikkerhedsmæssige henstillinger i forbindelse med udbud, i stk. 1.

KAPITEL V

INFORMATIONSSTRØMME, CYBERANGREB OG KRISESTYRING

Artikel 37

Regler om deling af oplysninger

1. Hvis en kompetent myndighed modtager oplysninger vedrørende et indberetningspligtigt cyberangreb, gør den følgende:

a) vurderer fortrolighedsgraden af oplysningerne og underretter enheden om resultatet af sin vurdering uden unødigt ophold og senest 24 timer efter modtagelsen af oplysningerne

b) forsøger at finde andre, lignende cyberangreb i Unionen, som er indberettet til andre kompetente myndigheder, med henblik på at sammenkæde de oplysninger, der er modtaget i forbindelse med det indberetningspligtige cyberangreb, med oplysninger, der er givet i forbindelse med andre cyberangreb, og berige eksisterende oplysninger og styrke og koordinere cybersikkerhedsindsatsen

c) er ansvarlig for at fjerne forretningshemmeligheder og anonymisere oplysningerne i overensstemmelse med de relevante nationale regler og EU-regler

d) deler oplysningerne med de nationale centrale kontaktpunkter, CSIRT'er og alle kompetente myndigheder, der er udpeget i henhold til artikel 4 i andre medlemsstater, uden unødigt ophold og senest 24 timer efter modtagelsen af oplysningerne om et indberetningspligtigt cyberangreb og giver regelmæssigt disse myndigheder og organer ajourførte oplysninger

e) formidler oplysningerne om cyberangrebet efter at have anonymiseret dem og fjernet forretningshemmeligheder i overensstemmelse med stk. 1, litra c), til enheder med kritisk indvirkning og stor indvirkning i sin medlemsstat uden unødigt ophold og senest 24 timer efter at have modtaget oplysningerne, jf. stk. 1, litra a), og giver regelmæssigt ajourførte oplysninger, der gør det muligt for enhederne effektivt at tilrettelægge deres forsvar

f) anmoder eventuelt den enhed med stor indvirkning eller kritisk indvirkning, der har indberettet oplysningerne, om yderligere at formidle de indberetningspligtige oplysninger om cyberangrebet på en sikker måde til andre enheder, der kan være berørt, med henblik på at skabe situationsbevidsthed i elsektoren og forhindre, at der opstår en risiko, der kan eskalere til en grænseoverskridende cybersikkerhedsmæssig elektricitetshændelse

g) deler en sammenfattende rapport med oplysningerne om cyberangrebet med ENISA efter at have anonymiseret oplysningerne og fjernet forretningshemmeligheder.

2. Hvis en CSIRT får kendskab til en aktivt udnyttet sårbarhed, der ikke er afhjulpet, gør den følgende:

a) deler dette med ENISA uden ophold via en passende sikker informationsudvekslingskanal, medmindre andet er fastsat i anden EU-lovgivning

b) bistår den berørte enhed i fra producentens eller udbyderens side at opnå en effektiv, koordineret og hurtig håndtering af den aktivt udnyttede sårbarhed, der ikke er afhjulpet, eller effektive og virkningsfulde afbødende foranstaltninger

c) deler de tilgængelige oplysninger med leverandøren og anmoder producenten eller udbyderen om, hvis det er muligt, at udfærdige en liste over CSIRT'er i de medlemsstater, der er berørt af den aktivt udnyttede sårbarhed, der ikke er afhjulpet, som skal informeres

d) deler de tilgængelige oplysninger med de CSIRT'er, der er identificeret i henhold til foregående litra, efter »need-to-know«-princippet

e) deler strategier og foranstaltninger til at begrænse den indberettede aktivt udnyttede sårbarhed, der ikke er afhjulpet, hvis sådanne findes.

3. Hvis en kompetent myndighed får kendskab til en aktivt udnyttet sårbarhed, der ikke er afhjulpet, gør den kompetente myndighed følgende:

a) deler strategier og foranstaltninger til at begrænse den indberettede aktivt udnyttede sårbarhed, der ikke er afhjulpet, hvis sådanne findes, i samarbejde med CSIRT'erne i den pågældende medlemsstat

b) deler oplysningerne med en CSIRT i den medlemsstat, hvor den aktivt udnyttede sårbarhed, der ikke er afhjulpet, er blevet indberettet.

4. Hvis den kompetente myndighed får kendskab til en sårbarhed, der ikke er afhjulpet, men endnu ikke har bevis for, at denne aktivt udnyttes, koordinerer den uden unødigt ophold med CSIRT'en med henblik på koordineret offentliggørelse af sårbarheden som fastsat i artikel 12, stk. 1, i direktiv (EU) 2022/2555.

5. Hvis en CSIRT modtager oplysninger vedrørende cybertrusler fra én eller flere enheder med stor indvirkning eller kritisk indvirkning i henhold til artikel 38, stk. 6, formidler den disse oplysninger eller andre oplysninger af betydning for at forebygge, opdage, reagere på eller afbøde den pågældende risiko til enheder med kritisk indvirkning eller stor indvirkning i den pågældende medlemsstat og, hvis det er relevant, til alle berørte CSIRT'er og til det nationale centrale kontaktpunkt uden unødigt ophold og senest fire timer efter at have modtaget oplysningerne.

6. Hvis en kompetent myndighed får kendskab til oplysninger vedrørende cybertrusler fra én eller flere enheder med stor indvirkning eller kritisk indvirkning, videresender den disse oplysninger til CSIRT'en med henblik på stk. 5.

7. De kompetente myndigheder kan helt eller delvist uddelegere ansvaret i stk. 3 og 4 for så vidt angår en eller flere enheder med stor indvirkning eller kritisk indvirkning, som er aktive i mere end én medlemsstat, til en anden kompetent myndighed i en af disse medlemsstater efter aftale mellem de berørte kompetente myndigheder.

8. TSO'erne udarbejder med bistand fra ENTSO for elektricitet og i samarbejde med EU DSO-enheden en metode til skalaklassificering af cyberangreb senest den **13. juni 2025**. TSO'erne kan med bistand fra ENTSO for elektricitet og EU DSO-enheden anmode de kompetente myndigheder om at høre ENISA og deres kompetente myndigheder med ansvar for cybersikkerhed med henblik på støtte i udarbejdelsen af en sådan klassificeringsskala. Metoden omfatter klassificering af alvorsgraden af cyberangreb efter fem niveauer, hvoraf de to højeste niveauer er »høj« og »kritisk«. Klassificeringen baseres på en vurdering af følgende parametre:

a) den potentielle virkning under hensyntagen til de eksponerede aktiver og områder som fastlagt i overensstemmelse med artikel 26, stk. 4, litra c) og

b) cyberangrebets omfang.

