Den Europæiske Unions

Tidende

L 333

Dansk udgave

Retsforskrifter

65. årgang

27. december 2022

Indhold

[1] EØS-relevant tekst.

DA

De akter, hvis titel er trykt med magre typer, er løbende retsakter inden for landbrugspolitikken og har normalt en begrænset gyldighedsperiode.

Titlen på alle øvrige akter er trykt med fede typer efter en asterisk.

I

(Lovgivningsmæssige retsakter)

FORORDNINGER

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

(EØS-relevant tekst)

EUROPA-PARLAMENTET OG RÅDET FOR DEN EUROPÆISKE UNION HAR —

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

under henvisning til forslag fra Europa-Kommissionen,

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

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

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

efter den almindelige lovgivningsprocedure ([3]), og

ud fra følgende betragtninger:

(1) I den digitale tidsalder understøtter informations- og kommunikationsteknologi (IKT) komplekse systemer, der anvendes i forbindelse med hverdagsaktiviteter. Den holder vores økonomier i gang i centrale sektorer, herunder den finansielle sektor, og fremmer det indre markeds funktion. Øget digitalisering og indbyrdes forbundethed forstærker også IKT-risiko, der gør samfundet som helhed og især det finansielle system mere sårbart over for cybertrusler eller IKT-forstyrrelser. Universel brug af IKT-systemer og en høj grad af digitalisering og konnektivitet er i dag vigtige kendetegn ved alle aktiviteter i Unionens finansielle enheder, men der skal gøres mere ved deres digitale modstandsdygtighed, og den skal integreres i deres bredere operationelle rammer.

(2) Brugen af IKT har i de seneste årtier indtaget en så central rolle inden for levering af finansielle tjenesteydelser, at den i dag har fået kritisk betydning for driften af typiske daglige funktioner i alle finansielle enheder. Digitalisering omfatter nu f.eks. betalinger, som i stigende grad er gået fra kontanter og papirbaserede metoder til brugen af digitale løsninger, samt clearing og afvikling af værdipapirer, elektronisk og algoritmisk handel, låntagning og finansiering, peer-to-peer-finansiering, kreditvurdering, behandling af skadesanmeldelser og back office-funktioner. Forsikringssektoren har også forandret sig med brugen af IKT, fra fremkomsten af forsikringsformidlere, der tilbyder

([1]) EUT C 343 af 26.8.2021, s. 1.
([2]) EUT C 155 af 30.4.2021, s. 38.
([3]) Europa-Parlamentets holdning af 10.11.2022 (endnu ikke offentliggjort i EUT) og Rådets afgørelse af 28.11.2022.

deres tjenester online ved anvendelse af InsurTech, til digital tegning af forsikring. Finansiering er ikke kun blevet overvejende digital i hele sektoren, men digitalisering har også uddybet den indbyrdes forbundethed og afhængighed inden for den finansielle sektor og med og af tredjeparters infrastruktur og tredjepartsudbydere af tjenester.

(3) Det Europæiske Udvalg for Systemiske Risici (ESRB) bekræftede på ny i en rapport fra 2020 om systemiske cyberrisici, hvordan det eksisterende høje niveau af indbyrdes forbundethed blandt finansielle enheder, finansielle markeder og finansielle markedsinfrastrukturer, og navnlig deres IKT-systemers indbyrdes forbundethed, kan udgøre en systemisk sårbarhed, fordi lokaliserede cyberhændelser hurtigt kan sprede sig fra én af de ca. 22 000 finansielle enheder i Unionen til hele det finansielle system, uhindret af geografiske grænser. Alvorlige IKT-overtrædelser i den finansielle sektor har ikke kun virkninger for finansielle enheder isoleret set. De baner også vejen for udbredelsen af lokaliserede sårbarheder på tværs af de finansielle transmissionskanaler og udløser potentielt negative konsekvenser for stabiliteten i Unionens finansielle system såsom skabelse af likviditetsudstrømning og et generelt tab af tillid og tiltro til finansielle markeder.

(4) I de seneste år har politiske beslutningstagere, lovgivere og standardiseringsorganer på internationalt plan, EU-plan og nationalt plan sat fokus på IKT-risiko i et forsøg på at øge den digitale modstandsdygtighed, fastsætte standarder og koordinere det regulerings- og tilsynsmæssige arbejde. På internationalt plan sigter Baselkomitéen for Banktilsyn, Udvalget om Betalings- og Markedsinfrastrukturer, Rådet for Finansiel Stabilitet, the Financial Stability Institute samt G7 og G20 mod at udstyre kompetente myndigheder og markedsoperatører på tværs af forskellige jurisdiktioner med værktøjer, der skal styrke deres finansielle systemers modstandsdygtighed. Dette arbejde har også været drevet af behovet for at tage behørigt hensyn til IKT-risiko i forbindelse med et stærkt indbyrdes forbundet globalt finansielt system og for at tilstræbe større sammenhæng i relevant bedste praksis.

(5) Til trods for målrettede politiske og lovgivningsmæssige initiativer på EU-plan og nationalt plan udgør IKT-risiko fortsat en udfordring for den operationelle modstandsdygtighed, præstation og stabilitet i Unionens finansielle system. De reformer, der fulgte efter den finansielle krise i 2008 styrkede primært den finansielle modstandsdygtighed i Unionens finansielle sektor og sigtede mod at bevare Unionens konkurrenceevne og stabilitet set fra et økonomisk, tilsyns- og markedsadfærdsmæssigt perspektiv. Selv om IKT-sikkerhed og digital modstandsdygtighed er led i den operationelle risiko, har der været mindre fokus herpå i den reguleringsmæssige dagsorden efter den finansielle krise, og de er kun blevet udviklet på nogle områder inden for Unionens politik for finansielle tjenesteydelser og reguleringsmæssige rammer eller kun i nogle få medlemsstater.

(6) I Kommissionens meddelelse af 8. marts 2018 med titlen »Fintechhandlingsplan for en mere konkurrencedygtig og innovativ finanssektor i Europa« fremhævedes den afgørende betydning af at gøre Unionens finansielle sektor mere modstandsdygtig, herunder set fra et operationelt perspektiv, for at sikre dens teknologiske sikkerhed, og at den fungerer godt, at den hurtigt kan genoprettes efter IKT-overtrædelser og -hændelser, hvilket i sidste ende gør det muligt at udbyde finansielle tjenesteydelser på en effektiv og gnidningsfri måde i hele Unionen, herunder i situationer med stresspåvirkning, samtidig med at forbrugernes og markedets tiltro og tillid bevares.

(7) I april 2019 udsendte Den Europæiske Tilsynsmyndighed (Den Europæiske Banktilsynsmyndighed) (EBA), der er oprettet ved Europa-Parlamentets og Rådets forordning (EU) nr. 1093/2010 ([4]), Den Europæiske Tilsynsmyndighed (Den Europæiske Tilsynsmyndighed for Forsikrings- og Arbejdsmarkedspensionsordninger) (»EIOPA«), der er oprettet ved Europa-Parlamentets og Rådets forordning (EU) nr. 1094/2010 ([5]), og Den Europæiske Tilsynsmyndighed (Den Europæiske Værdipapir- og Markedstilsynsmyndighed) (»ESMA«), der er oprettet ved

([4]) Europa-Parlamentets og Rådets forordning (EU) nr. 1093/2010 af 24. november 2010 om oprettelse af en europæisk tilsynsmyndighed (Den Europæiske Banktilsynsmyndighed), om ændring af afgørelse nr. 716/2009/EF og om ophævelse af Kommissionens afgørelse 2009/78/EF (EUT L 331 af 15.12.2010, s. 12).

([5]) Europa-Parlamentets og Rådets forordning (EU) nr. 1094/2010 af 24. november 2010 om oprettelse af en europæisk tilsynsmyndighed (Den Europæiske Tilsynsmyndighed for Forsikrings- og Arbejdsmarkedspensionsordninger), om ændring af afgørelse 716/2009/EF og om ophævelse af Kommissionens afgørelse 2009/79/EF (EUT L 331 af 15.12.2010, s. 48).

Europa-Parlamentets og Rådets forordning (EU) nr. 1095/2010 ([6]), (samlet betegnet som »europæiske tilsynsmyndigheder« eller »ESA'er«) i fællesskab teknisk rådgivning, hvori de opfordrede til en sammenhængende tilgang til IKT-risiko inden for finansiering og henstillede til på en forholdsmæssigt afpasset måde at styrke den digitale operationelle modstandsdygtighed i sektoren for finansielle tjenesteydelser gennem et sektorspecifikt EU-initiativ.

(8) Unionens finansielle sektor er reguleret af et fælles regelsæt og underlagt et europæisk finanstilsynssystem. Ikke desto mindre er bestemmelserne om håndtering af digital operationel modstandsdygtighed og IKT-sikkerhed endnu ikke harmoniseret fuldt ud eller konsekvent, og det til trods for, at digital operationel modstandsdygtighed er afgørende for at sikre finansiel stabilitet og markedsintegritet i den digitale tidsalder og ikke er mindre vigtig end f.eks. fælles standarder for tilsyn og markedsadfærd. Det fælles regelsæt og tilsynssystemet bør derfor udvikles med henblik på også at omfatte digital operationel modstandsdygtighed ved at styrke mandatet for de kompetente myndigheder, så de får mulighed for at føre tilsyn med IKT-risikostyring i den finansielle sektor med henblik på at beskytte det indre markeds integritet og effektivitet og for at fremme, at det fungerer efter sin hensigt.

(9) Lovgivningsmæssige forskelle og uensartede nationale regulerings- eller tilsynsmæssige tilgange med hensyn til IKT-risiko udløser hindringer for et velfungerende indre marked for finansielle tjenesteydelser, som hæmmer en problemfri udøvelse af den frie etableringsret og af retten til fri udveksling af tjenesteydelser for finansielle enheder, som har aktiviteter på et grænseoverskridende grundlag. Konkurrencen mellem samme type af finansielle enheder, som har aktiviteter i forskellige medlemsstater, kan også blive fordrejet. Dette gælder navnlig for områder, hvor EU-harmonisering har været meget begrænset, såsom test af digital operationel modstandsdygtighed, eller ikkeeksisterende, såsom overvågning af IKT-tredjepartsrisici. Forskelle, der skyldes en påtænkt udvikling på nationalt plan, vil kunne udløse yderligere hindringer for et velfungerende indre marked til skade for markedsdeltagere og den finansielle stabilitet.

(10) Da bestemmelser vedrørende IKT-risiko kun delvis er blevet behandlet på EU-plan, er der på nuværende tidspunkt huller eller overlapninger på vigtige områder, f.eks. indberetning af IKT-relaterede hændelser og test af digital operationel modstandsdygtighed og uoverensstemmelser som følge af nye divergerende nationale regler eller omkostningsineffektiv anvendelse af overlappende regler. Dette er særligt skadeligt for en IKT-intensiv bruger som den finansielle sektor, da teknologiske risici er grænseoverskridende, og den finansielle sektor udbyder sine tjenesteydelser på et bredt grænseoverskridende grundlag inden for og uden for Unionen. Individuelle finansielle enheder, som har aktiviteter på et grænseoverskridende grundlag, eller som er indehavere af flere tilladelser (f.eks. kan én finansiel enhed have tilladelser til henholdsvis at udøve bankvirksomhed, udøve virksomhed som investeringsselskab og betalingsinstitut, som hver især er meddelt af en forskellig kompetent myndighed i en eller flere medlemsstater), står over for operationelle udfordringer i forbindelse med at imødegå IKT-risiko og afbøde negative virkninger af IKT-hændelser på egen hånd og på en sammenhængende omkostningseffektiv måde.

(11) Da det fælles regelsæt ikke er blevet ledsaget af en omfattende IKT-ramme eller ramme for operationel risiko, er der behov for yderligere harmonisering af centrale krav til digital operationel modstandsdygtighed for alle finansielle enheder. De IKT-kapaciteter og den samlede modstandsdygtighed, som finansielle enheder med udgangspunkt i disse centrale krav skal udvikle for at modstå operationelle driftstop, vil bidrage til at bevare stabiliteten og integriteten på Unionens finansielle markeder og dermed bidrage til at sikre et højt beskyttelsesniveau for investorer og forbrugere i Unionen. Da denne forordning har til formål at bidrage til et velfungerende indre marked, bør den bygge på bestemmelserne i artikel 114 i traktaten om Den Europæiske Unions funktionsmåde (TEUF) som fortolket i overensstemmelse med EU-Domstolens (Domstolens) faste praksis.

(12) Denne forordning har til formål at konsolidere og opgradere kravene til IKT-risiko som en del af kravene til operationel risiko, som hidtil er blevet behandlet separat i forskellige EU-retsakter. Disse retsakter omfattede hovedkategorierne af finansiel risiko (f.eks. kreditrisiko, markedsrisiko, modpartskreditrisiko og likviditetsrisiko, risiko forbundet med markedsadfærd), men på tidspunktet for deres vedtagelse tacklede de ikke alle de komponenter, der indgår i operationel modstandsdygtighed, på fyldestgørende vis. I reglerne om operationel risiko blev der, da de blev yderligere udviklet i de pågældende EU-retsakter, ofte foretrukket en traditionel kvantitativ tilgang til risikohåndtering (dvs. ved at fastsætte et kapitalkrav til at dække IKT-risiko) frem for målrettede kvalitative regler for beskyttelses-, detektions-, inddæmnings-, genopretnings- og reparationskapaciteter som værn mod IKT-relaterede hændelser eller for indberetningskapaciteter og digitale testkapaciteter. Disse retsakter skulle primært

([6]) Europa-Parlamentets og Rådets forordning (EU) nr. 1095/2010 af 24. november 2010 om oprettelse af en europæisk tilsynsmyndighed (Den Europæiske Værdipapir- og Markedstilsynsmyndighed), om ændring af afgørelse nr. 716/2009/EF og om ophævelse af Kommissionens afgørelse 2009/77/EF (EUT L 331 af 15.12.2010, s. 84).

omfatte og ajourføre væsentlige regler om tilsyn, markedsintegritet eller -adfærd. Ved at konsolidere og opgradere de forskellige regler om IKT-risici bør alle bestemmelser om digital risiko i den finansielle sektor for første gang blive samlet på en konsekvent måde i én enkelt lovgivningsmæssig retsakt. Denne forordning udfylder derfor hullerne eller afhjælper uoverensstemmelserne i nogle af de nævnte tidligere retsakter, herunder med hensyn til den heri anvendte terminologi, og henviser eksplicit til IKT-risiko gennem målrettede regler om kapaciteter til IKT-risikostyring, indberetning af hændelser, test af operationel modstandsdygtighed, samt overvågning af IKT-tredjepartsrisiko. Denne forordning bør således også øge bevidstheden om IKT-risiko og anerkende, at IKT-hændelser og manglende operationel modstandsdygtighed potentielt kan udgøre en fare for finansielle enheders soliditet.

(13) Finansielle enheder bør følge samme tilgang og samme principbaserede regler ved behandling af IKT-risiko under hensyntagen til deres størrelse og samlede risikoprofil samt karakteren, omfanget og kompleksiteten af deres tjenester, aktiviteter og operationer. Konsekvens bidrager til at øge tilliden til det finansielle system og bevare dets stabilitet, navnlig i tider med høj afhængighed af IKT-systemer, platforme og infrastrukturer, hvilket medfører øgede digitale risici. Overholdelse af en grundlæggende cyberhygiejne bør også hindre, at økonomien påføres store omkostninger ved at minimere virkningerne af og omkostningerne i forbindelse med IKT-forstyrrelser.

(14) En forordning hjælper med at mindske reguleringsmæssig kompleksitet, fremmer tilsynsmæssig konvergens og øger retssikkerheden og bidrager også til at begrænse overholdelsesomkostningerne, navnlig for finansielle enheder, der har aktiviteter på tværs af grænserne, og til at mindske konkurrenceforvridninger. Valget af en forordning med henblik på oprettelse af en fælles ramme for digital operationel modstandsdygtighed i finansielle enheder er derfor den mest hensigtsmæssige metode til at sikre en homogen og sammenhængende anvendelse af alle de komponenter, der indgår i IKT-risikostyring i Unionens finansielle sektor.

(15) Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 ([7]) var den første horisontale ramme for cybersikkerhed, der blev vedtaget på EU-plan, som også finder anvendelse på tre typer af finansielle enheder, nemlig kreditinstitutter, markedspladser og centrale modparter. Eftersom direktiv (EU) 2016/1148 fastsatte en mekanisme til identifikation på nationalt plan af operatører af væsentlige tjenester, var det imidlertid kun visse kreditinstitutter, markedspladser og centrale modparter, der blev udpeget af medlemsstaterne, og som blev medtaget under dets anvendelsesområde i praksis, og som derfor skal overholde de heri fastsatte krav til IKT-risici og indberetning af hændelser. Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 ([8]) fastsætter et ensartet kriterium til bestemmelse af de enheder, der er omfattet af dets anvendelsesområde (størrelsesloftet), samtidig med at anvendelsesområdet stadig omfatter de tre typer finansielle enheder.

(16) Da denne forordning øger niveauet af harmonisering af de forskellige komponenter, der indgår i digital modstandsdygtighed, ved at indføre krav til IKT-risikostyring og indberetning af IKT-relaterede hændelser, som er strengere i forhold til de krav, der er fastlagt i den nuværende EU-ret om finansielle tjenesteydelser, udgør dette højere niveau imidlertid ligeledes en øget harmonisering i sammenligning med de krav, der er fastlagt i direktiv (EU) 2022/2555. Derfor udgør denne forordning *lex specialis* i forhold til direktiv (EU) 2022/2555. Det er samtidig yderst vigtigt at bevare en tæt forbindelse mellem cybersikkerhedsrammen for den finansielle sektor og Unionens horisontale ramme for cybersikkerhed, som i øjeblikket fastsat i direktiv (EU) 2022/2555, for at sikre sammenhæng med de strategier om cybersikkerhed, som medlemsstaterne har vedtaget, og for at give de finansielle tilsynsmyndigheder mulighed for at få kendskab til cyberhændelser, der har virkninger for de øvrige sektorer, som er omfattet af nævnte direktiv.

([7]) Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (EUT L 194 af 19.7.2016, s. 1).

([8]) 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-direktiv) (se side 80 i denne EUT).

(17) I overensstemmelse med artikel 4, stk. 2, i traktaten om Den Europæiske Union og med forbehold af Domstolens prøvelse bør denne forordning ikke berøre medlemsstaternes ansvar for så vidt angår centrale statslige funktioner vedrørende offentlig sikkerhed, forsvar og beskyttelse af den nationale sikkerhed f.eks. i forbindelse med forelæggelse af oplysninger, der ville være i strid med beskyttelsen af den nationale sikkerhed.

(18) For at muliggøre tværsektoriel læring og for effektivt at udnytte andre sektorers erfaringer med håndtering af cybertrusler bør de finansielle enheder, der er omhandlet i direktiv (EU) 2022/2555, fortsat indgå i nævnte direktivs »økosystem« (f.eks. samarbejdsgruppen og enheder, der håndterer IT-sikkerhedshændelser (CSIRT'er)). ESA'er og nationale kompetente myndigheder bør have mulighed for at deltage i de strategiske politiske drøftelser og det tekniske arbejde i samarbejdsgruppen i henhold til nævnte direktiv og for at udveksle oplysninger og samarbejde yderligere med de centrale kontaktpunkter, der er udpeget eller oprettet i overensstemmelse med nævnte direktiv. De kompetente myndigheder i henhold til denne forordning bør også rådføre sig med og samarbejde med CSIRT'erne. De kompetente myndigheder bør også kunne anmode om teknisk rådgivning hos de kompetente myndigheder, der er udpeget eller oprettet i overensstemmelse med henhold til direktiv (EU) 2022/2555, og etablere samarbejdsordninger, der har til formål at sikre effektive og hurtigt reagerende koordineringsmekanismer.

(19) I betragtning af de stærke indbyrdes forbindelser mellem finansielle enheders digitale modstandsdygtighed og fysiske modstandsdygtighed er det nødvendigt med en sammenhængende tilgang i denne forordning og i Europa-Parlamentets og Rådets direktiv (EU) 2022/2557 ([9]) til kritiske enheders modstandsdygtighed. Eftersom finansielle enheders fysiske modstandsdygtighed behandles omfattende af forpligtelserne med hensyn til IKT-risikostyring og IKT-indberetning i denne forordning, bør forpligtelserne i kapitel III og IV i direktiv (EU) 2022/2557 ikke finde anvendelse på finansielle enheder, der er omfattet af nævnte direktivs anvendelsesområde.

(20) Udbydere af cloudcomputingtjenester er én kategori af digital infrastruktur, som er omfattet af direktiv (EU) 2022/2555 Den EU-tilsynsramme (»tilsynsramme«), der fastlægges ved denne forordning, finder anvendelse på alle kritiske tredjepartsudbydere af IKT-tjenester, herunder udbydere af cloudcomputingtjenester, når de udbyder IKT-tjenester til finansielle enheder, og bør betragtes som et supplement til tilsynet gennemført i henhold til direktiv (EU) 2022/2555 Derudover bør den tilsynsramme, der fastlægges ved denne forordning, omfatte udbydere af cloudcomputingtjenester i fravær af en horisontal EU-ramme om oprettelse af en digital tilsynsmyndighed.

(21) For at bevare den fulde kontrol med IKT-risiko er det nødvendigt, at finansielle enheder har omfattende kapaciteter, der muliggør en stærk og effektiv IKT-risikostyring, og specifikke mekanismer og politikker med henblik på håndtering af alle IKT-relaterede hændelser og indberetning af større IKT-relaterede hændelser. På samme måde bør finansielle enheder indføre politikker for test af IKT-systemer, -kontroller og -processer samt for håndtering af IKT-tredjepartsrisici. Standarden for digital operationel modstandsdygtighed for finansielle enheder bør højnes, samtidig med at der også skabes mulighed for en forholdsmæssigt afpasset anvendelse af krav til visse finansielle enheder, især mikrovirksomheder, og finansielle enheder, der er omfattet af en forenklet ramme for IKT-risikostyring. For at muliggøre et effektivt tilsyn med arbejdsmarkedsrelaterede pensionskasser, der er forholdsmæssigt og imødekommer behovet for at mindske de administrative byrder for de kompetente myndigheder, bør de relevante nationale tilsynsmæssige rammer med hensyn til sådanne finansielle enheder tage højde for deres størrelse og samlede risikoprofil samt karakteren, omfanget og kompleksiteten af deres tjenester, aktiviteter og operationer, selv hvis de relevante tærskler i artikel 5 i Europa-Parlamentets og Rådets direktiv (EU) 2016/2341 ([10]) overskrides. Navnlig bør tilsynsaktiviteterne primært fokusere på behovet for at imødegå alvorlige risici i forbindelse med IKT-risikostyring i en bestemt enhed.

([9]) Europa-Parlamentets og Rådets direktiv (EU) 2022/2557 af 14. december 2022 om kritiske enheders modstandsdygtighed og om ophævelse af Rådets direktiv 2008/114/EF (se side 164 i denne EUT).

([10]) Europa-Parlamentets og Rådets direktiv (EU) 2016/2341 af 14. december 2016 om arbejdsmarkedsrelaterede pensionskassers (IORP'ers) aktiviteter og tilsynet hermed (EUT L 354 af 23.12.2016, s. 37).

Kompetente myndigheder bør også fastholde en årvågen, men forholdsmæssig, tilgang til tilsynet med arbejdsmarkedsrelaterede pensionskasser, som i overensstemmelse med artikel 31 i direktiv (EU) 2016/2341 outsourcer en betydelig del af deres centrale forretningsområder såsom kapitalforvaltning, aktuarmæssig beregning, regnskab og dataforvaltning til tjenesteydere.

(22) Tærskler og klassificeringssystemer vedrørende indberetning af IKT-relaterede hændelser varierer væsentligt på nationalt plan. Der kan sandsynligvis opnås enighed gennem det relevante arbejde, der udføres af Den Europæiske Unions Agentur for Cybersikkerhed (ENISA), der er oprettet ved Europa-Parlamentets og Rådets forordning (EU) 2019/881 ([11]), og samarbejdsgruppen i henhold til direktiv (EU) 2022/2555, men der findes stadig, eller der kan opstå divergerende tilgange til fastsættelse af tærskler og anvendelse af klassificeringssystemer for de resterende finansielle enheder. På grund af disse forskelle er der flere krav, som de finansielle enheder skal overholde, navnlig når de har aktiviteter på tværs af flere medlemsstater, og når de er del af en finansiel koncern. Disse forskelle kan desuden potentielt hindre indførelsen af yderligere ensartede eller centraliserede EU-mekanismer, der fremskynder indberetningsprocessen og understøtter en hurtig og problemfri informationsudveksling mellem kompetente myndigheder, hvilket er yderst vigtigt for imødegåelsen af IKT-risikoen i tilfælde af storstilede angreb med potentielle systemiske konsekvenser til følge.

(23) For at mindske den administrative byrde og mulige overlappende indberetningsforpligtelser for visse finansielle enheder bør kravet om indberetning af hændelser i henhold til Europa-Parlamentets og Rådets direktiv (EU) 2015/2366 ([12]) ikke længere finde anvendelse på betalingstjenesteudbydere, der er omfattet af denne forordnings anvendelsesområde. Derfor bør kreditinstitutter, e-pengeinstitutter, betalingsinstitutter og kontooplysningstjenesteudbydere som omhandlet i nævnte direktivs artikel 33, stk. 1, fra datoen for denne forordnings anvendelse i henhold til denne forordning indberette alle de operationelle eller sikkerhedsmæssige betalingsrelaterede hændelser, som tidligere blev indberettet i henhold til nævnte direktiv, uanset om sådanne hændelser er IKT-relaterede.

(24) For at sætte kompetente myndigheder i stand til at opfylde tilsynsmæssige roller ved at opnå et fuldstændigt overblik over IKT-relaterede hændelsers karakter, frekvens, betydning og virkninger og for at styrke informationsudvekslingen mellem relevante offentlige myndigheder, herunder retshåndhævende myndigheder og afviklingsmyndigheder, bør denne forordning fastlægge en robust ordning for indberetning af IKT-relaterede hændelser, hvorved de relevante krav afhjælper nuværende mangler i retten om finansielle tjenesteydelser og fjerne eksisterende overlapninger og dobbeltbestemmelser for at mindske omkostningerne. Det er afgørende at harmonisere ordningen for indberetning af IKT-relaterede hændelser ved at kræve, at alle finansielle enheder indberetter til deres kompetente myndigheder gennem en enkelt strømlinet ramme som fastsat i denne forordning. ESA'erne bør desuden tillægges beføjelse til yderligere at præcisere relevante elementer vedrørende rammen for indberetning af IKT-relaterede hændelser, f.eks. klassificeringssystemer, tidsrammer, datasæt, modeller og gældende tærskler. For at sikre fuld overensstemmelse med direktiv (EU) 2022/2555 bør de finansielle enheder have mulighed for på frivillig basis at underrette den relevante kompetente myndighed om væsentlige cybertrusler, når de anser cybertruslen for at være relevant for det finansielle system, tjenestebrugere eller kunder.

(25) Krav til test af digital operationel modstandsdygtighed er blevet udviklet i visse finansielle delsektorer og udgør rammer, der ikke altid er fuldt afstemt. Dette fører potentielt til en fordobling af omkostninger for grænseoverskridende finansielle enheder, og gør den gensidige anerkendelse af resultaterne af test af digital operationel modstandsdygtighed kompleks, hvilket igen kan fragmentere det indre marked.

([11]) 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).

([12]) Europa-Parlamentets og Rådets direktiv (EU) 2015/2366 af 25. november 2015 om betalingstjenester i det indre marked, og om ændring af direktiv 2002/65/EF, 2009/110/EF og 2013/36/EU og forordning (EU) nr. 1093/2010 og om ophævelse af direktiv 2007/64/EF (EUT L 337 af 23.12.2015, s. 35).

(26) Når IKT-test ikke er påkrævet, vil sårbarheder ikke blive detekteret, hvilket medfører, at en finansiel enhed udsættes for en IKT-risiko, og i sidste ende skaber en højere risiko for stabiliteten og integriteten i den finansielle sektor. Uden en indsats på EU-plan vil test af digital operationel modstandsdygtighed fortsat være inkonsekvent og mangle en ordning for gensidig anerkendelse af IKT-testresultater på tværs af de forskellige jurisdiktioner. Da det er usandsynligt, at andre finansielle delsektorer vil indgå sådanne testordninger i et meningsfuldt omfang, vil de desuden gå glip af de potentielle fordele ved en testramme med hensyn til detektion af IKT-sårbarheder og -risici, og test af forsvarskapaciteter og driftsstabilitet, der bidrager til at øge tiltroen blandt kunder, leverandører og forretningspartnere. For at afhjælpe disse overlapninger, forskelle og huller er det nødvendigt at fastlægge regler for en koordineret testordning og dermed lette den gensidige anerkendelse af avancerede test for finansielle enheder, der opfylder kriterierne i denne forordning.

(27) Finansielle enheders afhængighed af brugen af IKT-tjenester skyldes delvist deres behov for at tilpasse sig en ny konkurrencepræget digital og global økonomi og for at fremme deres forretningseffektivitet og imødekomme forbrugerefterspørgslen. Karakteren og omfanget af denne afhængighed har løbende udviklet sig gennem de senere år og har drevet omkostningsreduktionen inden for finansiel formidling, muliggjort ekspansion og skalerbarhed af virksomheder i forbindelse med udrulningen af finansielle aktiviteter og stillet en bred vifte af IKT-værktøjer til styring af komplekse interne processer til rådighed.

(28) Den vidtgående anvendelse af IKT-tjenester dokumenteres ved komplekse kontraktlige ordninger, i forbindelse med hvilke finansielle enheder ofte støder på vanskeligheder med at forhandle kontraktvilkår, der er tilpasset til de tilsynsmæssige standarder eller andre forskriftsmæssige krav, som de er omfattet af, eller på anden måde med at håndhæve specifikke rettigheder, f.eks. adgangs- eller revisionsrettigheder, selv hvis sidstnævnte er fastsat i deres kontraktlige ordninger. Mange af disse kontraktlige ordninger indeholder desuden ikke tilstrækkelige garantier for en fuldgyldig overvågning af underentrepriseforhold hvorved den finansielle enhed berøves sin evne til at vurdere de dertil knyttede risici. Dertil kommer, at sådanne kontraktlige ordninger ikke altid i tilstrækkeligt omfang tager højde for individuelle eller specifikke behov blandt aktører i den finansielle sektor, da tredjepartsudbydere af IKT-tjenester ofte udbyder standardiserede tjenester til forskellige kundetyper.

(29) Selv om EU-retten vedrørende finansielle tjenesteydelser indeholder visse generelle regler om outsourcing, er overvågningen af den kontraktlige dimension ikke fuldt ud forankret i EU-retten. I mangel af klare og skræddersyede EU-standarder, som finder anvendelse på de kontraktlige ordninger, der indgås med tredjepartsudbydere af IKT-tjenester, er der ikke på fyldestgørende vis taget højde for den eksterne kilde til IKT-risiko. Derfor er det nødvendigt at fastsætte visse centrale principper, der skal fungere som rettesnor for finansielle enheders styring af IKT-tredjepartsrisici, som er af særlig betydning, når finansielle enheder benytter tredjepartsudbydere af IKT-tjenester til at støtte deres kritiske eller vigtige funktioner. Disse principper bør ledsages af et sæt centrale kontraktlige rettigheder i forhold til flere elementer af opfyldelse og opsigelse af kontraktlige ordninger med henblik på at yde visse minimumsgarantier for at styrke finansielle enheders evne til effektivt at overvåge alle IKT-risici, der opstår hos tredjepartstjenesteudbydere. Disse principper supplerer den sektorspecifikke ret, der finder anvendelse på outsourcing.

(30) I dag er det tydeligt, at der er en vis mangel på homogenitet og konvergens i forbindelse med overvågningen af IKT-tredjepartsrisiko og afhængighed af IKT-tredjeparter. På trods af bestræbelser på at tackle outsourcing såsom EBA's retningslinjer om outsourcing fra 2019 og ESMA's retningslinjer for outsourcing til udbydere af cloudtjenester fra 2021, tages der i EU-retten ikke i tilstrækkelig grad højde for den bredere problematik, der er forbundet med imødegåelse af systemisk risiko, som kan udløses af den finansielle sektors eksponering for et begrænset antal kritiske tredjepartsudbydere af IKT-tjenester. Manglen på regler på EU-plan forværres af manglen på nationale regler om mandater og værktøjer, som giver nationale tilsynsmyndigheder mulighed for at opnå en god forståelse for afhængigheden af IKT-tredjeparter og foretage en tilstrækkelig overvågning af risici, der opstår som følge af koncentrationer af afhængighed af IKT-tredjeparter.

(31) I betragtning af den potentielle systemiske risiko, som øget anvendelse af outsourcing og koncentration af IKT-tredjepartsafhængighed medfører, og henset til de nationale mekanismers utilstrækkelighed med hensyn til at give finansielle tilsynsmyndigheder tilstrækkelige værktøjer til at kvantificere, kvalificere og afhjælpe konsekvenserne af IKT-risiko, der opstår hos kritiske tredjepartsudbydere af IKT-tjenester, er det nødvendigt at fastlægge en passende tilsynsramme, som gør det muligt at foretage løbende overvågning af aktiviteter hos tredjepartsudbydere af IKT-tjenester, som er kritiske tredjepartsudbydere af IKT-tjenester til finansielle enheder, samtidig med at det sikres, at fortroligheden og sikkerheden for andre kunder end finansielle enheder bevares. Selv om koncernintern levering af IKT-tjenester indebærer specifikke risici og fordele, bør denne ikke automatisk anses for at være mindre risikofyldt end levering af IKT-tjenester fra udbydere uden for en finansiel koncern, og den bør derfor være omfattet af den samme reguleringsmæssige ramme. Når IKT-tjenester leveres inden for samme finansielle koncern, kan finansielle enheder imidlertid have en højere grad af kontrol med koncerninterne udbydere, hvilket der bør tages hensyn til i den samlede risikovurdering.

(32) I takt med at IKT-risiko bliver mere og mere komplekse og sofistikerede, afhænger gode foranstaltninger til detektion og forebyggelse af IKT-risiko i høj grad af regelmæssig udveksling mellem finansielle enheder af trussels- og sårbarhedsefterretninger. Informationsudveksling bidrager til at skabe øget bevidsthed om cybertrusler. Dette styrker også finansielle enheders evne til at forhindre cybertrusler i at blive faktiske IKT-relaterede hændelser og sætter finansielle enheder i stand til mere effektivt at inddæmme virkningen af IKT-relaterede hændelser og til at foretage hurtigere genopretning. I fravær af vejledning på EU-plan synes flere faktorer at have hæmmet en sådan udveksling af efterretninger, især usikkerhed omkring foreneligheden med databeskyttelsesregler, antitrustregler og regler om ansvar.

(33) Dertil kommer, at tvivl med hensyn til, hvilken type oplysninger der kan udveksles med en anden markedsdeltager eller med ikketilsynsmyndigheder (f.eks. ENISA, med henblik på analytisk input, eller Europol, med henblik på retshåndhævelse), medfører, at nyttige oplysninger tilbageholdes. Omfanget og kvaliteten af informationsudvekslingen er derfor fortsat begrænset og fragmenteret, da de relevante udvekslinger mest er lokale (gennem nationale initiativer), og da der på EU-plan ikke findes nogen konsekvente ordninger for informationsudveksling, som er skræddersyet til behovene i et integreret finansielt system. Det er derfor vigtigt at styrke disse kommunikationskanaler.