9. Senest den **13. juni 2026** foretager ENTSO for elektricitet i samarbejde med EU DSO-enheden en gennemførlighedsundersøgelse for at vurdere muligheden for at udvikle et fælles værktøj, der gør det muligt for alle enheder at dele oplysninger med de relevante nationale myndigheder, og de finansielle omkostninger, det vil kræve at udvikle værktøjet.

10. I gennemførlighedsundersøgelsen behandles mulighederne for, at et sådant fælles værktøj kan:

a) støtte enheder med kritisk indvirkning og stor indvirkning med relevante sikkerhedsrelaterede oplysninger med henblik på drift af grænseoverskridende elektricitetsstrømme, som f.eks. indberetning af cyberangreb i næsten realtid, tidlig varsling i cybersikkerhedsspørgsmål og skjulte sårbarheder i udstyr, der anvendes i elektricitetssystemet

b) vedligeholdes i et passende miljø med en høj grad af tillid

c) muliggøre dataindsamling fra enheder med kritisk indvirkning og stor indvirkning og gøre det nemmere at fjerne fortrolige oplysninger og anonymisere dataene og formidle dem hurtigt til enheder med kritisk indvirkning og stor indvirkning.

11. ENTSO for elektricitet gør i samarbejde med EU DSO-enheden følgende:

a) hører ENISA og NIS-samarbejdsgruppen, de nationale centrale kontaktpunkter og repræsentanterne for de vigtigste interessenter, når de vurderer gennemførligheden

b) forelægger resultaterne af gennemførlighedsundersøgelsen for ACER og NIS-samarbejdsgruppen.

12. ENTSO for elektricitet kan i samarbejde med EU DSO-enheden analysere og facilitere initiativer, der er foreslået af enheder med kritisk indvirkning eller stor indvirkning, med henblik på at evaluere og afprøve sådanne værktøjer til deling af oplysninger.

Artikel 38

Rollen for enheder med stor indvirkning og kritisk indvirkning i delingen af oplysninger

1. Hver enhed med stor indvirkning eller kritisk indvirkning:

a) etablerer for alle aktiver inden for sit cybersikkerhedsområde som fastlagt i overensstemmelse med artikel 26, stk. 4, litra c), som minimum CSOC-kapacitet til at:

   i) sikre, at de relevante net- og informationssystemer og -applikationer indeholder sikkerhedslogfiler til sikkerhedsovervågning for at gøre det muligt at opdage uregelmæssigheder og indsamle oplysninger om cyberangreb

   ii) foretage sikkerhedsovervågning, herunder afsløring af indtrængen og vurdering af sårbarheder i net- og informationssystemer

   iii) analysere og om nødvendigt træffe alle nødvendige foranstaltninger inden for dens ansvarsområde og efter dens kapacitet til at beskytte enheden

   iv) deltage i indsamlingen og delingen af oplysninger som beskrevet i nærværende artikel

b) har ret til at indkøbe alle eller dele af den i litra a) omhandlede kapacitet gennem udbydere af administrerede sikkerhedstjenester. Enheder med kritisk indvirkning eller stor indvirkning forbliver ansvarlige for udbydere af administrerede sikkerhedstjenester og fører tilsyn med deres indsats

c) udpeger et centralt kontaktpunkt på enhedsniveau med henblik på deling af oplysninger.

2. ENISA kan som led i den opgave, der er fastsat i artikel 6, stk. 2, i forordning (EU) 2019/881, give ikkebindende vejledning om etablering af en sådan kapacitet eller om underentreprise af tjenester til udbydere af administrerede sikkerhedstjenester.

3. Hver enhed med kritisk indvirkning eller stor indvirkning deler relevante oplysninger vedrørende et indberetningspligtigt cyberangreb med sine CSIRT'er og sin kompetente myndighed uden unødigt ophold og senest fire timer efter at have fået kendskab til, at hændelsen er indberetningspligtig.

4. Oplysninger vedrørende et cyberangreb anses for at være indberetningspligtige, når den berørte enhed vurderer cyberangrebet til at have en alvorsgrad, der spænder fra »høj« til »kritisk« efter den i artikel 37, stk. 8, omhandlede metode til skalaklassificering af cyberangreb. Det centrale kontaktpunkt på enhedsniveau, der er udpeget i henhold til stk. 1, litra c), meddeler klassificeringen af hændelsen.

5. Når enheder med kritisk indvirkning eller stor indvirkning indberetter relevante oplysninger vedrørende aktivt udnyttede sårbarheder, der ikke er afhjulpet, til en CSIRT, kan sidstnævnte fremsende oplysningerne til sin kompetente myndighed. Alt efter følsomhedsgraden af de indberettede oplysninger kan CSIRT'en tilbageholde oplysningerne eller udsætte fremsendelsen af dem af begrundede cybersikkerhedsrelaterede årsager.

6. Hver enhed med kritisk indvirkning eller stor indvirkning stiller uden unødigt ophold alle oplysninger vedrørende en indberetningspligtig cybertrussel, som kan have en grænseoverskridende virkning, til rådighed for sine CSIRT'er. Oplysninger vedrørende en cybertrussel anses for at være indberetningspligtige, når mindst én af følgende betingelser er opfyldt:

a) de indeholder oplysninger, der er relevante for, at andre enheder med kritisk indvirkning eller stor indvirkning kan forebygge, opdage, reagere på eller afbøde indvirkningen af risikoen

b) de pågældende teknikker, taktikker og procedurer, der er anvendt i forbindelse med et angreb, fører til oplysninger, som f.eks. kompromitterede URL- eller IP-adresser, hashfunktioner eller andre attributter, der er nyttige for at kontekstualisere og finde sammenhænge i angrebet

c) en cybertrussel kan yderligere vurderes og kontekstualiseres med flere oplysninger fra tjenesteudbydere eller tredjeparter, der ikke er omfattet af denne forordning.