(34) Finansielle enheder bør tilskyndes til indbyrdes at udveksle oplysninger og efterretninger om cybertrusler og til i fællesskab at udnytte deres individuelle viden og praktiske erfaring på strategisk, taktisk og operationelt plan til at styrke deres kapaciteter til i tilstrækkeligt omfang at vurdere, overvåge, forsvare sig mod og sætte ind over for cybertrusler ved at deltage i ordninger for informationsudveksling. Det er derfor nødvendigt at muliggøre indførelsen på EU-plan af mekanismer med henblik på frivillige ordninger for informationsudveksling, som, når de gennemføres i pålidelige miljøer, vil hjælpe den finansielle sektor til at forebygge og i fællesskab sætte ind over for cybertrusler ved hurtigt at begrænse spredningen af IKT-risici og hindre potentiel afsmitning på tværs af de finansielle kanaler. Disse mekanismer bør overholde de gældende regler i Unionens konkurrenceret, der fremgår af Kommissionens meddelelse af 14. januar 2011 med titlen »Retningslinjer for anvendelsen af artikel 101 i traktaten om Den Europæiske Unions funktionsmåde på horisontale samarbejdsaftaler«, og Unionens databeskyttelsesregler, navnlig Europa-Parlamentets og Rådets forordning (EU) 2016/679 ([13]). De bør fungere på grundlag af et eller flere af de retsgrundlag, der er fastsat i artikel 6 i nævnte forordning, f.eks. i forbindelse med behandling af personoplysninger, som er nødvendig for, at den dataansvarlige eller tredjemand kan forfølge en legitim interesse, jf. nævnte forordnings artikel 6, stk. 1, litra f), samt i forbindelse med behandling af personoplysninger, der er nødvendig for at overholde en retlig forpligtelse, som påhviler den dataansvarlige, og som er nødvendig af hensyn til udførelse af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt, jf. henholdsvis artikel 6, stk. 1, litra c) og e), i nævnte forordning.

([13]) 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).

(35) For at opretholde et højt niveau af digital operationel modstandsdygtighed i hele den finansielle sektor og samtidig holde trit med den teknologiske udvikling bør denne forordning imødegå risici, der hidrører fra alle typer IKT-tjenester. Med henblik herpå bør definitionen af IKT-tjenester i forbindelse med denne forordning forstås bredt og omfatte digitale tjenester og datatjenester, der løbende leveres gennem IKT-systemer til én eller flere interne eller eksterne brugere. Denne definition bør f.eks. omfatte såkaldte »over the top«-tjenester, som falder ind under kategorien elektroniske kommunikationstjenester. Den bør kun udelukke den begrænsede kategori af traditionelle analoge telefonitjenester, der kan betegnes som offentlige telefonnettjenester med omkobling (PSTN), fastnettjenester, traditionel telefoni (POTS) eller fastnettelefontjenester.

(36) Til trods for den brede dækning, der påtænkes i denne forordning, bør der ved anvendelse af reglerne om digital operationel modstandsdygtighed tages hensyn til de væsentlige forskelle mellem finansielle enheder med hensyn til deres størrelse og samlede risikoprofil. Som et overordnet princip bør de finansielle enheder, når de fordeler ressourcer og kapaciteter til gennemførelsen af rammen for IKT-risikostyring, nøje afveje deres IKT-relaterede behov i forhold til deres størrelse og samlede risikoprofil og karakteren, omfanget og kompleksiteten af deres tjenester, aktiviteter og operationer, mens de kompetente myndigheder fortsat bør vurdere og gennemgå tilgangen til en sådan fordeling.

(37) Kontooplysningstjenesteudbydere som omhandlet i artikel 33, stk. 1, i direktiv (EU) 2015/2366 er udtrykkeligt omfattet af nærværende forordnings anvendelsesområde under hensyntagen til deres aktiviteters særlige karakter og de dermed forbundne risici. Desuden er e-pengeinstitutter og betalingsinstitutter, der er undtaget i henhold til artikel 9, stk. 1, i Europa-Parlamentets og Rådets direktiv 2009/110/EF ([14]) og artikel 32, stk. 1, i direktiv (EU) 2015/2366, omfattet af nærværende forordnings anvendelsesområde, selv om de ikke er blevet meddelt tilladelse i henhold til direktiv 2009/110/EF til at udstede elektroniske penge, eller de ikke er blevet meddelt tilladelse i henhold til direktiv (EU) 2015/2366 til at udbyde og gennemføre betalingstjenester. Postgirokontorer som omhandlet i artikel 2, stk. 5, nr. 3), i Europa-Parlamentets og Rådets direktiv 2013/36/EU ([15]) er imidlertid ikke omfattet af nærværende forordnings anvendelsesområde. Den kompetente myndighed for betalingsinstitutter, der er undtaget i henhold til direktiv (EU) 2015/2366, e-pengeinstitutter, der er undtaget i henhold til direktiv 2009/110/EF, og kontooplysningstjenesteudbydere, jf. artikel 33, stk. 1, i direktiv (EU) 2015/2366, bør være den kompetente myndighed, der er udpeget i henhold til artikel 22 i direktiv (EU) 2015/2366.

(38) Da større finansielle enheder kan have adgang til flere ressourcer og hurtigt kan afsætte midler til at udvikle forvaltningsstrukturer og indføre forskellige virksomhedsstrategier, er det kun finansielle enheder, der ikke er mikrovirksomheder i denne forordnings forstand, som skal pålægges at indføre mere komplekse forvaltningsordninger. Sådanne enheder er bedre rustet til at indføre særlige ledelsesfunktioner med henblik på tilsynsordninger med tredjepartsudbydere af IKT-tjenester eller til at varetage krisestyring, til at tilrettelægge deres egen IKT-risikostyring efter modellen med tre forsvarslinjer eller til at etablere en intern model for risikostyring og kontrol og til at underkaste deres ramme for IKT-risikostyring intern revision.

(39) Nogle finansielle enheder drager fordel af undtagelser eller er underlagt en meget lempelig reguleringsmæssig ramme i henhold til den relevante sektorspecifikke EU-ret. Sådanne finansielle enheder omfatter forvaltere af alternative investeringsfonde som omhandlet i artikel 3, stk. 2, i Europa-Parlamentets og Rådets direktiv 2011/61/EU ([16]), forsikrings- og genforsikringsselskaber som omhandlet i artikel 4 i Europa-Parlamentets og Rådets direktiv 2009/138/EF ([17]) og arbejdsmarkedsrelaterede pensionskasser, der forvalter pensionsordninger, som tilsammen ikke

([14]) Europa-Parlamentets og Rådets direktiv 2009/110/EF af 16. september 2009 om adgang til at optage og udøve virksomhed som udsteder af elektroniske penge og tilsyn med en sådan virksomhed, ændring af direktiv 2005/60/EF og 2006/48/EF og ophævelse af direktiv 2000/46/EF (EUT L 267 af 10.10.2009, s. 7).

([15]) Europa-Parlamentets og Rådets direktiv 2013/36/EU af 26. juni 2013 om adgang til at udøve virksomhed som kreditinstitut og om tilsyn med kreditinstitutter, om ændring af direktiv 2002/87/EF og om ophævelse af direktiv 2006/48/EF og 2006/49/EF (EUT L 176 af 27.6.2013, s. 338).

([16]) Europa-Parlamentets og Rådets direktiv 2011/61/EU af 8. juni 2011 om forvaltere af alternative investeringsfonde og om ændring af direktiv 2003/41/EF og 2009/65/EF samt forordning (EF) nr. 1060/2009 og (EU) nr. 1095/2010 (EUT L 174 af 1.7.2011, s. 1).

([17]) Europa-Parlamentets og Rådets direktiv 2009/138/EF af 25. november 2009 om adgang til og udøvelse af forsikrings- og genforsikringsvirksomhed (Solvens II) (EUT L 335 af 17.12.2009, s. 1).

har mere end 15 medlemmer i alt. I lyset af disse undtagelser ville det ikke være rimeligt at medtage sådanne finansielle enheder i denne forordnings anvendelsesområde. Desuden anerkender denne forordning de særlige forhold, der gør sig gældende for markedsstrukturen for forsikringsformidling, med det resultat, at forsikringsformidlere, genforsikringsformidlere og accessoriske forsikringsformidlere, der kan betegnes som mikrovirksomheder eller som små eller mellemstore virksomheder, ikke bør være omfattet af denne forordning.

(40) Da enheder, der er omhandlet i artikel 2, stk. 5, nr. 4)-23), i direktiv 2013/36/EU, er udelukket fra nævnte direktivs anvendelsesområde, bør medlemsstaterne derfor kunne vælge at undtage sådanne enheder, der er beliggende på deres respektive områder, fra denne forordnings anvendelse.

(41) For at tilpasse denne forordning til anvendelsesområdet for Europa-Parlamentets og Rådets direktiv 2014/65/EU ([18]) bør de fysiske og juridiske personer, der er omhandlet i artikel 2 og 3 i nævnte direktiv, og som må yde investeringsservice uden at skulle indhente tilladelse i henhold til direktiv 2014/65/EU, ligeledes udelukkes fra denne forordnings anvendelsesområde. I henhold til artikel 2 i direktiv 2014/65/EU er enheder, der betragtes som finansielle enheder med henblik på denne forordning, f.eks. værdipapircentraler, institutter for kollektiv investering eller forsikrings- og genforsikringsselskaber, dog også undtaget fra nævnte direktivs anvendelsesområde. Undtagelsen fra denne forordnings anvendelsesområde for de personer og enheder, der er omhandlet i artikel 2 og 3 i nævnte direktiv, bør ikke omfatte disse værdipapircentraler, institutter for kollektiv investering eller forsikrings- og genforsikringsselskaber.

(42) I henhold til sektorspecifik EU-ret er nogle finansielle enheder underlagt lempeligere krav eller undtagelser som følge af deres størrelse eller de tjenester, de leverer. Denne kategori af finansielle enheder omfatter små og ikke indbyrdes forbundne investeringsselskaber, små arbejdsmarkedsrelaterede pensionskasser, som den pågældende medlemsstat kan udelukke fra anvendelsesområdet for direktiv (EU) 2016/2341 på de betingelser, der er fastsat i artikel 5 i nævnte direktiv, og som forvalter pensionsordninger, som tilsammen ikke har mere end 100 medlemmer i alt, samt institutter, der er fritaget i henhold til direktiv 2013/36/EU. I overensstemmelse med proportionalitetsprincippet og for at bevare ånden i den sektorspecifikke EU-ret er det derfor også hensigtsmæssigt at underlægge disse finansielle enheder en forenklet ramme for IKT-risikostyring i henhold til denne forordning. Den forholdsmæssige karakter af rammen for IKT-risikostyring, der omfatter disse finansielle enheder, bør ikke ændres af de reguleringsmæssige tekniske standarder, der skal udvikles af ESA'erne. I overensstemmelse med proportionalitetsprincippet er det desuden hensigtsmæssigt også at underlægge betalingsinstitutter som omhandlet i artikel 32, stk. 1, i direktiv (EU) 2015/2366 og e-pengeinstitutter som omhandlet i artikel 9 i direktiv 2009/110/EF, der er undtaget i overensstemmelse med national ret, der gennemfører disse EU-retsakter, en forenklet ramme for IKT-risikostyring i henhold til denne forordning, hvorimod betalingsinstitutter og e-pengeinstitutter, som ikke er blevet undtaget i overensstemmelse med deres respektive nationale ret, der gennemfører sektorspecifik EU-ret, bør overholde den generelle ramme, der er fastsat ved denne forordning.

(43) Tilsvarende bør finansielle enheder, der betragtes som mikrovirksomheder eller er underlagt den forenklede ramme for IKT-risikostyring i henhold til denne forordning, ikke være forpligtet til at oprette en overvågningsfunktion for deres ordninger indgået med tredjepartsudbydere af IKT-tjenester vedrørende brugen af IKT-tjenester eller at udpege et medlem af den øverste ledelse som tilsynsansvarlig for den dermed forbundne risikoeksponering og relevante dokumentation, at overdrage ansvaret for styring af og tilsyn med IKT-risiko til en kontrolfunktion og sikre, at en sådan kontrolfunktion har en passende grad af uafhængighed for at undgå interessekonflikter, mindst én gang om året at dokumentere og gennemgå rammen for IKT-risikostyring, regelmæssigt at underkaste rammen for IKT-risikostyring intern revision, at foretage tilbundsgående vurderinger efter større ændringer i deres net- og informationssysteminfrastrukturer og -processer, regelmæssigt at foretage risikoanalyser af legacy-IKT-systemer, at underkaste gennemførelsen af planerne for IKT-indsats og -genopretning uafhængig intern revisionsgennemgang, at have en krisestyringsfunktion, at udvide test af driftsstabiliteten samt indsats- og genopretningsplaner til at dække overgangsscenarier mellem den primære IKT-infrastruktur og redundante faciliteter, efter deres anmodning at indberette et skøn over de samlede årlige omkostninger og tab som følge af større IKT-relaterede hændelser til de kompetente myndigheder, at opretholde redundante IKT-kapaciteter, at informere nationale kompetente myndigheder om gennemførte ændringer efter gennemgange af IKT-relaterede hændelser, løbende at overvåge relevant teknologisk udvikling, at etablere et omfattende program for test af digital operationel modstandsdygtighed som en integreret

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

del af den ramme for IKT-risikostyring, der er fastsat i denne forordning, eller at vedtage og regelmæssigt gennemgå en strategi for IKT-tredjepartsrisiko. Desuden bør mikrovirksomheder kun være forpligtet til at vurdere behovet for at opretholde sådanne redundante IKT-kapaciteter på grundlag af deres risikoprofil. Mikrovirksomheder bør drage fordel af en mere fleksibel ordning for så vidt angår programmer for test af digital operationel modstandsdygtighed. Når de skal tage stilling til typen og hyppigheden af de test, der skal foretages, bør de skabe en passende balance mellem målet om at opretholde en høj digital operationel modstandsdygtighed og de tilgængelige ressourcer og deres samlede risikoprofil. Mikrovirksomheder og finansielle enheder, der er underlagt den forenklede ramme for IKT-risikostyring i henhold til denne forordning, bør undtages fra kravet om at foretage avancerede test af IKT-værktøjer, -systemer og -processer baseret på trusselsbaserede penetrationstest (TLPT), da kun finansielle enheder, der opfylder kriterierne i denne forordning, bør pålægges at foretage en sådan test. I lyset af deres begrænsede kapaciteter bør mikrovirksomheder kunne aftale med tredjepartsudbyderen af IKT-tjenester, at den finansielle enheds ret til adgang, inspektion og revision delegeres til en uafhængig tredjepart, der udpeges af tredjepart-sudbyderen af IKT-tjenester, forudsat at den pågældende finansielle enhed til enhver tid kan anmode den respektive uafhængige tredjepart om alle relevante oplysninger og garantier vedrørende de resultater, som tredjepartsudbyderen af IKT-tjenester opnår.

(44) Da kun de finansielle enheder, der er udpeget med henblik på avanceret test af digital modstandsdygtighed, bør pålægges at foretage trusselsbaserede penetrationstest, bør de administrative processer og finansielle omkostninger, som gennemførelsen af sådanne test indebærer, afholdes af en lille procentdel af finansielle enheder.

(45) For at sikre fuld tilpasning af og generel konsekvens mellem finansielle enheders virksomhedsstrategier på den ene side og gennemførelse af IKT-risikostyring på den anden side bør de finansielle enheders ledelsesorganer pålægges fortsat at indtage en central og aktiv rolle i styringen og tilpasningen af rammen for IKT-risikostyring og den samlede strategi for digital operationel modstandsdygtighed. Den tilgang, som ledelsesorganer skal anlægge, bør ikke kun fokusere på midlerne til at sikre modstandsdygtighed i IKT-systemer, men bør også omfatte mennesker og processer gennem en række politikker, som på hvert virksomhedsniveau og for alt personale fremmer stor bevidsthed om cybersikkerhed og et tilsagn om at overholde en streng cyberhygiejne på alle niveauer. Ledelsesorganets endelige ansvar for styringen af en finansiel enheds IKT-risiko bør være det overordnede princip i denne omfattende tilgang, der skal udmøntes yderligere i ledelsesorganets fortsatte indsats for at føre kontrol med overvågningen af IKT-risikostyring.

(46) Desuden går princippet om ledelsesorganets fulde og endelige ansvar for styringen af den finansielle enheds IKT-risiko hånd i hånd med behovet for at sikre et vist niveau af IKT-relaterede investeringer og et samlet budget for den pågældende finansielle enhed, der gør det muligt for den finansielle enhed at opnå et højt niveau af digital operationel modstandsdygtighed.

(47) Med inspiration fra relevant bedste praksis og relevante retningslinjer, henstillinger eller tilgange på internationalt og nationalt plan samt på sektorplan vedrørende styring af cyberrisici fremmer denne forordning et sæt principper, der letter den samlede struktur for IKT-risikostyring. Så længe de hovedkapaciteter, som finansielle enheder indfører, håndterer de forskellige funktioner inden for IKT-risikostyring (identifikation, beskyttelse og forebyggelse, detektion, indsats og genopretning, læring og udvikling og kommunikation), som er omhandlet i denne forordning, bør det derfor stå finansielle enheder frit for at anvende modeller for IKT-risikostyring, som er udformet eller kategoriseret på en anden måde.

(48) For at holde trit med et cybertrusselsbillede i udvikling bør finansielle enheder opretholde opdaterede IKT-systemer, der er pålidelige og egnede til ikke kun at garantere den databehandling, der er nødvendig for deres tjenester, men også for at sikre tilstrækkelig teknologisk modstandsdygtighed, så de i tilstrækkelig grad kan tackle yderligere behandlingsrelaterede behov som følge af stressede markedsforhold eller andre vanskelige situationer.

(49) Effektive planer for driftsstabilitet og genopretningsplaner er nødvendige for, at finansielle enheder omgående og hurtigt kan finde en løsning på IKT-relaterede hændelser, navnlig cyberangreb, ved at begrænse skaden og prioritere genoptagelsen af aktiviteter og genopretningstiltag i overensstemmelse med deres politikker for sikkerhedskopiering. En sådan genoptagelse bør dog på ingen måde bringe net- og informationssystemernes integritet og sikkerhed eller tilgængeligheden, autenticiteten, integriteten eller fortroligheden af data i fare.

(50) Om end denne forordning giver finansielle enheder mulighed for at fastsætte deres mål for genopretningstid og genopretningspunkt på en fleksibel måde og dermed fastsætte sådanne mål under fuld hensyntagen til de relevante funktioners karakter og kritiske betydning og eventuelle specifikke forretningsmæssige behov, bør den ikke desto mindre kræve, at de foretager en vurdering af den potentielle samlede indvirkning på markedseffektiviteten, når sådanne mål fastsættes.