7. Hver enhed med kritisk indvirkning eller stor indvirkning angiver ved deling af oplysninger i henhold til denne artikel følgende:

a) at oplysningerne forelægges i henhold til denne forordning

b) om oplysningerne vedrører:

   i) et indberetningspligtigt cyberangreb, jf. stk. 3

   ii) aktivt udnyttede sårbarheder, der ikke er afhjulpet, og som ikke er offentligt kendte, jf. stk. 4

   iii) en indberetningspligtig cybertrussel, jf. stk. 5

c) hvis der er tale om et indberetningspligtigt cyberangreb, cyberangrebets niveau efter den i artikel 37, stk. 8, omhandlede metode til skalaklassificering af cyberangreb og de oplysninger, der fører til denne klassificering, herunder som minimum cyberangrebets alvorsgrad.

8. Når en enhed med kritisk indvirkning eller stor indvirkning underretter om en væsentlig hændelse i henhold til artikel 23 i direktiv (EU) 2022/2555, og underretningen af hændelsen i henhold til nævnte artikel indeholder relevante oplysninger som omhandlet i nærværende artikels stk. 3, udgør enhedens underretning i henhold til nævnte direktivs artikel 23, stk. 1, indberetning af oplysninger i henhold til nærværende artikels stk. 3.

9. Hver enhed med kritisk indvirkning eller stor indvirkning rapporterer til sin kompetente myndighed eller CSIRT og angiver klart specifikke oplysninger, som kun må deles med den kompetente myndighed eller CSIRT'en, hvis delingen af oplysningerne kan være kilde til et cyberangreb. Hver enhed med kritisk indvirkning eller stor indvirkning har ret til at fremsende en ikkefortrolig udgave af oplysningerne til den kompetente CSIRT.

Artikel 39

Afsløring af cyberangreb og håndtering af relaterede oplysninger

1. Enheder med kritisk indvirkning eller stor indvirkning udvikler den nødvendige kapacitet til at håndtere afslørede cyberangreb med den nødvendige støtte fra den relevante kompetente myndighed, ENTSO for elektricitet og EU DSO-enheden. Enheder med kritisk indvirkning eller stor indvirkning kan støttes af den CSIRT, der er udpeget i deres respektive medlemsstat, som led i den opgave, der er tildelt CSIRT'erne i henhold til artikel 11, stk. 5, litra a), i direktiv (EU) 2022/2555. Enheder med kritisk indvirkning eller stor indvirkning indfører effektive procedurer til at afsløre, klassificere og reagere på cyberangreb, der vil eller kan påvirke grænseoverskridende elektricitetsstrømme, med henblik på at minimere deres virkning.

2. Hvis et cyberangreb påvirker grænseoverskridende elektricitetsstrømme, samarbejder de centrale kontaktpunkter på enhedsniveau for de berørte enheder med kritisk indvirkning eller stor indvirkning om at dele oplysninger mellem dem under koordinering af den kompetente myndighed i den medlemsstat, hvor cyberangrebet første gang blev indberettet.

3. Enheder med kritisk indvirkning eller stor indvirkning:

a) sørger for, at deres eget centrale kontaktpunkt på enhedsniveau har adgang efter »need-to-know«-princippet til de oplysninger, de har modtaget fra det nationale centrale kontaktpunkt gennem deres kompetente myndighed

b) forelægger, medmindre dette allerede er sket i henhold til artikel 3, stk. 4, i direktiv (EU) 2022/2555, den kompetente myndighed i den medlemsstat, hvor de er etableret, og det nationale centrale kontaktpunkt en liste over deres centrale kontaktpunkter for cybersikkerhed på enhedsniveau:

   i) fra hvilke den kompetente myndighed og det nationale centrale kontaktpunkt kan forvente at modtage oplysninger om indberetningspligtige cyberangreb

   ii) til hvilke kompetente myndigheder og nationale centrale kontaktpunkter kan være nødt til at give oplysninger

c) fastsætter procedurer for håndtering af cyberangreb, herunder roller og ansvarsområder, opgaver og reaktioner på grundlag af den observerbare udvikling af cyberangrebet inden for områderne med kritisk indvirkning og stor indvirkning

d) afprøver de overordnede procedurer for håndtering af cyberangreb mindst hvert år ved at prøve mindst ét scenarium, der direkte eller indirekte påvirker grænseoverskridende elektricitetsstrømme. Den årlige afprøvning kan udføres af enheder med kritisk indvirkning eller stor indvirkning i forbindelse med de regelmæssige øvelser, der er omhandlet i artikel 43. Enhver direkte aktivitet som reaktion på et cyberangreb med en virkning på minimum niveau 2 efter den i artikel 37, stk. 8, omhandlede metode til skalaklassificering af cyberangreb, og hvis grundlæggende årsag er relateret til cybersikkerhed, kan tjene som årlig afprøvning af beredskabsplanen for cyberangreb.

4. De i stk. 1 nævnte opgaver kan af medlemsstaterne også uddelegeres til de regionale koordinationscentre i overensstemmelse med artikel 37, stk. 2, i forordning (EU) 2019/943.

Artikel 40

Krisestyring

1. Når den kompetente myndighed konstaterer, at en elkrise er forbundet med et cyberangreb, der påvirker mere end én medlemsstat, opretter de kompetente myndigheder i de berørte medlemsstater, de kompetente myndigheder med ansvar for cybersikkerhed, de myndigheder, der er kompetente inden for risikoberedskab, og NIS-cyberkrisestyringsmyndighederne fra de berørte medlemsstater i fællesskab en ad hoc-gruppe for grænseoverskridende krisekoordinering.

2. Ad hoc-gruppen for grænseoverskridende krisekoordinering:

a) koordinerer en effektiv indhentning og videreformidling af alle relevante cybersikkerhedsrelaterede oplysninger til de enheder, der er involveret i krisestyringen

b) tilrettelægger kommunikationen mellem alle enheder, der er berørt af krisen, og de kompetente myndigheder med henblik på at mindske overlapninger og øge effektiviteten af analyserne og de tekniske reaktioner for at afhjælpe de samtidige elkriser, hvis grundlæggende årsag er relateret til cybersikkerhed

c) stiller i samarbejde med de kompetente CSIRT'er den nødvendige ekspertise til rådighed, herunder operationel rådgivning om gennemførelsen af mulige afbødende foranstaltninger til de enheder, der er berørt af hændelsen

d) underretter og giver regelmæssigt Kommissionen og Elektricitetskoordinationsgruppen opdateringer om status for hændelsen i overensstemmelse med beskyttelsesprincipperne i artikel 46

e) søger rådgivning fra relevante myndigheder, agenturer eller enheder, der kan hjælpe med at afbøde elkrisen.

3. Hvis cyberangrebet kvalificeres eller forventes at kunne kvalificeres som en omfattende cybersikkerhedshændelse, underretter ad hoc-gruppen for grænseoverskridende krisekoordinering omgående de nationale cyberkrisestyringsmyndigheder som omhandlet i artikel 9, stk. 1, i direktiv (EU) 2022/2555 i de medlemsstater, der er berørt af hændelsen, samt Kommissionen og EU-CyCLONe. I disse tilfælde støtter ad hoc-gruppen for grænseoverskridende krisekoordinering EU-CyCLONe med hensyn til særlige sektorspecifikke forhold.

4. Enheder med kritisk indvirkning eller stor indvirkning udvikler og råder over kapacitet, interne retningslinjer, beredskabsplaner og personale til at tage del i at afdække og afbøde grænseoverskridende kriser. Enheder med kritisk indvirkning eller stor indvirkning, som er berørt af en samtidig elkrise, undersøger den grundlæggende årsag til denne krise i samarbejde med deres kompetente myndighed for at fastslå, i hvilket omfang krisen er forbundet med et cyberangreb.

5. Opgaverne i stk. 4 kan af medlemsstaterne også uddelegeres til de regionale koordinationscentre i overensstemmelse med artikel 37, stk. 2, i forordning (EU) 2019/943.

Artikel 41

Cybersikkerhedskrisestyrings- og -beredskabsplaner

1. Senest 24 måneder efter underretningen af ACER om rapporten om risikovurderingen på EU-plan udarbejder ACER i tæt samarbejde med ENISA, ENTSO for elektricitet, EU DSO-enheden, kompetente myndigheder med ansvar for cybersikkerhed, kompetente myndigheder, myndigheder, der er kompetente inden for risikoberedskab, nationale regulerende myndigheder og de nationale NIS-cyberkrisestyringsmyndigheder en cybersikkerhedskrisestyrings- og -beredskabsplan på EU-plan for elsektoren.

2. Senest 12 måneder efter ACER's udarbejdelse af cybersikkerhedskrisestyrings- og -beredskabsplanen på EU-plan for elsektoren i henhold til stk. 1 udarbejder hver kompetent myndighed en national cybersikkerhedskrisestyrings- og -beredskabsplan for grænseoverskridende elektricitetsstrømme under hensyntagen til cybersikkerhedskrisestyringsplanen på EU-plan og den nationale risikoberedskabsplan, der er udarbejdet i henhold til artikel 10 i forordning (EU) 2019/941. Planen skal være i overensstemmelse med beredskabsplanen for omfattende cybersikkerhedshændelser og kriser i henhold til artikel 9, stk. 4, i direktiv (EU) 2022/2555. Den kompetente myndighed koordinerer med enhederne med kritisk indvirkning og stor indvirkning og med den myndighed, der er kompetent inden for risikoberedskab i den pågældende medlemsstat.

3. Den nationale beredskabsplan for omfattende cybersikkerhedshændelser og kriser i henhold til artikel 9, stk. 4, i direktiv (EU) 2022/2555 anses for at være en national cybersikkerhedskrisestyringsplan som omhandlet i nærværende artikel, hvis den omfatter krisestyrings- og beredskabsbestemmelser med hensyn til de grænseoverskridende elektricitetsstrømme.

4. Opgaverne i stk. 1 og 2 kan af medlemsstaterne også uddelegeres til de regionale koordinationscentre i overensstemmelse med artikel 37, stk. 2, i forordning (EU) 2019/943.

5. Enheder med kritisk indvirkning eller stor indvirkning sørger for, at deres cybersikkerhedsrelaterede krisestyringsprocedurer:

a) omfatter kompatible procedurer for håndtering af hændelser som defineret i artikel 6, nr. 8), i direktiv (EU) 2022/2555 med hensyn til grænseoverskridende cybersikkerhed, som er formelt indarbejdet i deres krisestyringsplaner

b) er en del af de overordnede krisestyringsaktiviteter.

6. Senest 12 måneder efter underretningen af enheder med stor indvirkning og kritisk indvirkning i henhold til artikel 24, stk. 6, og hvert tredje år herefter udarbejder enheder med kritisk indvirkning og stor indvirkning en krisestyringsplan på enhedsniveau for cybersikkerhedsrelaterede kriser, og denne indgår i deres overordnede krisestyringsplaner. Planen skal mindst omfatte følgende oplysninger:

a) reglerne for erklæring af krisen, jf. artikel 14, stk. 2 og 3, i forordning (EU) 2019/941

b) klare roller og ansvarsområder med henblik på krisestyring, herunder den rolle, som andre relevante enheder med kritisk indvirkning eller stor indvirkning spiller

c) ajourførte kontaktoplysninger samt regler for kommunikation og deling af oplysninger i en krisesituation, herunder forbindelsen til CSIRT'erne.

7. Krisestyringsforanstaltninger som omhandlet i artikel 21, stk. 2, litra c), i direktiv (EU) 2022/2555 betragtes som en krisestyringsplan på enhedsniveau for elsektoren i henhold til nærværende artikel, hvis den opfylder alle krav i stk. 6.

8. Krisestyringsplanerne afprøves under de cybersikkerhedsøvelser, der er omhandlet i artikel 43, 44 og 45.

9. Enheder med kritisk indvirkning eller stor indvirkning medtager deres krisestyringsplaner på enhedsniveau i deres forretningskontinuitetsplaner for processer med kritisk indvirkning og stor indvirkning. Krisestyringsplanerne på enhedsniveau skal omfatte:

a) processer, der afhænger af IT-tjenesters tilgængelighed, integritet og pålidelighed

b) alle forretningskontinuitetslokationer, herunder lokationer med hardware og software

c) alle interne roller og ansvarsområder i forbindelse med forretningskontinuitetsprocedurer.

10. Enheder med kritisk indvirkning eller stor indvirkning ajourfører deres krisestyringsplaner på enhedsniveau mindst hvert tredje år, og når det er nødvendigt.

11. ACER ajourfører den cybersikkerhedskrisestyrings- og -beredskabsplan på EU-plan for elsektoren, der er udarbejdet i henhold til stk. 1, mindst hvert tredje år, og når det er nødvendigt.

12. Hver kompetent myndighed ajourfører den nationale cybersikkerhedskrisestyrings- og -beredskabsplan for grænseoverskridende elektricitetsstrømme, der er udarbejdet i henhold til stk. 2, mindst hvert tredje år, og når det er nødvendigt.