(51) Bagmændene bag cyberangreb har tendens til at søge at opnå finansielle gevinster direkte fra kilden og dermed udsætte finansielle enheder for væsentlige konsekvenser. For at forhindre, at IKT-systemer mister deres integritet eller bliver utilgængelige, og dermed undgå brud på datasikkerheden og skade på fysisk IKT-infrastruktur, bør finansielle enheders indberetning af større IKT-relaterede hændelser forbedres og strømlines væsentligt. Indberetningen af IKT-relaterede hændelser bør harmoniseres ved at indføre et krav om, at alle finansielle enheder foretager indberetning direkte til deres relevante kompetente myndigheder. Hvis en finansiel enhed er underlagt tilsyn ved mere end én national kompetent myndighed, bør medlemsstaterne udpege en fælles kompetent myndighed som modtager af en sådan indberetning. Kreditinstitutter, der er klassificeret som signifikante i henhold til artikel 6, stk. 4, i Rådets forordning (EU) nr. 1024/2013 ([19]), bør indsende en sådan indberetning til de kompetente nationale myndigheder, som efterfølgende bør fremsende indberetningen til Den Europæiske Centralbank (ECB).

(52) Den direkte indberetning bør give finansielle tilsynsmyndigheder mulighed for at have øjeblikkelig adgang til oplysninger om større IKT-relaterede hændelser. Finansielle tilsynsmyndigheder bør til gengæld videreformidle detaljerne om større IKT-relaterede hændelser til offentlige ikkefinansielle myndigheder (såsom kompetente myndigheder og centrale kontaktpunkter i henhold til direktiv (EU) 2022/2555, nationale databeskyttelsesmyndigheder og til retshåndhævende myndigheder ved større IKT-relaterede hændelser af kriminel karakter) for at øge sådanne myndigheders kendskab til sådanne hændelser og, for så vidt angår CSIRT'er, for at fremme hurtig bistand, der kan ydes til finansielle enheder, alt efter hvad der er relevant. Medlemsstaterne bør desuden kunne bestemme, at de finansielle enheder selv bør give sådanne oplysninger til offentlige myndigheder uden for området for finansielle tjenesteydelser. Disse informationsstrømme bør give finansielle enheder mulighed for hurtigt at drage fordel af alle relevante tekniske input, rådgivning om afhjælpende foranstaltninger og efterfølgende opfølgning fra sådanne myndigheders side. Oplysningerne om større IKT-relaterede hændelser bør sendes begge veje: De finansielle tilsynsmyndigheder bør give al nødvendig feedback eller vejledning til den finansielle enhed, mens ESA'erne bør dele anonymiserede data om cybertrusler og sårbarheder forbundet med en hændelse, for at bidrage til det bredere kollektive forsvar.

(53) Selv om alle finansielle enheder bør pålægges at foretage indberetning af hændelser, forventes dette krav ikke at påvirke dem alle på samme måde. Relevante væsentlighedstærskler samt rapporteringsfrister bør således tilpasses behørigt i forbindelse med delegerede retsakter baseret på de reguleringsmæssige tekniske standarder, der skal udvikles af ESA'erne, med henblik på kun at dække større IKT-relaterede hændelser. Desuden bør der tages hensyn til de særlige forhold, der gør sig gældende for finansielle enheder, når der fastsættes tidsfrister for indberetningsforpligtelser.

(54) Denne forordning bør fastsætte et krav om, at kreditinstitutter, betalingsinstitutter, kontooplysningstjenesteudbydere og e-pengeinstitutter indberetter alle operationelle eller sikkerhedsmæssige betalingsrelaterede hændelser, som tidligere blev indberettet i henhold til direktiv (EU) 2015/2366, uanset hændelsens IKT-karakter.

([19]) Rådets forordning (EU) nr. 1024/2013 af 15. oktober 2013 om overdragelse af specifikke opgaver til Den Europæiske Centralbank i forbindelse med politikker vedrørende tilsyn med kreditinstitutter (EUT L 287 af 29.10.2013, s. 63).

(55) ESA'erne bør have til opgave at vurdere den praktiske mulighed og betingelserne for en mulig centralisering af indberetninger af IKT-relaterede hændelser på EU-niveau. En sådan centralisering kunne bestå af et fælles EU-knudepunkt for indberetning af større IKT-relaterede hændelser, som enten direkte modtager de relevante indberetninger og automatisk underretter nationale kompetente myndigheder, eller som blot centraliserer relevante indberetninger, som de nationale kompetente myndigheder har indgivet, og dermed varetager en koordinatorrolle. ESA'erne bør i samråd med ECB og ENISA have til opgave at udarbejde en fælles rapport, hvori det undersøges, om det er praktisk muligt at oprette et fælles EU-knudepunkt.

(56) For at opnå et højt niveau af digital operationel modstandsdygtighed og skabe overensstemmelse med både de relevante internationale standarder (f.eks. G7 Fundamental Elements for Threat-Led Penetration Testing) og de rammer, der anvendes i Unionen, f.eks. TIBER-EU, bør finansielle enheder regelmæssigt teste deres IKT-systemer og medarbejdere med IKT-relaterede ansvar med hensyn til effektiviteten af deres forebyggelses-, detektions-, indsats- og genopretningskapaciteter for at afsløre og afhjælpe potentielle IKT-sårbarheder. For at afspejle de forskelle, der eksisterer på tværs af og inden for de forskellige finansielle delsektorer, for så vidt angår de finansielle enheders niveau af cybersikkerhedsberedskab, bør test omfatte en bred vifte af værktøjer og tiltag, der spænder lige fra vurderingen af grundlæggende krav (f.eks. sårbarhedsvurderinger og -scanninger, open source-analyser, vurderinger af netsikkerhed, mangelanalyser, fysiske sikkerhedsgennemgange, spørgeskemaer og scanningssoftwareløsninger, gennemgange af kildekoder når det er praktisk muligt, scenariebaserede test, kompatibilitetstest, præstationstest eller end-to-end-test) til mere avancerede test ved hjælp af TLPT. En sådan avanceret test bør kun kræves af finansielle enheder, der set fra et IKT-perspektiv er modne nok til at kunne gennemføre den på en rimelig måde. Den test af digital operationel modstandsdygtighed, der kræves i henhold til denne forordning, bør således være mere krævende for de finansielle enheder, der opfylder kriterierne i denne forordning (f.eks. store, systemiske og IKT-modne kreditinstitutter, børser, værdipapircentraler og centrale modparter) end for andre finansielle enheder. Samtidig bør test af digital operationel modstandsdygtighed ved hjælp af TLPT være mere relevant for finansielle enheder, der opererer inden for centrale delsektorer for finansielle tjenesteydelser, og som spiller en systemisk rolle (f.eks. betalinger, bankvirksomhed samt clearing og afvikling), og mindre relevant for andre delsektorer (f.eks. kapitalforvaltere og kreditvurderingsbureauer).

(57) Finansielle enheder, der er involveret i grænseoverskridende aktiviteter, og som udøver den frie etableringsret eller retten til fri udveksling af tjenesteydelser i Unionen, bør opfylde et fælles sæt avancerede testkrav (dvs. TLPT) i deres hjemland, som bør inkludere IKT-infrastrukturerne i alle de jurisdiktioner, hvori den grænseoverskridende finansielle koncern opererer inden for Unionen, hvorved det for sådanne grænseoverskridende finansielle koncerners vedkommende gøres muligt kun at pådrage sig IKT-relaterede testomkostninger i én jurisdiktion.

(58) For at trække på den ekspertise, som visse kompetente myndigheder allerede har erhvervet, navnlig med hensyn til gennemførelse af TIBER-EU-rammen, bør denne forordning gøre det muligt for medlemsstater at udpege en fælles offentlig myndighed som ansvarlig i den finansielle sektor på nationalt plan for alle TLPT-spørgsmål eller for kompetente myndigheder, i mangel af en sådan udpegelse, at uddelegere udøvelsen af TLPT-relaterede opgaver til en anden national finansiel kompetent myndighed.

(59) Da denne forordning ikke stiller krav om, at finansielle enheder skal lade alle kritiske eller vigtige funktioner være omfattet af en enkelt trusselsbaseret penetrationstest, bør finansielle enheder frit kunne afgøre, hvilke og hvor mange kritiske eller vigtige funktioner der bør være omfattet af en sådan test.

(60) Samlede test som omhandlet i denne forordning, der indebærer deltagelse af flere finansielle enheder i en TLPT, og for hvilke en tredjepartsudbyder af IKT-tjenester direkte kan indgå kontraktlige ordninger med en ekstern tester, bør kun tillades, hvis kvaliteten eller sikkerheden af de tjenester, som tredjepartsudbyderen af IKT-tjenester leverer til kunder, der er enheder, som falder uden for denne forordnings anvendelsesområde, eller fortroligheden af data forbundet med sådanne tjenester, med rimelighed kan forventes at blive negativt påvirket. Samlede test bør også være omfattet af garantier (ledelse af én udpeget finansiel enhed, kalibrering af antallet af deltagende finansielle enheder) for at sikre en streng testøvelse for de involverede finansielle enheder, som opfylder målene for TLPT i henhold til denne forordning.

(61) For at udnytte de interne ressourcer, der er til rådighed på virksomhedsniveau, bør denne forordning gøre det muligt at anvende interne testere med henblik på at foretage TLPT under forudsætning af tilsynsmæssig godkendelse, fravær af interessekonflikter og af regelmæssige skift af anvendelsen af interne og eksterne testere (hver tredje test), samtidig med at det også kræves, at formidleren af trusselsefterretninger i TLPT'en altid skal være ekstern i forhold til den finansielle enhed. Ansvaret for at gennemføre TLPT bør forblive fuldt ud hos den finansielle enhed. Erklæringer fra myndigheder bør udelukkende have til formål at opnå gensidig anerkendelse og bør ikke udelukke eventuelle opfølgende foranstaltninger, der er nødvendige for at imødegå den IKT-risiko, som den finansielle enhed er udsat for, og de bør heller ikke betragtes som en tilsynsmæssig godkendelse af en finansiel enheds kapacitet til IKT-risikostyring og -risikoafbødning.

(62) For at sikre en forsvarlig overvågning af IKT-tredjepartsrisiko i den finansielle sektor er det nødvendigt at fastlægge en række principbaserede regler, der skal fungere som rettesnor for finansielle enheder, når de overvåger risici i forbindelse med funktioner, der outsources til tredjepartsudbydere af IKT-tjenester, navnlig for IKT-tjenester, der understøtter kritiske eller vigtige funktioner, og mere generelt i forbindelse med afhængighed af alle IKT-tredjeparter.

(63) For at tage højde for kompleksiteten af de forskellige kilder til IKT-risiko og samtidig tage hensyn til de mange forskellige udbydere af teknologiske løsninger, der muliggør en gnidningsløs levering af finansielle tjenesteydelser, bør denne forordning omfatte en bred vifte af tredjepartsudbydere af IKT-tjenester, herunder udbydere af cloudcomputingtjenester, software, dataanalysetjenester og udbydere af datacentertjenester. Da finansielle enheder på effektiv og sammenhængende vis bør identificere og styre alle typer risici, herunder i forbindelse med IKT-tjenester indkøbt inden for en finansiel koncern, bør det ligeledes præciseres, at virksomheder, der er en del af en finansiel koncern og hovedsagelig leverer IKT-tjenester til deres modervirksomhed eller til dattervirksomheder eller filialer af deres modervirksomhed, samt finansielle enheder, der leverer IKT-tjenester til andre finansielle enheder, også bør betragtes som tredjepartsudbydere af IKT-tjenester i henhold til denne forordning. Endelig, i lyset af udviklingen på betalingstjenestemarkedet, der bliver stadig mere afhængigt af komplekse tekniske løsninger, og i betragtning af nye typer betalingstjenester og betalingsrelaterede løsninger, bør deltagere i økosystemet for betalingstjenester, der leverer betalingsbehandlingsaktiviteter eller driver betalingsinfrastrukturer, også betragtes som tredjepartsudbydere af IKT-tjenester i henhold til denne forordning, bortset fra centralbanker, når de driver betalings- eller værdipapirafviklingssystemer, og offentlige myndigheder, når de leverer IKT-relaterede tjenester i forbindelse med udførelsen af statslige funktioner.

(64) En finansiel enhed bør til enhver tid fortsat være fuldt ansvarlig for opfyldelsen af sine forpligtelser i henhold til denne forordning. Finansielle enheder bør anvende en forholdsmæssigt afpasset tilgang til overvågningen af de risici, som opstår hos tredjepartsudbydere af IKT-tjenester, under behørig hensyntagen til karakteren, omfanget, kompleksiteten og betydningen af deres IKT-relaterede afhængighed eller tjenesternes kritiske karakter eller betydning, processer eller funktioner, der er omfattet af de kontraktlige ordninger, og i sidste ende på grundlag af en omhyggelig vurdering af en eventuel potentiel indvirkning på kvaliteten af finansielle tjenesteydelser og deres stabilitet på individuelt plan og koncernplan, alt efter hvad der er relevant.

(65) Udførelsen af en sådan overvågning bør følge en strategisk tilgang til IKT-tredjepartsrisiko, der formaliseres ved, at den finansielle enheds ledelsesorgan vedtager en særlig strategi for IKT-tredjepartsrisiko, som tager udgangspunkt i en løbende screening af enhver afhængighed af IKT-tredjeparter. For at øge den tilsynsmæssige bevidsthed om afhængighed af IKT-tredjeparter og med henblik på yderligere at understøtte arbejdet i forbindelse med den tilsynsramme, der oprettes ved denne forordning, bør alle finansielle enheder forpligtes til at opretholde et register over oplysninger med alle kontraktlige ordninger om brugen af IKT-tjenester, der leveres af tredjepartsudbydere af IKT-tjenester. Finansielle tilsynsmyndigheder bør have mulighed for at anmode om det fulde register eller anmode om specifikke afsnit heraf og dermed indhente væsentlige oplysninger med henblik på at opnå en bredere forståelse af finansielle enheders IKT-afhængighed.

(66) En grundig analyse forud for kontraktindgåelsen bør understøtte og gå forud for den formelle indgåelse af kontraktlige ordninger, navnlig ved at fokusere på elementer såsom den kritiske karakter eller betydningen af de tjenester, der understøttes af den påtænkte IKT-kontrakt, de nødvendige tilsynsmæssige godkendelser eller andre betingelser, den mulige koncentrationsrisiko, der er forbundet hermed, samt anvendelse af due diligence i processen med udvælgelse og vurdering af tredjepartsudbydere af IKT-tjenester og vurdering af potentielle interessekonflikter. I forbindelse med kontraktlige ordninger vedrørende kritiske eller vigtige funktioner bør finansielle enheder tage hensyn til tredjepartsudbydere af IKT-tjenesters brug af de seneste og højeste informationssikkerhedsstandarder. Opsigelse af kontraktlige ordninger kan som minimum være foranlediget af en række omstændigheder, der påviser

mangler hos tredjepartsudbyderen af IKT-tjenester, navnlig væsentlige overtrædelser af love eller kontraktvilkår, omstændigheder, der afslører en potentiel ændring i udførelsen af de funktioner, der er fastsat i de kontraktlige ordninger, tegn på svagheder hos tredjepartsudbyderen af IKT-tjenester i dens samlede IKT-risikostyring eller omstændigheder, der tyder på, at den relevante kompetente myndighed ikke er i stand til at føre effektivt tilsyn med den finansielle enhed.

(67) For at tackle de systemiske virkninger af den koncentrationsrisiko, der er forbundet med IKT-tredjeparter, fremmer denne forordning en afbalanceret løsning ved at anlægge en fleksibel og gradvis tilgang til en sådan koncentrationsrisiko, da indførelsen af ufleksible lofter eller strenge begrænsninger kan hindre udøvelsen af virksomhed og begrænse kontraktfriheden. Finansielle enheder bør foretage en grundig vurdering af deres påtænkte kontraktlige ordninger for at identificere sandsynligheden for, at sådanne risici opstår, herunder ved hjælp af tilbundsgående analyser af underentrepriseordninger, navnlig når de er indgået med tredjepartsudbydere af IKT-tjenester med hjemsted i et tredjeland. På nuværende tidspunkt og med henblik på at finde en rimelig balance mellem nødvendigheden af at bevare kontraktfriheden og af at sikre den finansielle stabilitet anses det ikke for hensigtsmæssigt at fastsætte regler om strenge lofter og begrænsninger for eksponeringen for IKT-tredjeparter. I forbindelse med tilsynsrammen bør en ledende tilsynsførende, der er udpeget i henhold til denne forordning, for så vidt angår kritiske tredjepartsudbydere af IKT-tjenester være særligt opmærksom på at opnå fuld forståelse for omfanget af den indbyrdes afhængighed, identificere specifikke tilfælde, hvor en høj koncentrationsgrad af kritiske tredjepartsudbydere af IKT-tjenester i Unionen sandsynligvis vil lægge pres på stabiliteten og integriteten i Unionens finansielle system, og opretholde en dialog med kritiske tredjepartsudbydere af IKT-tjenester, hvor en sådan specifik risiko er identificeret.

(68) For regelmæssigt at vurdere og overvåge evnen hos en tredjepartsudbyder af IKT-tjenester til sikkert at levere tjenester til en finansiel enhed, uden at dette har negative virkninger for en finansiel enheds digitale operationelle modstandsdygtighed, bør flere centrale kontraktlige elementer med tredjepartsudbydere af IKT-tjenester harmoniseres. En sådan harmonisering bør omfatte minimumsområder, som er afgørende for, at den finansielle enhed kan foretage en fuld overvågning af de risici, der kan opstå fra tredjepartsudbyderen af IKT-tjenester, set i lyset af en finansiel enheds behov for at sikre sin digitale modstandsdygtighed, da den er dybt afhængig af de modtagne IKT-tjenesters stabilitet, funktionalitet, tilgængelighed og sikkerhed.

(69) Når finansielle enheder og tredjepartsudbydere af IKT-tjenester genforhandler kontraktlige ordninger med henblik på at opnå overensstemmelse med kravene i denne forordning, bør de sikre, at de centrale kontraktbestemmelser som fastsat i denne forordning er omfattet.

(70) Definitionen af »kritisk eller vigtig funktion« i denne forordning omfatter de »kritiske funktioner« som defineret i artikel 2, stk. 1, nr. 35), i Europa-Parlamentets og Rådets direktiv 2014/59/EU ([20]). Funktioner, der anses for at være kritiske i henhold til direktiv 2014/59/EU, er derfor medtaget i definitionen af kritiske funktioner i henhold til denne forordning.

(71) Uanset den kritiske karakter eller vigtigheden af den funktion, der understøttes af IKT-tjenesterne, bør kontraktlige ordninger navnlig indeholde en specifikation bestående af de komplette beskrivelser af funktioner og tjenester, af steder, hvor sådanne funktioner leveres, og hvor der skal behandles data, samt beskrivelser af serviceniveauet. Andre væsentlige elementer for at muliggøre en finansiel enheds overvågning af IKT-tredjepartsrisiko er: kontraktlige bestemmelser, der præciserer, hvordan adgangen, tilgængeligheden, integriteten, sikkerheden og beskyttelsen af personoplysninger sikres af tredjepartsudbyderen af IKT-tjenester, bestemmelser, der fastsætter de relevante garantier for at muliggøre adgang, genopretning og returnering af data i tilfælde af insolvens eller afvikling eller i tilfælde af, at tredjepartsudbyderen af IKT-tjenester afbryder sine forretningsaktiviteter, samt bestemmelser, der kræver, at tredjepartsudbyderen af IKT-tjenester yder bistand i tilfælde af IKT-hændelser i forbindelse med de leverede tjenester, uden yderligere omkostninger eller til en omkostning, der fastsættes på forhånd, bestemmelser

([20]) Europa-Parlamentets og Rådets direktiv 2014/59/EU af 15. maj 2014 om et regelsæt for genopretning og afvikling af kreditinstitutter og investeringsselskaber og om ændring af Rådets direktiv 82/891/EØF og Europa-Parlamentets og Rådets direktiv 2001/24/EF, 2002/47/EF, 2004/25/EF, 2005/56/EF, 2007/36/EF, 2011/35/EU, 2012/30/EU og 2013/36/EU samt forordning (EU) nr. 1093/2010 og (EU) nr. 648/2012 (EUT L 173 af 12.6.2014, s. 190).

om forpligtelsen for tredjepartsudbyderen af IKT-tjenester til at samarbejde fuldt ud med den finansielle enheds kompetente myndigheder og afviklingsmyndigheder, samt bestemmelser om opsigelsesrettigheder og dertil knyttede minimumsfrister for opsigelse af de kontraktlige ordninger i overensstemmelse med de kompetente myndigheders og afviklingsmyndighedernes forventninger.

(72) Ud over sådanne kontraktlige bestemmelser og med henblik på at sikre, at finansielle enheder fortsat har fuld kontrol over alle udviklingstendenser på tredjepartsniveau, som risikerer at forringe deres IKT-sikkerhed, bør kontrakterne om levering af IKT-tjenester, der understøtter kritiske eller vigtige funktioner, også indeholde følgende: en fuldstændig beskrivelse af serviceniveauer med præcise kvantitative og kvalitative præstationsmål, således at der uden unødigt ophold kan træffes passende afhjælpende foranstaltninger, når de aftalte serviceniveauer ikke overholdes; de relevante opsigelsesfrister og indberetningsforpligtelser for tredjepartsudbyderen af IKT-tjenester i tilfælde af udviklingstendenser, som har en potentiel væsentlig indvirkning på evnen hos tredjepartsudbyderen af IKT-tjenester til effektivt at levere de respektive IKT-tjenester; et krav til tredjepartsudbyderen af IKT-tjenester om at gennemføre og teste forretningsberedskabsplaner og indføre IKT-sikkerhedsforanstaltninger, -værktøjer og -politikker, som giver mulighed for sikker levering af tjenester, og om at deltage og samarbejde fuldt ud i den TLPT, der udføres af den finansielle enhed.

(73) Kontrakter om levering af IKT-tjenester, der understøtter kritiske eller vigtige funktioner, bør også indeholde bestemmelser, der giver den finansielle enhed eller en udpeget tredjepart ret til adgang, inspektion og revision og ret til at tage kopier som afgørende instrumenter i de finansielle enheders løbende overvågning af de resultater, som tredjepartsudbyderen af IKT-tjenester opnår, kombineret med tjenesteudbyderens fulde samarbejde i forbindelse med inspektioner. Tilsvarende bør den finansielle enheds kompetente myndighed på grundlag af underretninger have ret til at inspicere og foretage revision af tredjepartsudbyderen af IKT-tjenester, med forbehold af beskyttelsen af fortrolige oplysninger.

(74) Sådanne kontraktlige ordninger bør også indeholde særlige exitstrategier for navnlig at muliggøre obligatoriske overgangsperioder, i løbet af hvilke tredjepartsudbydere af IKT-tjenester fortsat bør levere de relevante tjenester med henblik på at mindske risikoen for forstyrrelser i den finansielle enhed, eller at give sidstnævnte mulighed for effektivt at skifte til anvendelsen af andre tredjepartsudbydere af IKT-tjenester, eller alternativt at skifte til interne løsninger, der stemmer overens med den leverede IKT-tjenestes kompleksitet. Desuden bør finansielle enheder, der er omfattet af direktiv 2014/59/EU, sikre, at de relevante kontrakter for IKT-tjenester er robuste og kan håndhæves fuldt ud i tilfælde af afvikling af de pågældende finansielle enheder. I overensstemmelse med afviklingsmyndighedernes forventninger bør disse finansielle enheder derfor sikre, at de relevante kontrakter for IKT-tjenester er modstandsdygtige over for afvikling. Så længe disse finansielle enheder fortsat opfylder deres betalingsforpligtelser, bør de bl.a. sikre, at de relevante kontrakter for IKT-tjenester indeholder bestemmelser om, at omstrukturering eller afvikling ikke medfører opsigelse, suspension eller ændring.

(75) Desuden kan den frivillige anvendelse af de standardkontraktbestemmelser, der er udviklet af offentlige myndigheder eller EU-institutioner, navnlig anvendelsen af kontraktbestemmelser udviklet af Kommissionen for cloudcomputingtjenester, give de finansielle enheder og tredjepartsudbydere af IKT-tjenester yderligere tryghed ved at øge deres retssikkerhedsniveau med hensyn til anvendelsen af cloudcomputingtjenester i den finansielle sektor, i fuld overensstemmelse med de krav og forventninger, der er fastsat i EU-retten om finansielle tjenesteydelser. Udarbejdelsen af standardkontraktbestemmelser bygger på de foranstaltninger, der allerede var påtænkt i fintechhandlingsplanen fra 2018, der bekendtgjorde, at Kommissionen har til hensigt at tilskynde til og fremme udarbejdelsen af standardkontraktbestemmelser for finansielle enheders anvendelse af cloudcomputingtjenester og i den forbindelse trække på indsatsen blandt tværsektorielle interessenter på området for cloudcomputingtjenester, som Kommissionen har fremmet gennem inddragelse af den finansielle sektor.

(76) Med henblik på at fremme konvergens og effektivitet i forbindelse med tilsynsmæssige tilgange til håndtering af IKT-tredjepartsrisiko i den finansielle sektor samt for at styrke den digitale operationelle modstandsdygtighed i finansielle enheder, der er afhængige af kritiske tredjepartsudbydere af IKT-tjenester for levering af de IKT-tjenester, der understøtter leveringen af finansielle tjenesteydelser, og dermed bidrage til at bevare stabiliteten i Unionens finansielle system og integriteten i det indre marked for finansielle tjenesteydelser, bør kritiske tredjepartsudbydere af IKT-tjenester være omfattet af en EU-tilsynsramme. Selv om oprettelsen af tilsynsrammen er begrundet i merværdien af at træffe foranstaltninger på EU-plan, og i kraft af den iboende rolle og de særlige forhold, der gør sig

gældende for brugen af IKT-tjenester i forbindelse med levering af finansielle tjenesteydelser, bør det samtidig erindres, at denne løsning kun forekommer hensigtsmæssig inden for rammerne af denne forordning, der specifikt omhandler digital operationel modstandsdygtighed i den finansielle sektor. En sådan tilsynsramme bør imidlertid ikke betragtes som en ny model for EU-tilsyn inden for finansielle tjenesteydelser og aktiviteter.

(77) Tilsynsrammen bør kun finde anvendelse på kritiske tredjepartsudbydere af IKT-tjenester. Der bør derfor være en udpegelsesmekanisme for at tage hensyn til omfanget og karakteren af den finansielle sektors afhængighed af sådanne tredjepartsudbydere af IKT-tjenester. Denne mekanisme bør indebære et sæt kvantitative og kvalitative kriterier til fastsættelse af parametre for kritisk karakter som grundlag for medtagelse i tilsynsrammen. For at sikre nøjagtigheden af denne vurdering og uanset tredjepartsudbyderen af IKT-tjenesters virksomhedsstruktur bør sådanne kriterier, hvis der er tale om en tredjepartsudbyder af IKT-tjenester, der er en del af en større koncern, tage hensyn til hele koncernstrukturen for tredjepartsudbyderen af IKT-tjenester. På den ene side bør kritiske tredjepartsudbydere af IKT-tjenester, som ikke automatisk udpeges i medfør af disse kriterier, have mulighed for at deltage i tilsynsrammen på frivillig basis, men på den anden side bør tredjepartsudbydere af IKT-tjenester, der allerede er omfattet af tilsynsrammer, som understøtter udførelsen af Det Europæiske System af Centralbankers opgaver som omhandlet i artikel 127, stk. 2, i TEUF, undtages.

(78) Tilsvarende bør finansielle enheder, der leverer IKT-tjenester til andre finansielle enheder, selv om de tilhører kategorien af tredjepartsudbydere af IKT-tjenester i henhold til denne forordning, også undtages fra tilsynsrammen, da de allerede er underlagt tilsynsmekanismer, der er oprettet ved den relevante EU-ret om finansielle tjenesteydelser. Hvor det er relevant, bør de kompetente myndigheder i forbindelse med deres tilsynsaktiviteter tage hensyn til den IKT-risiko, som finansielle enheder, der leverer IKT-tjenester, udgør for finansielle enheder. På grund af de eksisterende risikoovervågningsmekanismer på koncernniveau bør den samme undtagelse ligeledes indføres for tredjepartsudbydere af IKT-tjenester, der hovedsageligt leverer tjenester til enheder i deres egen koncern. Tredjepartsudbydere af IKT-tjenester, der udelukkende leverer IKT-tjenester i én medlemsstat til finansielle enheder, der kun er aktive i den pågældende medlemsstat, bør også undtages fra udpegelsesmekanismen på grund af deres begrænsede aktiviteter og manglende grænseoverskridende virkninger.

(79) Den digitale omstilling, der er sket inden for finansielle tjenesteydelser, har medført en hidtil uset grad af anvendelse og afhængighed af IKT-tjenester. Eftersom det er blevet utænkeligt at levere finansielle tjenesteydelser uden brug af cloudcomputingtjenester, softwareløsninger og datarelaterede tjenester, er Unionens finansielle økosystem blevet uløseligt forbundet med visse IKT-tjenester, der leveres af leverandører af IKT-tjenester. Nogle af disse leverandører, som er innovatorer i udviklingen og anvendelsen af IKT-baserede teknologier, spiller en væsentlig rolle i leveringen af finansielle tjenesteydelser eller er blevet integreret i værdikæden for finansielle tjenesteydelser. De er således blevet afgørende for stabiliteten og integriteten af Unionens finansielle system. Denne udbredte afhængighed af tjenester, der leveres af kritiske tredjepartsudbydere af IKT-tjenester, kombineret med den indbyrdes afhængighed mellem forskellige markedsoperatørers informationssystemer skaber en direkte og potentielt alvorlig risiko for Unionens system for finansielle tjenesteydelser og for kontinuiteten i leveringen af finansielle tjenesteydelser, hvis kritiske tredjepartsudbydere af IKT-tjenester påvirkes af operationelle forstyrrelser eller større cyberhændelser. Cyberhændelser har en markant evne til at vokse og sprede sig i hele det finansielle system i betydeligt hurtigere tempo end andre typer risici, der overvåges i den finansielle sektor, og kan brede sig over sektorer og geografiske grænser. De har potentiale til at udvikle sig til en systemisk krise, hvor tilliden til det finansielle system udhules på grund af forstyrrelser af funktioner, der understøtter realøkonomien, eller til betydelige finansielle tab, der når et niveau, som det finansielle system ikke kan holde til, eller som kræver anvendelse af omfattende foranstaltninger til at absorbere chok. For at forhindre, at disse scenarier finder sted og derved bringer den finansielle stabilitet og integritet i Unionen i fare, er det afgørende at sikre konvergens i tilsynspraksis vedrørende IKT-tredjepartsrisiko inden for finansiering, navnlig gennem nye regler, der giver Unionen mulighed for at føre tilsyn med kritiske tredjepartsudbydere af IKT-tjenester.

(80) Tilsynsrammen afhænger i høj grad af graden af samarbejde mellem den ledende tilsynsførende og den kritiske tredjepartsudbyder af IKT-tjenester, der til finansielle enheder leverer tjenester, som påvirker leveringen af finansielle tjenesteydelser. Et vellykket tilsyn er bl.a. baseret på den ledende tilsynsførendes evne til effektivt at gennemføre overvågningsmissioner og inspektioner for at vurdere de regler, kontroller og processer, der anvendes af de kritiske tredjepartsudbydere af IKT-tjenester, samt for at vurdere deres aktiviteters potentielle kumulative indvirkning på den finansielle stabilitet og det finansielle systems integritet. Samtidig er det afgørende, at kritiske tredjepartsudbydere af IKT-tjenester følger den ledende tilsynsførendes henstillinger og imødekommer dennes betænkeligheder. Eftersom manglende samarbejde fra en kritisk tredjepartsudbyder af IKT-tjenester, der leverer tjenester, som påvirker leveringen af finansielle tjenesteydelser, f.eks. afslag på at give adgang til sine lokaler eller indgive oplysninger, i sidste ende vil fratage den ledende tilsynsførende sine afgørende værktøjer for at vurdere IKT-tredjepartsrisiko og kan have en negativ indvirkning på den finansielle stabilitet og det finansielle systems integritet, er det nødvendigt også at indføre en passende sanktionsordning.

(81) På denne baggrund bør det sikres, at den ledende tilsynsførendes behov for at kunne pålægge tvangsbøder for at tvinge kritiske tredjepartsudbydere af IKT-tjenester til at efterleve de gennemsigtigheds- og adgangsrelaterede forpligtelser, der er fastsat i denne forordning, ikke bringes i fare på grund af de vanskeligheder, som håndhævelsen af disse tvangsbøder giver anledning til over for kritiske tredjepartsudbydere af IKT-tjenester med hjemsted i tredjelande. For at sikre, at sådanne sanktioner kan håndhæves, og for at muliggøre en hurtig indførelse af procedurer, der opretholder de kritiske tredjepartsudbydere af IKT-tjenesters ret til forsvar i forbindelse med udpegelsesmekanismen og udstedelsen af henstillinger, bør disse kritiske tredjepartsudbydere af IKT-tjenester, der leverer tjenester til finansielle enheder, som påvirker leveringen af finansielle tjenesteydelser, være forpligtet til at opretholde en passende forretningsmæssig tilstedeværelse i Unionen. På grund af tilsynets karakter og manglen på sammenlignelige ordninger i andre jurisdiktioner er der ingen egnede alternative mekanismer til at nå dette mål gennem et effektivt samarbejde med finansielle tilsynsmyndigheder i tredjelande om overvågning af virkningen af de digitale operationelle risici hidrørende fra de systemiske tredjepartsudbydere af IKT-tjenester, som betragtes som kritiske tredjepartsudbydere af IKT-tjenester med hjemsted i tredjelande. For at fortsætte leveringen af IKT-tjenester til finansielle enheder i Unionen bør en tredjepartsudbyder af IKT-tjenester med hjemsted i tredjelande, der er udpeget som kritisk i overensstemmelse med denne forordning, derfor senest 12 måneder efter udpegelsen træffe alle nødvendige foranstaltninger for at sikre sin registrering som selskab i Unionen ved at oprette en dattervirksomhed som defineret i gældende EU-ret, nemlig i Europa-Parlamentets og Rådets direktiv 2013/34/EU ([21]).

(82) Kravet om at oprette en dattervirksomhed i Unionen bør ikke forhindre den kritiske tredjepartsudbyder af IKT-tjenester i at levere IKT-tjenester og dertil knyttet teknisk support fra faciliteter og infrastruktur beliggende uden for Unionen. Denne forordning pålægger ikke en datalokaliseringsforpligtelse, da den ikke kræver, at datalagring eller -behandling skal finde sted i Unionen.