13. Enheder med kritisk indvirkning eller stor indvirkning afprøver deres forretningskontinuitetsplaner mindst én gang hvert tredje år eller efter større ændringer i en proces med kritisk indvirkning. Resultatet af afprøvninger af forretningskontinuitetsplanerne dokumenteres. Enheder med kritisk indvirkning eller stor indvirkning kan lade afprøvningen af deres forretningskontinuitetsplan indgå i cybersikkerhedsøvelserne.

14. Enheder med kritisk indvirkning eller stor indvirkning ajourfører deres forretningskontinuitetsplan, når det er nødvendigt, og mindst én gang hvert tredje år under hensyntagen til resultatet af afprøvningen.

15. Hvis der ved en afprøvning konstateres mangler i forretningskontinuitetsplanen, afhjælper enheden med kritisk indvirkning eller stor indvirkning disse mangler senest 180 kalenderdage efter afprøvningen og gennemfører en ny afprøvning for at dokumentere, at de korrigerende foranstaltninger har haft effekt.

16. Hvis en enhed med kritisk indvirkning eller stor indvirkning ikke kan afhjælpe manglerne inden for 180 kalenderdage, medtager enheden årsagerne hertil i den rapport, der skal forelægges enhedens kompetente myndighed i henhold til artikel 27.

Artikel 42

Kapacitet til tidlig varsling i cybersikkerhedsspørgsmål for elsektoren

1. De kompetente myndigheder samarbejder med ENISA om at udvikle kapacitet til tidlig varsling i cybersikkerhedsspørgsmål i forbindelse med elektricitetsstrømme (ECEAC) som en del af bistanden til medlemsstaterne i henhold til artikel 6, stk. 2 og 7, i forordning (EU) 2019/881.

2. ECEAC sætter ENISA i stand til, når det udfører opgaverne i artikel 7, stk. 7, i forordning (EU) 2019/881:

a) at indsamle frivillige delte oplysninger fra:

   i) CSIRT'er og kompetente myndigheder

   ii) de enheder, der er opført i nærværende forordnings artikel 2

   iii) enhver anden enhed, der ønsker at dele relevante oplysninger på frivillig basis

b) at vurdere og klassificere de indsamlede oplysninger

c) at vurdere de oplysninger, ENISA har adgang til, med henblik på at kortlægge cyberrisikoforhold og relevante indikatorer for aspekter af grænseoverskridende elektricitetsstrømme

d) at kortlægge forhold og indikatorer, der ofte hænger sammen med cyberangreb, i elsektoren

e) gennem vurdering og kortlægning af risikofaktorer at fastslå, om der skal foretages yderligere analyser og træffes yderligere forebyggende foranstaltninger

f) at oplyse de kompetente myndigheder om de konstaterede risici og de anbefalede forebyggende foranstaltninger, som er specifikke for de berørte enheder

g) at underrette alle relevante enheder, der er opført i artikel 2, om resultatet af vurderingen af oplysningerne, jf. dette stykkes litra b), c) og d)

h) regelmæssigt at medtage de relevante oplysninger i den situationsrapport, der udarbejdes i henhold til artikel 7, stk. 6, i forordning (EU) 2019/881

i) hvor det er muligt, at udlede relevante data, der indikerer et potentielt brud på sikkerheden eller cyberangreb (»kompromitteringsindikatorer«), fra de indsamlede oplysninger.

3. CSIRT'erne formidler uden ophold oplysninger modtaget fra ENISA til de berørte enheder inden for rammerne af deres opgaver i artikel 11, stk. 3, litra b), i direktiv (EU) 2022/2555.

4. ACER overvåger, hvor effektiv ECEAC'en er. ENISA bistår ACER ved at stille alle nødvendige oplysninger til rådighed i overensstemmelse med artikel 6, stk. 2, og artikel 7, stk. 1, i forordning (EU) 2019/881. Analysen af denne overvågning er en del af overvågningen i henhold til nærværende forordnings artikel 12.

KAPITEL VI

RAMME FOR CYBERSIKKERHEDSØVELSER I FORBINDELSE MED ELEKTRICITETSSTRØMME

Artikel 43

Cybersikkerhedsøvelser på enhedsniveau og medlemsstatsniveau

1. Senest den 31. december i året efter underretningen af enheder med kritisk indvirkning og hvert tredje år herefter gennemfører hver enhed med kritisk indvirkning en cybersikkerhedsøvelse, der omfatter ét eller flere scenarier med cyberangreb, der direkte eller indirekte påvirker grænseoverskridende elektricitetsstrømme, og vedrører de risici, der er konstateret i cybersikkerhedsrisikovurderingerne på medlemsstatsniveau og enhedsniveau, jf. artikel 20 og artikel 27.

2. Uanset stk. 1 kan den myndighed, der er kompetent inden for risikoberedskab, efter høring af den kompetente myndighed og den relevante cyberkrisestyringsmyndighed som udpeget eller oprettet i henhold til artikel 9 i direktiv (EU) 2022/2555 beslutte at tilrettelægge en cybersikkerhedsøvelse på medlemsstatsniveau som beskrevet i stk. 1 i stedet for at gennemføre cybersikkerhedsøvelsen på enhedsniveau. I den forbindelse underretter den kompetente myndighed:

a) alle enheder med kritisk indvirkning i den pågældende medlemsstat, den nationale regulerende myndighed, CSIRT'erne og den kompetente myndighed med ansvar for cybersikkerhed senest den 30. juni i det år, der går forud for cybersikkerhedsøvelsen på enhedsniveau

b) hver enhed, der skal deltage i cybersikkerhedsøvelsen på medlemsstatsniveau, senest 6 måneder før øvelsen afholdes.

3. Den myndighed, der er kompetent inden for risikoberedskab, tilrettelægger med teknisk støtte fra sine CSIRT'er den i stk. 2 beskrevne cybersikkerhedsøvelse på medlemsstatsniveau uafhængigt af eller i forbindelse med en anden cybersikkerhedsøvelse i den pågældende medlemsstat. For at kunne gruppere øvelserne kan den myndighed, der er kompetent inden for risikoberedskab, udsætte cybersikkerhedsøvelsen på medlemsstatsniveau i stk. 1 med ét år.

4. Cybersikkerhedsøvelserne på enhedsniveau og medlemsstatsniveau skal være i overensstemmelse med de nationale rammer for cybersikkerhedskrisestyring, jf. artikel 9, stk. 4, litra d), i direktiv (EU) 2022/2555.