(83) Kritiske tredjepartsudbydere af IKT-tjenester bør kunne levere IKT-tjenester fra et hvilket som helst sted i verden og derfor ikke nødvendigvis eller ikke kun fra lokaler beliggende i Unionen. Tilsynsaktiviteter bør først gennemføres på lokaler beliggende i Unionen og ved at interagere med enheder, der er beliggende i Unionen, herunder de dattervirksomheder, der er etableret af kritiske tredjepartsudbydere af IKT-tjenester i henhold til denne forordning. Sådanne tiltag inden for Unionen kan imidlertid være utilstrækkelige til, at den ledende tilsynsførende fuldt ud og effektivt kan varetage sine opgaver i henhold til denne forordning. Den ledende tilsynsførende bør derfor også kunne udøve sine relevante tilsynsbeføjelser i tredjelande. Udøvelsen af disse beføjelser i tredjelande bør gøre det muligt for den ledende tilsynsførende at undersøge de faciliteter, hvorfra IKT-tjenesterne eller de tekniske supporttjenester faktisk leveres eller forvaltes af den kritiske tredjepartsudbyder af IKT-tjenester, og bør give den ledende tilsynsførende en omfattende og operationel forståelse af IKT-risikostyringen ved den kritiske tredjepartsudbyder af IKT-tjenester. Den ledende tilsynsførendes mulighed for som et EU-agentur at udøve beføjelser uden for Unionens område bør være behørigt afgrænset af relevante betingelser, navnlig samtykke fra den berørte kritiske tredjepartsudbyder af IKT-tjenester. Tilsvarende bør de relevante myndigheder i tredjelandet underrettes om og ikke have gjort indsigelse mod den ledende tilsynsførendes udøvelse af aktiviteter på deres eget område. For at sikre en effektiv gennemførelse, og

([21]) Europa-Parlamentets og Rådets direktiv 2013/34/EU af 26. juni 2013 om årsregnskaber, konsoliderede regnskaber og tilhørende beretninger for visse virksomhedsformer, om ændring af Europa-Parlamentets og Rådets direktiv 2006/43/EF og om ophævelse af Rådets direktiv 78/660/EØF og 83/349/EØF (EUT L 182 af 29.6.2013, s. 19).

uden at det berører EU-institutionernes og medlemsstaternes respektive beføjelser, er det imidlertid også nødvendigt, at sådanne beføjelser er fuldt forankret i indgåelsen af administrative samarbejdsordninger med de relevante myndigheder i det berørte tredjeland. Denne forordning bør derfor give ESA'erne mulighed for at indgå administrative samarbejdsordninger med de relevante myndigheder i tredjelande, som ikke derudover bør skabe retlige forpligtelser for Unionen og dens medlemsstater.

(84) For at lette kommunikationen med den ledende tilsynsførende og sikre passende repræsentation bør kritiske tredjepartsudbydere af IKT-tjenester, som indgår i en koncern, udpege én juridisk person som deres koordinationspunkt.

(85) Tilsynsrammen bør ikke berøre medlemsstaternes beføjelser til at gennemføre deres egne tilsyns- eller overvågningsmissioner i forhold til tredjepartsudbydere af IKT-tjenester, som ikke er udpeget som kritiske i henhold til denne forordning, men som anses for at være vigtige på nationalt plan.

(86) For at sikre effekten af den institutionelle flerlagsarkitektur på området for finansielle tjenesteydelser bør Det Fælles Udvalg af ESA'er fortsat sikre samlet koordinering på tværs af sektorer af alle forhold, der vedrører IKT-risiko, i overensstemmelse med dets opgaver vedrørende cybersikkerhed. Det bør få støtte fra et nyt underudvalg (»tilsynsforummet«), der udfører det forberedende arbejde både med henblik på individuelle afgørelser rettet mod kritiske tredjepartsudbydere af IKT-tjenester og med henblik på udstedelse af kollektive henstillinger, navnlig i forbindelse med benchmarking af tilsynsprogrammerne for kritiske tredjepartsudbydere af IKT-tjenester, og fastlæggelse af bedste praksis for håndtering af spørgsmål vedrørende IKT-koncentrationsrisiko.

(87) For at sikre et passende og effektivt tilsyn på EU-plan med kritiske tredjepartsudbydere af IKT-tjenester, fastsættes det i denne forordning, at enhver af de tre ESA'er kan udpeges som en ledende tilsynsførende. Den individuelle tildeling af en kritisk tredjepartsudbyder af IKT-tjenester til en af de tre ESA'er bør være resultatet af en vurdering af, hvilke finansielle enheder der overvejende opererer i de finansielle sektorer, som den pågældende ESA har ansvaret for. Denne tilgang bør føre til en afbalanceret fordeling af opgaver og ansvarsområder mellem de tre ESA'er i forbindelse med udøvelsen af tilsynsfunktionerne og bør gøre bedst mulig brug af de menneskelige ressourcer og den tekniske ekspertise, der er til rådighed i hver af de tre ESA'er.

(88) Ledende tilsynsførende bør tildeles de nødvendige beføjelser til at foretage undersøgelser, gennemføre inspektioner på stedet og eksterne inspektioner i lokaler og på steder hos kritiske tredjepartsudbydere af IKT-tjenesters og indhente fuldstændige og ajourførte oplysninger. Disse beføjelser bør sætte den ledende tilsynsførende i stand til at opnå en reel indsigt i typen, omfanget og virkningerne af den IKT-tredjepartsrisiko, der berører finansielle enheder og i sidste ende Unionens finansielle system. Overdragelse af hovedansvaret for tilsynsrollen til ESA'erne udgør en forudsætning for at forstå og håndtere den systemiske dimension af IKT-risiko inden for finansiering. Den indvirkning, som kritiske tredjepartsudbydere af IKT-tjenester har på Unionens finansielle sektor, og de potentielle problematikker, der skyldes den deraf følgende IKT-koncentrationsrisiko, kræver en kollektiv tilgang på EU-plan. Samtidig gennemførelse af flere revisioner og adgangsrettigheder, der udføres separat af en lang række kompetente myndigheder med begrænset eller ingen indbyrdes koordinering, vil forhindre de finansielle tilsynsmyndigheder i at få et fuldstændigt og omfattende overblik over IKT-tredjepartsrisiko i Unionen, samtidig med at der også skabes redundans, byrder og kompleksitet for kritiske tredjepartsudbydere af IKT-tjenester, hvis de er genstand for mange overvågnings- og inspektionsanmodninger.

(89) Da udpegelsen som kritisk har en betydelig indvirkning, bør denne forordning sikre, at rettighederne for kritiske tredjepartsudbydere af IKT-tjenester overholdes i hele gennemførelsen af tilsynsrammen. Inden sådanne udbydere udpeges som kritiske, bør de f.eks. have ret til at indgive en begrundet erklæring til den ledende tilsynsførende med alle relevante oplysninger med henblik på vurderingen i forbindelse med deres udpegelse. Eftersom den ledende tilsynsførende bør have beføjelse til at fremsætte henstillinger vedrørende IKT-risiko og passende afhjælpende foranstaltninger dertil, hvilket omfatter beføjelsen til at gøre indsigelse mod visse kontraktlige ordninger, som i sidste ende påvirker stabiliteten i den finansielle enhed eller det finansielle system, bør kritiske tredjepartsudbydere af IKT-tjenester også have mulighed for inden færdiggørelsen af disse henstillinger at fremlægge redegørelser for den forventede virkning af de løsninger, der påtænkes i henstillingen, for kunder, som er enheder, der ikke er omfattet af denne forordnings anvendelsesområde, og for at udarbejde løsninger til at afbøde risici. Kritiske tredjepartsudbydere

af IKT-tjenester, der er uenige i henstillingerne, bør indgive en begrundet redegørelse for deres hensigt om ikke at tilslutte sig henstillingen. Hvis en sådan begrundet redegørelse ikke indgives, eller hvis den anses for at være utilstrækkelig, bør den ledende tilsynsførende udsende en offentlig meddelelse, der kort beskriver den manglende overholdelse.

(90) De kompetente myndigheder bør på behørig vis medtage opgaven med at kontrollere den indholdsmæssige overholdelse af henstillinger, som er udstedt af den ledende tilsynsførende, i deres funktioner med hensyn til tilsyn med finansielle enheder. De kompetente myndigheder bør kunne kræve, at finansielle enheder træffer yderligere foranstaltninger for at imødegå de risici, der er konstateret i den ledende tilsynsførendes henstillinger, og bør i rette tid udstede underretninger herom. Hvis den ledende tilsynsførende retter henstillinger til kritiske tredjepart-sudbydere af IKT-tjenester, der er underlagt tilsyn i henhold til direktiv (EU) 2022/2555, bør de kompetente myndigheder på frivillig basis og inden vedtagelsen af yderligere foranstaltninger kunne høre de kompetente myndigheder i henhold til nævnte direktiv for at fremme en koordineret tilgang til håndteringen af de pågældende kritiske tredjepartsudbydere af IKT-tjenester.

(91) Udøvelsen af tilsynet bør styres af tre operationelle principper, der har til formål at sikre: a) tæt koordinering mellem ESA'erne i deres rolle som ledende tilsynsførende gennem et fælles tilsynsnetværk, b) overensstemmelse med den ramme, der er fastlagt ved direktiv (EU) 2022/2555 (gennem en frivillig høring af organer i henhold til nævnte direktiv, for at undgå overlapning af foranstaltninger rettet mod kritiske tredjepartsudbydere af IKT-tjenester), og c) anvendelse af omhu for at minimere den potentielle risiko for forstyrrelser af tjenester, der leveres af kritiske tredjepartsudbydere af IKT-tjenester til kunder, der er enheder, som ikke er omfattet af denne forordnings anvendelsesområde.

(92) Tilsynsrammen bør ikke erstatte eller på nogen måde eller for nogen dels vedkommende træde i stedet for kravet til de finansielle enheder om selv at forvalte de risici, der er forbundet med brugen af tredjepartsudbydere af IKT-tjenester, herunder deres forpligtelse til at opretholde en løbende overvågning af kontraktlige ordninger, der indgås med kritiske tredjepartsudbydere af IKT-tjenester. Ligeledes bør tilsynsrammen ikke berøre finansielle enheders fulde ansvar for at overholde og opfylde alle de retlige forpligtelser, der er fastsat i denne forordning og i den relevante finansielle tjenesteydelsesret.

(93) For at undgå dobbeltbestemmelser og overlapninger bør de kompetente myndigheder afholde sig fra individuelt at træffe foranstaltninger, der har til formål at overvåge risici hos den kritiske tredjepartsudbyder af IKT-tjenester, og bør i den forbindelse basere sig på den relevante ledende tilsynsførendes vurdering. Alle foranstaltninger bør under alle omstændigheder koordineres og vedtages på forhånd med den ledende tilsynsførende som led i udførelsen af opgaver i tilsynsrammen.

(94) For at fremme konvergens på internationalt plan vedrørende brug af bedste praksis for gennemgangen og overvågningen af den digitale risikostyring, der foretages af tredjepartsudbydere af IKT-tjenester, bør ESA'erne opfordres til at indgå samarbejdsordninger med relevante tilsyns- og reguleringsmyndigheder i tredjelande.

(95) Med henblik på at udnytte de specifikke kompetencer, tekniske færdigheder og ekspertisen blandt personale, der er specialiseret i operationel risiko og IKT-risiko hos de kompetente myndigheder, de tre ESA'er og, på frivillig basis, de kompetente myndigheder i henhold til direktiv (EU) 2022/2555, bør den ledende tilsynsførende trække på national tilsynskapacitet og -viden og oprette særlige undersøgelsesteams for hver kritisk tredjepartsudbyder af IKT-tjenester, samle tværfaglige teams til støtte for forberedelsen og udførelsen af tilsynsaktiviteter, herunder generelle undersøgelser og inspektioner hos kritiske tredjepartsudbydere af IKT-tjenester, samt med henblik på enhver nødvendig opfølgning heraf.

(96) Om end omkostninger som følge af tilsynsopgaver vil blive fuldt ud finansieret af gebyrer, der opkræves af kritiske tredjepartsudbydere af IKT-tjenester, vil ESA'erne dog sandsynligvis inden starten af tilsynsrammen pådrage sig omkostninger for gennemførelsen af særlige IKT-systemer, der understøtter det kommende tilsyn, eftersom der på forhånd vil skulle udvikles og deployeres særlige IKT-systemer. Denne forordning indeholder derfor bestemmelser om en hybrid finansieringsmodel, hvorved tilsynsrammen som sådan vil blive fuldt ud finansieret af gebyrer, mens udviklingen af ESA'ernes IKT-systemer vil blive finansieret af bidrag fra Unionen og de nationale kompetente myndigheder.

(97) De kompetente myndigheder bør have alle de påkrævede tilsyns-, undersøgelses- og sanktionsbeføjelser, således at de kan sikre, at de udfører deres opgaver i henhold til denne forordning korrekt. De bør i princippet offentliggøre meddelelser om de administrative sanktioner, de pålægger. Da finansielle enheder og tredjepartsudbydere af IKT-tjenester kan have hjemsted i forskellige medlemsstater og være underlagt forskellige kompetente myndigheders tilsyn, bør anvendelsen af denne forordning lettes, dels af et tæt samarbejde blandt de relevante kompetente myndigheder, herunder ECB for så vidt angår specifikke opgaver, som den er tillagt ved Rådets forordning (EU) nr. 1024/2013, dels af høring af ESA'erne gennem gensidig informationsudveksling og levering af bistand i forbindelse med relevante tilsynsaktiviteter.

(98) For yderligere at kvantificere og kvalificere kriterierne for udpegelsen af tredjepartsudbydere af IKT-tjenester som kritiske og harmonisere tilsynsgebyrerne bør beføjelsen til at vedtage retsakter delegeres til Kommissionen i overensstemmelse med artikel 290 i TEUF for at supplere denne forordning for så vidt angår yderligere præcisering af de systemiske virkninger, som et svigt eller et operationelt driftstop foretaget af en tredjepartsudbyder af IKT-tjenester kan få for de finansielle enheder, den leverer IKT-tjenester til, antallet af globale systemisk vigtige institutter (G-SII'er) eller andre systemisk vigtige institutter (O-SII'er), som er afhængige af den pågældende tredjepartsudbyder af IKT-tjenester, antallet af tredjepartsudbydere af IKT-tjenester, der er aktive på et givet marked, omkostningerne forbundet med at migrere data og IKT-arbejdsbyrden til andre tredjepartsudbydere af IKT-tjenester samt omfanget af tilsynsgebyrerne og den måde, hvorpå de skal betales. Det er navnlig vigtigt, at Kommissionen gennemfører relevante høringer under sit forberedende arbejde, herunder på ekspertniveau, og at disse høringer gennemføres i overensstemmelse med principperne i den interinstitutionelle aftale af 13. april 2016 om bedre lovgivning ([22]). For at sikre lige deltagelse i forberedelsen af delegerede retsakter bør Europa-Parlamentet og Rådet navnlig modtage alle dokumenter på samme tid som medlemsstaternes eksperter, og deres eksperter bør have systematisk adgang til møder i Kommissionens ekspertgrupper, der beskæftiger sig med forberedelse af delegerede retsakter.

(99) Reguleringsmæssige tekniske standarder bør sikre en konsekvent harmonisering af kravene i denne forordning. ESA'erne bør i deres egenskab af organer med højt specialiseret faglig kompetence udarbejde udkast til reguleringsmæssige tekniske standarder, som ikke indebærer politikbeslutninger, med henblik på forelæggelse for Kommissionen. Der bør udarbejdes reguleringsmæssige tekniske standarder på områderne IKT-risikostyring, indberetning af større IKT-relaterede hændelser, test samt i forbindelse med centrale krav med henblik på en forsvarlig overvågning af IKT-tredjepartsrisiko. Kommissionen og ESA'erne bør sikre, at disse standarder og krav kan anvendes af alle finansielle enheder på en måde, der står i rimeligt forhold til deres størrelse og samlede risikoprofil samt karakteren, omfanget og kompleksiteten af deres tjenester, aktiviteter og operationer. Kommissionen bør tillægges beføjelse til at vedtage sådanne reguleringsmæssige tekniske standarder ved hjælp af delegerede retsakter i henhold til artikel 290 i TEUF og i overensstemmelse med artikel 10-14 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.

(100) For at gøre det lettere at sammenligne indberetninger af større IKT-relaterede hændelser og større operationelle eller sikkerhedsmæssige betalingsrelaterede hændelser samt sikre gennemsigtighed med hensyn til kontraktlige ordninger for brugen af IKT-tjenester, der leveres af tredjepartsudbydere af IKT-tjenester, bør ESA'erne udarbejde udkast til gennemførelsesmæssige tekniske standarder, der fastlægger standardiserede modeller, formularer og procedurer, således at finansielle enheder kan indberette en større IKT-relateret hændelse og en større operationel eller sikkerhedsmæssig betalingsrelateret hændelse, samt standardiserede modeller for registret over oplysninger. Når ESA'erne udarbejder disse standarder, bør de tage hensyn til den finansielle enheds størrelse og samlede risikoprofil samt karakteren, omfanget og kompleksiteten af dens tjenester, aktiviteter og operationer. Kommissionen bør tillægges beføjelse til at vedtage sådanne gennemførelsesmæssige tekniske standarder ved hjælp af gennemførelsesretsakter i henhold til artikel 291 i TEUF og i overensstemmelse med artikel 15 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.

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

(101) Da der allerede er fastsat yderligere krav ved delegerede retsakter og gennemførelsesretsakter baseret på de reguleringsmæssige og gennemførelsesmæssige tekniske standarder i Europa-Parlamentets og Rådets forordning (EF) nr. 1060/2009 ([23]), (EU) nr. 648/2012 ([24]), (EU) nr. 600/2014 ([25]) og (EU) nr. 909/2014 ([26]), bør ESA'erne bemyndiges til enten individuelt eller i fællesskab via Det Fælles Udvalg at forelægge reguleringsmæssige og gennemførelsesmæssige tekniske standarder for Kommissionen med henblik på vedtagelse af delegerede retsakter og gennemførelsesretsakter om overførsel og ajourføring af eksisterende regler for IKT-risikostyring.

(102) Eftersom denne forordning sammen med Europa-Parlamentets og Rådets direktiv (EU) 2022/2556 ([27]) for at sikre fuld sammenhæng indebærer en konsolidering af bestemmelserne om IKT-risikostyring i forskellige forordninger og direktiver i gældende EU-ret vedrørende finansielle tjenesteydelser, herunder forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014 og (EU) nr. 909/2014 og Europa-Parlamentets og Rådets forordning (EU) 2016/1011 ([28]), bør nævnte forordninger ændres for at præcisere, at de gældende IKT-risikorelaterede bestemmelser er fastsat i nærværende forordning.

(103) Derfor bør anvendelsesområdet for de relevante artikler vedrørende operationel risiko, i henhold til hvilke de beføjelser, der er fastsat i forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011, gav mandat til vedtagelsen af delegerede retsakter og gennemførelsesretsakter, indskrænkes med henblik på at overføre alle de bestemmelser om aspekterne vedrørende digital operationel modstandsdygtighed, som i dag indgår i nævnte forordninger, til nærværende forordning.

(104) Den potentielle systemiske cyberrisiko, der er forbundet med anvendelsen af IKT-infrastrukturer, som muliggør drift af betalingssystemer og levering af betalingsbehandlingsaktiviteter, bør håndteres behørigt på EU-plan gennem harmoniserede regler om digital modstandsdygtighed. Kommissionen bør derfor hurtigt vurdere behovet for at gennemgå denne forordnings anvendelsesområde og samtidig tilpasse en sådan gennemgang til resultatet af den omfattende gennemgang, der er omhandlet i direktiv (EU) 2015/2366. Talrige storstilede angreb har det seneste årti vist, hvordan betalingssystemer er blevet eksponeret for cybertrusler. Med en central placering i betalingstjenestekæden og stærke indbyrdes forbindelser til det finansielle system som helhed har betalingssystemer og betalingsbehandlingsaktiviteter fået afgørende betydning for, at Unionens finansielle markeder kan fungere. Cyberangreb på sådanne systemer kan forårsage alvorlige operationelle driftsforstyrrelser med direkte konsekvenser for centrale økonomiske funktioner såsom lettelse af betalinger og indirekte virkninger for dermed forbundne økonomiske processer. Indtil der er indført en harmoniseret ordning og tilsyn med operatører af betalingssystemer og behandlingsenheder på EU-plan, kan medlemsstaterne med henblik på at anvende lignende markedspraksisser lade sig inspirere af de krav til digital operationel modstandsdygtighed, der er fastsat i denne forordning, når de anvender regler på operatører af betalingssystemer og behandlingsenheder, der er underlagt tilsyn i deres egne jurisdiktioner.

([23]) Europa-Parlamentets og Rådets forordning (EF) nr. 1060/2009 af 16. september 2009 om kreditvurderingsbureauer (EUT L 302 af 17.11.2009, s. 1).

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

([25]) Europa-Parlamentets og Rådets forordning (EU) nr. 600/2014 af 15. maj 2014 om markeder for finansielle instrumenter og om ændring af forordning (EU) nr. 648/2012 (EUT L 173 af 12.6.2014, s. 84).

([26]) Europa-Parlamentets og Rådets forordning (EU) nr. 909/2014 af 23. juli 2014 om forbedring af værdipapirafviklingen i Den Europæiske Union og om værdipapircentraler samt om ændring af direktiv 98/26/EF og 2014/65/EU samt forordning (EU) nr. 236/2012 (EUT L 257 af 28.8.2014, s. 1).

([27]) Europa-Parlamentets og Rådets direktiv (EU) 2022/2556 af 14. december 2022 om ændring af direktiv 2009/65/EF, 2009/138/EF, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 og (EU) 2016/2341 for så vidt angår digital operationel modstandsdygtighed i den finansielle sektor (se side 153 i denne EUT).

([28]) Europa-Parlamentets og Rådets forordning (EU) 2016/1011 af 8. juni 2016 om indeks, der bruges som benchmarks i finansielle instrumenter og finansielle kontrakter eller med henblik på at måle investeringsfondes økonomiske resultater, og om ændring af direktiv 2008/48/EF og 2014/17/EU samt forordning (EU) nr. 596/2014 (EUT L 171 af 29.6.2016, s. 1).

(105) Målet for denne forordning, nemlig at opnå et højt niveau af digital operationel modstandsdygtighed for regulerede finansielle enheder, kan ikke i tilstrækkelig grad opfyldes af medlemsstaterne, fordi det kræver harmonisering af flere forskellige regler i EU-retten og national ret, men kan på grund af dens omfang og virkninger bedre nås på EU-plan; Unionen kan derfor vedtage foranstaltninger i overensstemmelse med nærhedsprincippet, jf. artikel 5 i traktaten om Den Europæiske Union. I overensstemmelse med proportionalitetsprincippet, jf. nævnte artikel, går denne forordning ikke videre, end hvad der er nødvendigt for at nå dette mål.

(106) Den Europæiske Tilsynsførende for Databeskyttelse er blevet hørt i overensstemmelse med artikel 42, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) 2018/1725 ([29]) og afgav en udtalelse den 10. maj 2021 ([30]) —

VEDTAGET DENNE FORORDNING:

KAPITEL I

Almindelige bestemmelser

Artikel 1

Genstand

1. For at opnå et højt fælles niveau af digital operationel modstandsdygtighed fastsætter denne forordning ensartede krav til sikkerheden i de net- og informationssystemer, der understøtter finansielle enheders forretningsprocesser på følgende måde:

a) krav til finansielle enheder vedrørende:

   i) risikostyring inden for informations- og kommunikationsteknologi (IKT)

   ii) indberetning af større IKT-relaterede hændelser og underretning, på frivillig basis, om væsentlige cybertrusler til de kompetente myndigheder

   iii) indberetning af større operationelle eller sikkerhedsmæssige betalingsrelaterede hændelser til de kompetente myndigheder fra de finansielle enheder, der er omhandlet i artikel 2, stk. 1, litra a)-d)

   iv) test af digital operationel modstandsdygtighed

   v) udveksling af oplysninger og efterretninger om cybertrusler og sårbarheder

   vi) foranstaltninger til forsvarlig styring af IKT-tredjepartsrisiko

b) krav vedrørende de kontraktlige ordninger, der indgås mellem tredjepartsudbydere af IKT-tjenester og finansielle enheder

c) regler for fastlæggelse og udførelse af tilsynsrammen for kritiske tredjepartsudbydere af IKT-tjenester, når de leverer tjenester til finansielle enheder

d) regler om samarbejde mellem kompetente myndigheder og regler om de kompetente myndigheders tilsyn og håndhævelse i forbindelse med alle spørgsmål, der er omfattet af denne forordning.

2. For så vidt angår finansielle enheder, der er identificeret som væsentlige eller vigtige enheder i henhold til nationale bestemmelser om gennemførelse af artikel 3 i direktiv (EU) 2022/2555, betragtes denne forordning som en sektorspecifik EU-retsakt med henblik på artikel 4 i nævnte direktiv.

3. Denne forordning berører ikke medlemsstaternes ansvar for så vidt angår væsentlige statslige funktioner vedrørende offentlig sikkerhed, forsvar og national sikkerhed i overensstemmelse med EU-retten.

([29]) 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).

([30]) EUT C 229 af 15.6.2021, s. 16.

Artikel 2

Anvendelsesområde

1. Med forbehold af stk. 3 og 4 finder denne forordning anvendelse på følgende enheder:

a) kreditinstitutter

b) betalingsinstitutter, herunder betalingsinstitutter, der er undtaget i henhold til direktiv (EU) 2015/2366

c) kontooplysningstjenesteudbydere

d) e-pengeinstitutter, herunder e-pengeinstitutter, der er undtaget i henhold til direktiv 2009/110/EF

e) investeringsselskaber

f) udbydere af kryptoaktivtjenester, som er meddelt tilladelse i henhold til Europa-Parlamentets og Rådets forordning om markeder for kryptoaktiver og om ændring af forordning (EU) nr. 1093/2010 og (EU) nr. 1095/2010 og direktiv 2013/36/EU og (EU) 2019/1937 (»forordningen om markeder for kryptoaktiver«), og udstedere af aktivbaserede tokens

g) værdipapircentraler

h) centrale modparter

i) markedspladser

j) transaktionsregistre

k) forvaltere af alternative investeringsfonde

l) administrationsselskaber

m) udbydere af dataindberetningstjenester

n) forsikrings- og genforsikringsselskaber

o) forsikringsformidlere, genforsikringsformidlere og accessoriske forsikringsformidlere

p) arbejdsmarkedsrelaterede pensionskasser

q) kreditvurderingsbureauer

r) administratorer af kritiske benchmarks

s) udbydere af crowdfundingtjenester

t) securitiseringsregistre

u) tredjepartsudbydere af IKT-tjenester.

2. Med henblik på denne forordning benævnes de enheder, der er omhandlet i stk. 1, litra a)-t), samlet »finansielle enheder«.

3. Denne forordning finder ikke anvendelse på:

a) forvaltere af alternative investeringsfonde, der er omhandlet i artikel 3, stk. 2, i direktiv 2011/61/EU

b) forsikrings- og genforsikringsselskaber, der er omhandlet i artikel 4 i direktiv 2009/138/EF

c) arbejdsmarkedsrelaterede pensionskasser, som forvalter pensionsordninger, som tilsammen ikke har mere end 15 medlemmer i alt

d) fysiske eller juridiske personer, der er undtaget i henhold til artikel 2 og 3 i direktiv 2014/65/EU

e) forsikringsformidlere, genforsikringsformidlere og accessoriske forsikringsformidlere, som er mikrovirksomheder eller små eller mellemstore virksomheder

f) postgirokontorer, der er omhandlet i artikel 2, stk. 5, nr. 3), i direktiv 2013/36/EU.

4. Medlemsstaterne kan undtage de enheder, som er omhandlet i artikel 2, stk. 5, nr. 4)-23), i direktiv 2013/36/EU, og som er beliggende på deres respektive områder, fra denne forordnings anvendelsesområde. Hvis en medlemsstat gør brug af denne mulighed, underretter den Kommissionen herom og om eventuelle efterfølgende ændringer heraf. Kommissionen gør disse oplysninger offentligt tilgængelige på sit websted eller på anden let tilgængelig måde.

Artikel 3

Definitioner

I denne forordning forstås ved:

1) »digital operationel modstandsdygtighed«: en finansiel enheds evne til at opbygge, sikre og gennemgå sin operationelle integritet og pålidelighed ved enten direkte eller indirekte gennem anvendelse af tjenester, der leveres af en tredjepart-sudbyder af IKT-tjenester, at sikre det fulde spektrum af nødvendige IKT-relaterede kapaciteter med henblik på at varetage sikkerheden i de net- og informationssystemer, som en finansiel enhed anvender, og som understøtter det løbende udbud af finansielle tjenesteydelser og kvaliteten heraf, herunder i forbindelse med forstyrrelser

2) »net- og informationssystem«: et net- og informationssystem som defineret i artikel 6, nr. 1), i direktiv (EU) 2022/2555

3) »legacy-IKT-system«: et IKT-system, som har nået enden på sin livscyklus (end-of-life), som af teknologiske eller kommercielle årsager ikke er egnet til opgraderinger eller udbedringer, eller som ikke længere understøttes af leverandøren eller af en tredjepartsudbyder af IKT-tjenester, men som stadig er i brug og understøtter den finansielle enheds funktioner

4) »sikkerhed i net- og informationssystemer«: sikkerhed i net- og informationssystemer som defineret i artikel 6, nr. 2), i direktiv (EU) 2022/2555

5) »IKT-risiko«: enhver rimeligt identificerbar omstændighed i forbindelse med brugen af net- og informationssystemer, som, hvis den forekommer, kan kompromittere sikkerheden i net- og informationssystemerne, i eventuelle teknologiafhængige værktøjer eller processer, i operationer og processer, eller i forbindelse med leveringen af tjenester, ved at skabe negative virkninger i det digitale eller fysiske miljø

6) »informationsaktiv«: en samling af oplysninger, både materielle og immaterielle, som det er værd at beskytte

7) »IKT-aktiv«: et software- eller hardwareaktiv i de net- og informationssystemer, der anvendes af den finansielle enhed

8) »IKT-relateret hændelse«: en enkeltstående hændelse eller en række af forbundne hændelser, som ikke har været planlagt af den finansielle enhed, og som kompromitterer sikkerheden i net- og informationssystemerne og har en negativ indvirkning på tilgængeligheden, autenticiteten, integriteten eller fortroligheden af data eller på de tjenester, som den finansielle enhed leverer

9) »operationel eller sikkerhedsmæssig betalingsrelateret hændelse«: en enkeltstående hændelse eller en række af forbundne hændelser, som ikke har været planlagt af de finansielle enheder, der er omhandlet i artikel 2, stk. 1, litra a)-d), uanset om de er IKT-relaterede eller ej, og som har en negativ indvirkning på tilgængeligheden, autenticiteten, integriteten eller fortroligheden af betalingsrelaterede data eller på de betalingsrelaterede tjenester, der leveres af den finansielle enhed

10) »større IKT-relateret hændelse«: en IKT-relateret hændelse, som har en stor negativ indvirkning på net- og informationssystemer, som understøtter kritiske eller vigtige funktioner i den finansielle enhed

11) »større operationel eller sikkerhedsmæssig betalingsrelateret hændelse«: en operationel eller sikkerhedsmæssig betalingsrelateret hændelse, som har en stor negativ indvirkning på de betalingsrelaterede tjenester, der leveres

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

13) »væsentlig cybertrussel«: en cybertrussel, hvis tekniske karakteristika indikerer, at den potentielt kan resultere i en større IKT-relateret hændelse eller en større operationel eller sikkerhedsmæssig betalingsrelateret hændelse

14) »cyberangreb«: en ondsindet IKT-relateret hændelse, som er forårsaget af en trusselsaktørs forsøg på ødelæggelse, eksponering, ændring, deaktivering, tyveri af eller opnåelse af uautoriseret adgang til eller uautoriseret brug af et aktiv

15) »trusselsefterretning«: oplysninger, der er blevet sammenfattet, omdannet, analyseret, fortolket eller beriget for at skabe den nødvendige kontekst for beslutningstagning og for at muliggøre relevant og tilstrækkelig forståelse med henblik på at afbøde virkningerne af en IKT-relateret hændelse eller af en cybertrussel, herunder de tekniske detaljer ved et cyberangreb, kendskab til dem, der er ansvarlige for angrebet, deres måde at operere på og deres hensigter

16) »sårbarhed«: en svaghed, følsomhed eller fejl i forbindelse med et aktiv, et system, en proces eller en kontrolfunktion, som kan udnyttes

17) »trusselsbaseret penetrationstest (TLPT)«: en ramme, der efterligner de taktikker, teknikker og procedurer, som bruges af rigtige trusselsaktører og betragtes som reelle cybertrusler, og som muliggør en kontrolleret, skræddersyet, efterretningsbaseret (red team-) test af den finansielle enheds kritiske live-produktionssystemer

18) »IKT-tredjepartsrisiko«: en IKT-risiko, der kan opstå for en finansiel enhed i forbindelse med dens brug af IKT-tjenester, der leveres af tredjepartsudbydere af IKT-tjenester eller af sidstnævntes underleverandører, herunder gennem ordninger for outsourcing

19) »tredjepartsudbyder af IKT-tjenester«: en virksomhed, der leverer IKT-tjenester

20) »koncernintern udbyder af IKT-tjenester«: en virksomhed, som er en del af en finansiel koncern, og som hovedsagelig leverer IKT-tjenester til finansielle enheder inden for samme koncern eller til finansielle enheder, der tilhører samme institutsikringsordning, herunder til deres moderselskaber, datterselskaber, filialer eller andre enheder, der er under fælles ejerskab eller kontrol

21) »IKT-tjenester«: digitale tjenester og datatjenester, der løbende leveres gennem IKT-systemer til én eller flere interne eller eksterne brugere, herunder hardware som en tjeneste og hardwaretjenester, som omfatter hardwareudbyderens levering af teknisk support via software- eller firmwareopdateringer, eksklusive traditionelle analoge telefonitjenester

22) »kritisk eller vigtig funktion«: en funktion, hvis forstyrrelse i væsentlig grad kan forringe en finansiel enheds finansielle resultater, eller robustheden eller kontinuiteten af dens tjenester og aktiviteter, eller som, hvis den pågældende funktion afbrydes, er fejlbehæftet eller mislykkes, i væsentlig grad kan forringe en finansiel enheds opfyldelse af de betingelser og forpligtelser, der er forbundet med dens tilladelse, eller af dens andre forpligtelser i henhold til gældende finansiel tjenesteydelsesret

23) »kritisk tredjepartsudbyder af IKT-tjenester«: en tredjepartsudbyder af IKT-tjenester, der er udpeget som kritisk i overensstemmelse med artikel 31

24) »tredjepartsudbyder af IKT-tjenester med hjemsted i et tredjeland«: en tredjepartsudbyder af IKT-tjenester, som er en juridisk person med hjemsted i et tredjeland, og som har indgået kontraktlige ordninger med en finansiel enhed om levering af IKT-tjenester

25) »dattervirksomhed«: en dattervirksomhed i den i artikel 2, nr. 10), og artikel 22 i direktiv 2013/34/EU anvendte betydning

26) »koncern«: en koncern som defineret i artikel 2, nr. 11), i direktiv 2013/34/EU

27) »modervirksomhed«: en modervirksomhed i den i artikel 2, nr. 9), og artikel 22 i direktiv 2013/34/EU anvendte betydning

28) »IKT-underleverandør med hjemsted i et tredjeland«: en IKT-underleverandør, som er en juridisk person med hjemsted i et tredjeland, og som har indgået kontraktlige ordninger enten med en tredjepartsudbyder af IKT-tjenester eller med en tredjepartsudbyder af IKT-tjenester med hjemsted i et tredjeland

29) »IKT-koncentrationsrisiko«: eksponering for individuelle eller flere indbyrdes forbundne kritiske tredjepartsudbydere af IKT-tjenester, som skaber en grad af afhængighed af sådanne udbydere, der bevirker, at manglende tilgængelighed, svigt eller andre typer af mangler i forbindelse med en sådan udbyder kan være til fare for en finansiel enheds evne til at varetage kritiske eller vigtige funktioner eller medføre andre former for negative virkninger for den, herunder store tab, eller være til fare for den finansielle stabilitet i Unionen som helhed

30) »ledelsesorgan«: et ledelsesorgan som defineret i artikel 4, stk. 1, nr. 36), i direktiv 2014/65/EU, artikel 3, stk. 1, nr. 7), i direktiv 2013/36/EU, artikel 2, stk. 1, litra s), i Europa-Parlamentets og Rådets direktiv 2009/65/EF ([31]), artikel 2, stk. 1, nr. 45), i forordning (EU) nr. 909/2014, artikel 3, stk. 1, nr. 20), i forordning (EU) 2016/1011 og i den relevante bestemmelse i forordningen om markeder for kryptoaktiver, eller dertil svarende personer, som varetager den faktiske drift af enheden eller nøglefunktioner i overensstemmelse med relevant EU-ret eller national ret

31) »kreditinstitut«: kreditinstitut som defineret i artikel 4, stk. 1, nr. 1), i Europa-Parlamentets og Rådets forordning (EU) nr. 575/2013 ([32])