5. Senest den **31. december 2026** og hvert tredje år herefter stiller ENTSO for elektricitet i samarbejde med EU DSO-enheden en model for et øvelsesscenarium til rådighed med henblik på gennemførelse af cybersikkerhedsøvelserne på enhedsniveau og medlemsstatsniveau i stk. 1. I modellen tages der hensyn til resultaterne af de senest gennemførte cybersikkerhedsrisikovurderinger på enhedsniveau og medlemsstatsniveau, og den skal omfatte centrale succeskriterier. ENTSO for elektricitet og EU DSO-enheden inddrager ACER og ENISA i udarbejdelsen af modellen.

Artikel 44

Regionale og tværregionale cybersikkerhedsøvelser

1. Senest den **31. december 2029** og hvert tredje år herefter tilrettelægger ENTSO for elektricitet i samarbejde med EU DSO-enheden en regional cybersikkerhedsøvelse i hvert systemdriftsområde. Enhederne med kritisk indvirkning i systemdriftsområdet deltager i den regionale cybersikkerhedsøvelse. ENTSO for elektricitet kan i samarbejde med EU DSO-enheden i stedet for en regional cybersikkerhedsøvelse tilrettelægge en tværregional cybersikkerhedsøvelse i mere end ét systemdriftsområde inden for samme tidsramme. I øvelsen bør der tages hensyn til andre, eksisterende cybersikkerhedsrisikovurderinger og -scenarier på EU-plan.

2. ENISA støtter ENTSO for elektricitet og EU DSO-enheden i forberedelsen og tilrettelæggelsen af cybersikkerhedsøvelsen på regionalt eller tværregionalt plan.

3. ENTSO for elektricitet underretter i samarbejde med EU DSO-enheden de enheder med kritisk indvirkning, der skal deltage i den regionale eller tværregionale cybersikkerhedsøvelse, seks måneder før øvelsen afholdes.

4. Tilrettelæggeren af en regelmæssig cybersikkerhedsøvelse på EU-plan i henhold til artikel 7, stk. 5, i forordning (EU) 2019/881 eller en anden obligatorisk cybersikkerhedsøvelse med forbindelse til elsektoren inden for samme geografiske område kan indbyde ENTSO for elektricitet og EU DSO-enheden til at deltage. I disse tilfælde finder forpligtelsen i stk. 1 ikke anvendelse, forudsat at alle enheder med kritisk indvirkning i systemdriftsområdet deltager i samme øvelse.

5. Hvis ENTSO for elektricitet og EU DSO-enheden deltager i en cybersikkerhedsøvelse som omhandlet i stk. 4, kan de udsætte den regionale eller tværregionale cybersikkerhedsøvelse i stk. 1 med ét år.

6. Senest den **31. december 2027** og hvert tredje år efter denne dato stiller ENTSO for elektricitet i samarbejde med EU DSO-enheden en øvelsesmodel til rådighed med henblik på gennemførelse af regionale og tværregionale cybersikkerhedsøvelser. I modellen tages der hensyn til resultaterne af de senest gennemførte cybersikkerhedsrisikovurderinger på regionalt plan, og den skal omfatte centrale succeskriterier. ENTSO for elektricitet hører Kommissionen og kan rådføre sig med ACER, ENISA og Det Fælles Forskningscenter om tilrettelæggelsen og gennemførelsen af de regionale og tværregionale cybersikkerhedsøvelser.

Artikel 45

Resultat af cybersikkerhedsøvelser på enhedsniveau, medlemsstatsniveau, regionalt plan og tværregionalt plan

1. Efter anmodning fra en enhed med kritisk indvirkning deltager kritiske tjenesteudbydere i de cybersikkerhedsøvelser, der er omhandlet i artikel 43, stk. 1 og 2, og i artikel 44, stk. 1, hvis de leverer tjenester til enheden med kritisk indvirkning på et område, der er omfattet af den pågældende cybersikkerhedsøvelse.

2. Tilrettelæggerne af de cybersikkerhedsøvelser, der er omhandlet i artikel 43, stk. 1 og 2, og i artikel 44, stk. 1, analyserer og afslutter med rådgivning fra ENISA, hvis de anmoder herom og i overensstemmelse med artikel 7, stk. 5, i forordning (EU) 2019/881, den pågældende cybersikkerhedsøvelse med en rapport, der sammenfatter erfaringerne, og som er henvendt til alle deltagere. Rapporten skal omfatte:

a) øvelsesscenarierne, møderapporter, de vigtigste holdninger, succeser og indhøstede erfaringer på alle niveauer i værdikæden for elektricitet

b) hvorvidt de vigtigste succeskriterier blev opfyldt

c) en liste over anbefalinger til de enheder, der deltog i den pågældende cybersikkerhedsøvelse, med henblik på at korrigere, tilpasse eller ændre cybersikkerhedskriseprocedurer, processer, tilknyttede styringsmodeller og eventuelle eksisterende kontraktlige forpligtelser med kritiske tjenesteudbydere.

3. Hvis CSIRT-netværket, NIS-samarbejdsgruppen eller EU-CyCLONe anmoder herom, deler tilrettelæggerne af de cybersikkerhedsøvelser, der er omhandlet i artikel 43, stk. 1 og 2, og i artikel 44, stk. 1, resultatet af den pågældende cybersikkerhedsøvelse. Tilrettelæggerne deler de oplysninger, der er omhandlet i nærværende artikels stk. 2, litra a) og b), med hver enhed, der deltog i øvelserne. Tilrettelæggerne deler listen over anbefalinger i nævnte stykkes litra c) udelukkende med de enheder, der er omfattet af anbefalingerne.

4. Tilrettelæggerne af de cybersikkerhedsøvelser, der er omhandlet i artikel 43, stk. 1 og 2, og artikel 44, stk. 1, følger regelmæssigt op med de enheder, der deltager i øvelserne, om gennemførelsen af de anbefalinger, der er omhandlet i nærværende artikels stk. 2, litra c).

KAPITEL VII

BEKYTTELSE AF OPLYSNINGER

Artikel 46

Principper for beskyttelse af udvekslede oplysninger

1. De enheder, der er opført i artikel 2, stk. 1, sikrer, at oplysninger, der stilles til rådighed, modtages, udveksles eller videregives i henhold til denne forordning, kun er tilgængelige efter need-to-know-princippet og i overensstemmelse med relevante EU-regler og nationale regler om informationssikkerhed.

2. De enheder, der er opført i artikel 2, stk. 1, sikrer, at oplysninger, der stilles til rådighed, modtages, udveksles eller videregives i henhold til denne forordning, håndteres og spores i hele oplysningernes livscyklus, og at de kun kan frigives ved afslutningen af deres livscyklus efter at være blevet anonymiseret.

3. De enheder, der er opført i artikel 2, stk. 1, sikrer, at der er truffet alle de beskyttelsesforanstaltninger af organisatorisk eller teknisk art, der er nødvendige for at garantere og beskytte fortroligheden, integriteten, tilgængeligheden og uafviseligheden af de oplysninger, der stilles til rådighed, modtages, udveksles eller videregives i henhold til denne forordning, uafhængigt af de anvendte midler. Beskyttelsesforanstaltningerne skal:

a) være forholdsmæssige

b) tage hensyn til cybersikkerhedsrisici i forbindelse med kendte tidligere og nye trusler, som oplysningerne kan være genstand for i forbindelse med denne forordning

c) så vidt muligt være baseret på nationale, europæiske eller internationale standarder og bedste praksis

d) være dokumenterede.

4. De enheder, der er opført i artikel 2, stk. 1, sikrer, at enhver person, som gives adgang til oplysninger, der er stillet til rådighed, modtaget, udvekslet eller videregivet i henhold til denne forordning, instrueres om de sikkerhedsregler, der finder anvendelse på enhedsniveau, og om de foranstaltninger og procedurer, der er relevante for beskyttelsen af oplysningerne. Enhederne sikrer, at den pågældende person anerkender ansvaret for at beskytte oplysningerne i overensstemmelse med instruksen.

5. De enheder, der er opført i artikel 2, stk. 1, sikrer, at adgangen til oplysninger, der stilles til rådighed, modtages, udveksles eller videregives i henhold til denne forordning, er begrænset til enkeltpersoner:

a) som har tilladelse til at tilgå oplysningerne på grundlag af deres funktion og i et omfang, der er begrænset til udførelsen af de tildelte opgaver

b) for hvem enheden har været i stand til at vurdere etiske principper og integritetsprincipper, og for hvem der ikke er dokumentation for et negativt resultat af et baggrundstjek for at vurdere vedkommendes pålidelighed i overensstemmelse med enhedens bedste praksis og standardsikkerhedskrav og, hvis det er nødvendigt, med nationale love og bestemmelser.

6. De enheder, der er opført i artikel 2, stk. 1, opnår skriftlig godkendelse fra den fysiske eller juridiske person, der oprindeligt skabte oplysningerne eller stillede dem til rådighed, inden de videregiver disse oplysninger til en tredjepart, der falder uden for denne forordnings anvendelsesområde.

7. En enhed, der er opført i artikel 2, stk. 1, kan vurdere, at oplysningerne skal deles uden at overholde nærværende artikels stk. 1 og 4 for at forhindre en samtidig elkrise, hvis grundlæggende årsag er relateret til cybersikkerhed, eller en grænseoverskridende krise i Unionen i en anden sektor. I disse tilfælde skal den:

a) høre og opnå godkendelse af den kompetente myndighed til at dele oplysningerne

b) anonymisere oplysningerne, uden at de elementer, der er nødvendige for at informere offentligheden om en overhængende og alvorlig risiko, der påvirker grænseoverskridende elektricitetsstrømme, og de mulige afbødende foranstaltninger, går tabt

c) beskytte identiteten af ophavsmanden og de enheder, der har behandlet oplysningerne, i overensstemmelse med denne forordning.

8. Uanset denne artikels stk. 6 kan de kompetente myndigheder give oplysninger, der er stillet til rådighed, modtaget, udvekslet eller videregivet i henhold til denne forordning, til en tredjepart, der ikke er opført i artikel 2, stk. 1, uden forudgående skriftligt samtykke fra ophavsmanden til oplysningerne, men skal underrette sidstnævnte så hurtigt som muligt. Inden den pågældende kompetente myndighed videregiver oplysninger, der er stillet til rådighed, modtaget, udvekslet eller videregivet i henhold til denne forordning, til en tredjepart, der ikke er opført i artikel 2, stk. 1, sikrer den med rimelighed, at den pågældende tredjepart er bekendt med de gældende sikkerhedsregler, og opnår rimelig sikkerhed for, at den pågældende tredjepart kan beskytte de modtagne oplysninger i overensstemmelse med nærværende artikels stk. 1-5. Den kompetente myndighed anonymiserer oplysningerne, uden at de elementer, der er nødvendige for at informere offentligheden om en overhængende og alvorlig risiko, der påvirker grænseoverskridende elektricitetsstrømme, og mulige afbødende foranstaltninger, går tabt, og beskytter identiteten af ophavsmanden til oplysningerne. I disse tilfælde beskytter tredjeparten, som ikke er opført i artikel 2, stk. 1, de modtagne oplysninger i overensstemmelse med allerede gældende bestemmelser på enhedsniveau eller, hvis dette ikke er muligt, med de bestemmelser og instrukser, som den relevante kompetente myndighed har givet.

9. Denne artikel finder ikke anvendelse på enheder, der ikke er opført i artikel 2, stk. 1, og som modtager oplysninger efter nærværende artikels stk. 6. I disse tilfælde finder nærværende artikels stk. 7 anvendelse, eller den kompetente myndighed kan give den pågældende enhed skriftlige bestemmelser, der finder anvendelse i tilfælde, hvor der modtages oplysninger i henhold til denne forordning.

Artikel 47

Fortroligheden af oplysninger

1. Alle oplysninger, der stilles til rådighed, modtages, udveksles eller videregives i henhold til denne forordning, er underlagt de betingelser vedrørende tavshedspligt, der er fastsat i denne artikels stk. 2-5, og de krav, der er fastsat i artikel 65 i forordning (EU) 2019/943. Alle oplysninger, der stilles til rådighed, modtages, udveksles eller videregives blandt enheder, der er opført i nærværende forordnings artikel 2, med henblik på gennemførelsen af nærværende forordning, beskyttes under hensyntagen til den fortrolighedsgrad, som ophavsmanden anvender for oplysningerne.

2. Tavshedspligten gælder for de enheder, der er opført i artikel 2.

3. De kompetente myndigheder med ansvar for cybersikkerhed, de nationale regulerende myndigheder, de myndigheder, der er kompetente inden for risikoberedskab, og CSIRT'erne udveksler alle de oplysninger, der er nødvendige for, at de kan udføre deres opgaver.

4. Alle oplysninger, der stilles til rådighed, modtages, udveksles eller videregives blandt enheder, der er opført i artikel 2, stk. 1, med henblik på gennemførelsen af artikel 23, anonymiseres og aggregeres.

5. Oplysninger, der modtages af en enhed eller myndighed, der er omfattet af denne forordning, i forbindelse med deres hverv, må ikke videregives til andre enheder eller myndigheder, medmindre dette sker i tilfælde, der er omfattet af national lovgivning, andre bestemmelser i denne forordning eller anden relevant EU-lovgivning.

6. Uden at det berører national lovgivning eller EU-lovgivning, må en myndighed, en enhed eller en fysisk person, der modtager oplysninger i henhold til denne forordning, ikke anvende dem til andre formål end at udføre sine opgaver i henhold til denne forordning.

7. ACER udsteder senest den **13. juni 2025** efter høring af ENISA, alle kompetente myndigheder, ENTSO for elektricitet og EU-DSO-enheden retningslinjer vedrørende mekanismer til udveksling af oplysninger for alle enheder, der er opført i artikel 2, stk. 1, navnlig påtænkte kommunikationsstrømme, og metoder til anonymisering og aggregering af oplysninger med henblik på gennemførelsen af nærværende artikel.

8. Oplysninger, der er fortrolige i henhold til EU-bestemmelser eller nationale regler, udveksles kun med Kommissionen og andre relevante myndigheder, hvis en sådan udveksling er nødvendig for anvendelsen af denne forordning. De udvekslede oplysninger begrænses til, hvad der er nødvendigt og forholdsmæssigt under hensyntagen til formålet med udvekslingen. I udvekslingen af oplysninger sikres oplysningernes fortrolighed, og sikkerheden og kommercielle interesser hos enheder med kritisk indvirkning eller stor indvirkning beskyttes.

KAPITEL VIII

AFSLUTTENDE BESTEMMELSER

Artikel 48

Midlertidige bestemmelser

1. Indtil de vilkår og betingelser eller metoder, der er omhandlet i artikel 6, stk. 2, eller de planer, der er omhandlet i artikel 6, stk. 3, er blevet godkendt, udarbejder ENTSO for elektricitet i samarbejde med EU DSO-enheden ikkebindende vejledning om følgende spørgsmål:

a) et foreløbigt indeks for indvirkning på cybersikkerheden i forbindelse med elektricitetsstrømme (»ECII«), jf. nærværende artikels stk. 2

b) en foreløbig liste over processer med stor indvirkning og kritisk indvirkning på EU-plan, jf. nærværende artikels stk. 4, og

c) en foreløbig liste over europæiske og internationale standarder og kontroller, der kræves i henhold til national lovgivning, og som er relevante for cybersikkerhedsmæssige aspekter af grænseoverskridende elektricitetsstrømme, jf. nærværende artikels stk. 6.

2. Senest den **13. oktober 2024** udarbejder ENTSO for elektricitet i samarbejde med EU DSO-enheden en anbefaling om et foreløbigt ECII. ENTSO for elektricitet meddeler i samarbejde med EU DSO-enheden de kompetente myndigheder det anbefalede foreløbige ECII.

3. Fire måneder efter modtagelsen af det anbefalede foreløbige ECII eller senest den **13. februar 2025** udpeger de kompetente myndigheder kandidater til enheder med stor indvirkning og kritisk indvirkning i deres medlemsstat på grundlag af det anbefalede ECII og udarbejder en foreløbig liste over enheder med stor indvirkning og kritisk indvirkning. Enheder med stor indvirkning eller kritisk indvirkning, der er opført på den foreløbige liste, kan frivilligt opfylde deres forpligtelser i henhold til denne forordning ud fra et forsigtighedsprincip. Senest den **13. marts 2025** underretter de kompetente myndigheder de enheder, der er opført på den foreløbige liste, om, at de er blevet udpeget som en enhed med stor indvirkning eller kritisk indvirkning.

4. Senest den **13. december 2024** udarbejder ENTSO for elektricitet i samarbejde med EU DSO-enheden en foreløbig liste over processer med stor indvirkning og kritisk indvirkning på EU-plan. De enheder, der underrettes i henhold til stk. 3, og som frivilligt beslutter at opfylde deres forpligtelser i henhold til denne forordning ud fra et forsigtighedsprincip, anvender den foreløbige liste over processer med stor indvirkning og kritisk indvirkning til at fastlægge de foreløbige områder med stor indvirkning og kritisk indvirkning og til at afgøre, hvilke aktiver der skal medtages i den første cybersikkerhedsrisikovurdering på enhedsniveau.

5. Senest den **13. September 2024** forelægger hver kompetent myndighed som omhandlet i artikel 4, stk. 1, ENTSO for elektricitet og EU DSO-enheden en liste over sin nationale lovgivning af relevans for cybersikkerhedsmæssige aspekter af grænseoverskridende elektricitetsstrømme.

6. Senest den **13. juni 2025** udarbejder ENTSO for elektricitet i samarbejde med EU DSO-enheden en foreløbig liste over europæiske og internationale standarder og kontroller, der kræves i henhold til national lovgivning, og som er relevante for cybersikkerhedsmæssige aspekter af grænseoverskridende elektricitetsstrømme, under hensyntagen til oplysningerne fra de kompetente myndigheder.

7. Den foreløbige liste over europæiske og internationale standarder og kontroller skal omfatte:

a) europæiske og internationale standarder og national lovgivning, der giver vejledning om metoder til cybersikkerhedsrisikostyring på enhedsniveau, og

b) cybersikkerhedskontroller, der svarer til de kontroller, der forventes at være en del af minimumscybersikkerhedskontrollen og den udvidede cybersikkerhedskontrol.

8. ENTSO for elektricitet og EU DSO-enheden tager hensyn til ENISA's og ACER's synspunkter i færdiggørelsen af den foreløbige liste over standarder. ENTSO for elektricitet og EU DSO-enheden offentliggør den foreløbige liste over europæiske og internationale standarder og kontroller på deres websteder.

9. ENTSO for elektricitet og EU DSO-enheden hører ENISA og ACER om forslag til ikkebindende vejledning i henhold til stk. 1.

10. Indtil minimumscybersikkerhedskontrollen og den udvidede cybersikkerhedskontrol er udviklet i henhold til artikel 29 og vedtaget i henhold til artikel 8, bestræber alle enheder, der er opført i artikel 2, stk. 1, sig på gradvist at anvende den ikkebindende vejledning, der er udarbejdet i henhold til stk. 1.

Artikel 49

Ikrafttræden

Denne forordning træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

Denne forordning er bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat.

Udfærdiget i Bruxelles, den 11. marts 2024.

På Kommissionens vegne
Ursula VON DER LEYEN
Formand