32) »institut, der er fritaget i henhold til direktiv 2013/36/EU«: en enhed som omhandlet i artikel 2, stk. 5, nr. 4)-23), i direktiv 2013/36/EU

33) »investeringsselskab«: et investeringsselskab som defineret i artikel 4, stk. 1, nr. 1), i direktiv 2014/65/EU

34) »lille og ikke indbyrdes forbundet investeringsselskab«: et investeringsselskab, som opfylder de betingelser, der er fastsat i artikel 12, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) 2019/2033 ([33])

35) »betalingsinstitut«: et betalingsinstitut som defineret i artikel 4, nr. 4), i direktiv (EU) 2015/2366

36) »betalingsinstitut, der er undtaget i henhold til direktiv (EU) 2015/2366«: et betalingsinstitut, der er undtaget i henhold til artikel 32, stk. 1, i direktiv (EU) 2015/2366

37) »kontooplysningstjenesteudbyder«: en kontooplysningstjenesteudbyder, jf. artikel 33, stk. 1, i direktiv (EU) 2015/2366

38) »e-pengeinstitut«: et e-pengeinstitut som defineret i artikel 2, nr. 1), i direktiv 2009/110/EF

39) »e-pengeinstitut, der er undtaget i henhold til direktiv 2009/110/EF«: et e-pengeinstitut, der er omfattet af en undtagelse som omhandlet i artikel 9, stk. 1, i direktiv 2009/110/EF

40) »central modpart«: en central modpart som defineret i artikel 2, nr. 1), i forordning (EU) nr. 648/2012

41) »transaktionsregister«: et transaktionsregister som defineret i artikel 2, nr. 2), i forordning (EU) nr. 648/2012

42) »værdipapircentral«: en værdipapircentral som defineret i artikel 2, stk. 1, nr. 1), i forordning (EU) nr. 909/2014

43) »markedsplads«: en markedsplads som defineret i artikel 4, stk. 1, nr. 24), i direktiv 2014/65/EU

44) »forvalter af alternative investeringsfonde«: en forvalter af alternative investeringsfonde som defineret i artikel 4, stk. 1, litra b), i direktiv 2011/61/EU

45) »administrationsselskab«: et administrationsselskab som defineret i artikel 2, stk. 1, litra b), i direktiv 2009/65/EF

46) »udbyder af dataindberetningstjenester«: en udbyder af dataindberetningstjenester i den i forordning (EU) nr. 600/2014 anvendte betydning, jf. artikel 2, stk. 1, nr. 34)-36) deraf

47) »forsikringsselskab«: et forsikringsselskab som defineret i artikel 13, nr. 1), i direktiv 2009/138/EF

48) »genforsikringsselskab«: et genforsikringsselskab som defineret i artikel 13, nr. 4), i direktiv 2009/138/EF

([31]) Europa-Parlamentets og Rådets direktiv 2009/65/EF af 13. juli 2009 om samordning af love og administrative bestemmelser om visse institutter for kollektiv investering i værdipapirer (investeringsinstitutter) (EUT L 302 af 17.11.2009, s. 32).

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

([33]) Europa-Parlamentets og Rådets forordning (EU) 2019/2033 af 27. november 2019 om tilsynsmæssige krav til investeringsselskaber og om ændring af forordning (EU) nr. 1093/2010, (EU) nr. 575/2013, (EU) nr. 600/2014 og (EU) nr. 806/2014 (EUT L 314 af 5.12.2019, s. 1).

49) »forsikringsformidler«: en forsikringsformidler som defineret i artikel 2, stk. 1, nr. 3), i Europa-Parlamentets og Rådets direktiv (EU) 2016/97 ([34])

50) »accessorisk forsikringsformidler«: en accessorisk forsikringsformidler som defineret i artikel 2, stk. 1, nr. 4), i direktiv (EU) 2016/97

51) »genforsikringsformidler«: en genforsikringsformidler som defineret i artikel 2, stk. 1, nr. 5), i direktiv (EU) 2016/97

52) »arbejdsmarkedsrelateret pensionskasse«: en arbejdsmarkedsrelateret pensionskasse som defineret i artikel 6, nr. 1), i direktiv (EU) 2016/2341

53) »lille arbejdsmarkedsrelateret pensionskasse«: en arbejdsmarkedsrelateret pensionskasse, der forvalter pensionsordninger, som tilsammen har mindre end 100 medlemmer i alt

54) »kreditvurderingsbureau«: et kreditvurderingsbureau som defineret i artikel 3, stk. 1, litra b), i forordning (EF) nr. 1060/2009

55) »udbyder af kryptoaktivtjenester«: en udbyder af kryptoaktivtjenester som defineret i den relevante bestemmelse i forordningen om markeder for kryptoaktiver

56) »udsteder af aktivbaserede tokens«: en udsteder af »aktivbaserede tokens« som defineret i den relevante bestemmelse i forordningen om markeder for kryptoaktiver

57) »administrator af kritiske benchmarks«: en administrator af »kritiske benchmarks« som defineret i artikel 3, stk. 1, nr. 25), i forordning (EU) 2016/1011

58) »udbyder af crowdfundingtjenester«: en udbyder af crowdfundingtjenester som defineret i artikel 2, stk. 1, litra e), i Europa-Parlamentets og Rådets forordning (EU) 2020/1503 ([35])

59) »securitiseringsregister«: et securitiseringsregister som defineret i artikel 2, nr. 23), i Europa-Parlamentets og Rådets forordning (EU) 2017/2402 ([36])

60) »mikrovirksomhed«: en finansiel enhed, som ikke er en markedsplads, en central modpart, et transaktionsregister eller en værdipapircentral, med mindre end 10 ansatte og en årlig omsætning og/eller en årlig samlet balance på højst 2 mio. EUR

61) »ledende tilsynsførende«: den europæiske tilsynsmyndighed, som er udpeget i overensstemmelse med denne forordnings artikel 31, stk. 1, litra b)

62) »Det Fælles Udvalg«: det udvalg, som er omhandlet i artikel 54 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010

63) »lille virksomhed«: en finansiel enhed med 10 eller flere ansatte men med mindre end 50 ansatte og en årlig omsætning og/eller en årlig samlet balance, der overstiger 2 mio. EUR men på højst 10 mio. EUR

64) »mellemstor virksomhed«: en finansiel enhed, som ikke er en lille virksomhed, med mindre end 250 ansatte og en årlig omsætning på højst 50 mio. EUR og/eller en årlig balance på højst 43 mio. EUR

65) »offentlig myndighed«: enhver offentlig enhed eller anden offentlig forvaltningsenhed, herunder nationale centralbanker.

([34]) Europa-Parlamentets og Rådets direktiv (EU) 2016/97 af 20. januar 2016 om forsikringsdistribution (EUT L 26 af 2.2.2016, s. 19).

([35]) Europa-Parlamentets og Rådets forordning (EU) 2020/1503 af 7. oktober 2020 om europæiske crowdfundingtjenesteudbydere for erhvervslivet og om ændring af forordning (EU) 2017/1129 og direktiv (EU) 2019/1937 (EUT L 347 af 20.10.2020, s. 1).

([36]) Europa-Parlamentets og Rådets forordning (EU) 2017/2402 af 12. december 2017 om en generel ramme for securitisering og om oprettelse af en specifik ramme for simpel, transparent og standardiseret securitisering og om ændring af direktiv 2009/65/EF, 2009/138/EF og 2011/61/EU og forordning (EF) nr. 1060/2009 og (EU) nr. 648/2012 (EUT L 347 af 28.12.2017, s. 35).

Artikel 4

Proportionalitetsprincippet

1. Finansielle enheder gennemfører de regler, der er fastsat i kapitel II i overensstemmelse med proportionalitetsprincippet, under hensyntagen til deres størrelse og samlede risikoprofil samt karakteren, omfanget og kompleksiteten af deres tjenester, aktiviteter og operationer.

2. Desuden skal finansielle enheders anvendelse af kapitel III, IV og kapitel V, afdeling I, stå i et rimeligt forhold til deres størrelse og samlede risikoprofil og til karakteren, omfanget og kompleksiteten af deres tjenester, aktiviteter og operationer, som specifikt fastsat i de relevante regler i de nævnte kapitler.

3. De kompetente myndigheder tager hensyn til finansielle enheders anvendelse af proportionalitetsprincippet, når de gennemgår sammenhængen i rammen for IKT-risikostyring på grundlag af de indberetninger, som indgives efter anmodning fra de kompetente myndigheder i henhold til artikel 6, stk. 5, og artikel 16, stk. 2.

KAPITEL II

IKT-risikostyring

Afdeling I

Artikel 5

Forvaltning og organisation

1. Finansielle enheder skal have indført en intern forvaltnings- og kontrolramme, der sikrer en effektiv og forsigtig styring af IKT-risiko, i overensstemmelse med artikel 6, stk. 4, for at opnå et højt niveau af digital operationel modstandsdygtighed.

2. Ledelsesorganet i den finansielle enhed fastlægger, godkender, fører tilsyn med og har ansvar for gennemførelsen af alle ordninger vedrørende de rammer for IKT-risikostyring, der er omhandlet i artikel 6, stk. 1.

Med henblik på første afsnit er det ledelsesorganet, som

a) har det endelige ansvar for styringen af den finansielle enheds IKT-risiko

b) indfører politikker, der har til formål at sikre opretholdelse af høje standarder for tilgængeligheden, autenticiteten, integriteten og fortroligheden af data

c) fastlægger klare roller og ansvarsområder for alle IKT-relaterede funktioner og etablerer passende forvaltningsordninger for at sikre effektiv og rettidig kommunikation, samarbejde og koordinering mellem disse funktioner

d) har det samlede ansvar for fastlæggelse og godkendelse af strategien for digital operationel modstandsdygtighed, jf. artikel 6, stk. 8, herunder fastsættelse af et passende risikotoleranceniveau for IKT-risiko i den finansielle enhed, jf. artikel 6, stk. 8, litra b)

e) godkender, fører tilsyn med og regelmæssigt gennemgår gennemførelsen af den finansielle enheds politik for IKT-driftsstabilitet og planer for IKT-indsats og -genopretning, jf. henholdsvis artikel 11, stk. 1 og 3, der kan vedtages som en særlig specifik politik, der udgør en integrerende del af den finansielle enheds samlede politik for driftsstabilitet og indsats- og genopretningsplan

f) godkender og regelmæssigt gennemgår den finansielle enheds interne IKT-revisionsplaner, IKT-revisioner og væsentlige ændringer heraf

g) tildeler og regelmæssigt gennemgår et passende budget for at opfylde den finansielle enheds behov i forbindelse med digital operationel modstandsdygtighed med hensyn til alle ressourcetyper, herunder relevante IKT-programmer til bevidstgørelse om IKT-sikkerhed og kurser i digital operationel modstandsdygtighed, jf. artikel 13, stk. 6, og IKT-færdigheder for alt personale

h) godkender og regelmæssigt gennemgår den finansielle enheds politik vedrørende ordninger for brug af IKT-tjenester, der leveres af tredjepartsudbydere af IKT-tjenester

i) indfører indberetningskanaler på virksomhedsniveau, der gør det muligt for det at blive behørigt underrettet om følgende:

   i) ordninger, der er indgået med tredjepartsudbydere af IKT-tjenester vedrørende brugen af IKT-tjenester

   ii) relevante planlagte væsentlige ændringer, som vedrører tredjepartsudbydere af IKT-tjenester

   iii) potentielle virkninger af sådanne ændringer på de kritiske eller vigtige funktioner, der er omfattet af disse ordninger, herunder en sammenfatning af risikoanalysen med henblik på at vurdere virkningerne af disse ændringer og som minimum større IKT-relaterede hændelser og deres virkninger samt indsatsforanstaltninger, genopretningsforanstaltninger og korrigerende foranstaltninger.

3. Finansielle enheder, som ikke er mikrovirksomheder, skal oprette en funktion med henblik på overvågning af de ordninger, der er indgået med tredjepartsudbydere af IKT-tjenester vedrørende brugen af IKT-tjenester, eller udpege et medlem af den øverste ledelse som tilsynsansvarlig for den dermed forbundne risikoeksponering og relevante dokumentation.

4. Medlemmerne af den finansielle enheds ledelsesorgan holder aktivt den viden og de færdigheder, der er nødvendige for at forstå og vurdere IKT-risiko og dens indvirkning på den finansielle enheds drift, ajour, herunder ved regelmæssigt at følge særlige kurser, svarende til den IKT-risiko, der styres.

Afdeling II

Artikel 6

Ramme for IKT-risikostyring

1. Finansielle enheder indfører en robust, omfattende og veldokumenteret ramme for IKT-risikostyring som en del af deres samlede risikostyringssystem, der sætter dem i stand til at håndtere IKT-risikoen hurtigt, effektivt og fyldestgørende, og som sikrer et højt niveau af digital operationel modstandsdygtighed.

2. Rammen for IKT-risikostyring skal som minimum omfatte strategier, politikker, procedurer, IKT-protokoller og -værktøjer, som er nødvendige for på behørig vis og i tilstrækkelig grad at beskytte alle informationsaktiver og IKT-aktiver, herunder computersoftware, -hardware og servere, samt for at beskytte alle relevante fysiske komponenter og infrastrukturer, såsom lokaler, datacentre og sensitive udpegede områder, for at sikre tilstrækkelig beskyttelse af alle informationsaktiver og IKT-aktiver mod risici, herunder skade og uautoriseret adgang eller brug.

3. I overensstemmelse med deres ramme for IKT-risikostyring minimerer de finansielle enheder virkningerne af IKT-risiko ved at indføre passende strategier, politikker, procedurer, IKT-protokoller og -værktøjer. De forelægger fuldstændige og ajourførte oplysninger om IKT-risiko og om deres ramme for IKT-styring for de kompetente myndigheder på disses anmodning.

4. Finansielle enheder, som ikke er mikrovirksomheder, overdrager ansvaret for styring af og tilsyn med IKT-risikoen til en kontrolfunktion og sikrer, at denne kontrolfunktion har et passende uafhængighedsniveau, således at interessekonflikter undgås. Finansielle enheder sikrer en passende adskillelse og uafhængighed af IKT-risikostyringsfunktioner, kontrolfunktioner og interne revisionsfunktioner efter modellen med tre forsvarslinjer eller en intern model for risikostyring og kontrol.

5. Rammen for IKT-risikostyring skal dokumenteres og gennemgås mindst én gang om året, eller regelmæssigt for så vidt angår mikrovirksomheder, samt når der forekommer større IKT-relaterede hændelser, og i henhold til tilsynsmæssige instrukser eller konklusioner, som er udledt af relevant test af digital operationel modstandsdygtighed eller revisionsprocesser. Den skal forbedres løbende på grundlag af indhøstede gennemførelses- og overvågningserfaringer. Der skal forelægges en rapport om gennemgangen af rammen for IKT-risikostyring for den kompetente myndighed på dens anmodning.

6. Revisorer foretager regelmæssigt intern revision af rammen for IKT-risikostyring for andre finansielle enheder end mikrovirksomheder i overensstemmelse med de finansielle enheders revisionsplan. Disse revisorer skal besidde tilstrækkelig viden, faglig kompetence og ekspertise med hensyn til IKT-risici og være tilstrækkeligt uafhængige. Hyppigheden af IKT-revisioner og deres fokus skal stå i rimeligt forhold til den finansielle enheds IKT-risiko.

7. De finansielle enheder etablerer på baggrund af konklusioner fra den interne revisionsgennemgang en formel opfølgningsproces, herunder regler for rettidig efterprøvning og udbedring af kritiske resultater af IKT-revisioner.

8. Rammen for IKT-risikostyring skal omfatte en strategi for digital operationel modstandsdygtighed, der fastsætter, hvordan rammen gennemføres. Med henblik herpå skal strategien for digital operationel modstandsdygtighed omfatte metoderne til håndtering af IKT-risiko og opfylde specifikke IKT-mål ved at

a) redegøre for, hvordan rammen for IKT-risikostyring understøtter den finansielle enheds forretningsstrategi og -mål

b) fastlægge risikotoleranceniveauet for IKT-risiko i overensstemmelse med den finansielle enheds risikovillighed og analysere tolerancen over for virkninger af IKT-forstyrrelser

c) fastsætte klare informationssikkerhedsmål, herunder centrale resultatindikatorer og centrale risikoparametre

d) redegøre for IKT-referencearkitekturen og eventuelle ændringer, der er nødvendige for at nå specifikke forretningsmål

e) beskrive de forskellige indførte mekanismer til detektion af IKT-relaterede hændelser, forebygge deres virkning og give beskyttelse mod den

f) dokumentere den nuværende situation for den digitale operationelle modstandsdygtighed på grundlag af antallet af indberettede større IKT-relaterede hændelser og de forebyggende foranstaltningers effektivitet

g) gennemføre test af digital operationel modstandsdygtighed i overensstemmelse med denne forordnings kapitel IV

h) fastlægge en kommunikationsstrategi i tilfælde af IKT-relaterede hændelser, hvis offentliggørelse er påkrævet i henhold til artikel 14.

9. Finansielle enheder kan i forbindelse med strategien for digital operationel modstandsdygtighed som omhandlet i stk. 8 fastlægge en helhedsorienteret strategi med flere IKT-udbydere på koncern- eller enhedsplan, som viser, hvor der er stor afhængighed af tredjepartsudbydere af IKT-tjenester, og begrunde den pågældende udbudssammensætning af tredjepartsudbydere af IKT-tjenester.

10. Finansielle enheder kan i overensstemmelse med sektorspecifik EU-ret og national ret outsource de opgaver, der er forbundet med efterprøvning af overholdelsen af kravene til IKT-risikostyring, til koncerninterne eller eksterne virksomheder. I tilfælde af en sådan outsourcing er den finansielle enhed fortsat fuldt ud ansvarlig for at efterprøve overholdelsen af kravene til IKT-risikostyring.

Artikel 7

IKT-systemer, -protokoller og-værktøjer

For at håndtere og styre IKT-risikoen anvender og vedligeholder finansielle enheder opdaterede IKT-systemer, -protokoller og -værktøjer, som er:

a) passende i forhold til omfanget af de operationer, der ligger til grund for gennemførelsen af deres aktiviteter, i overensstemmelse med proportionalitetsprincippet som omhandlet i artikel 4

b) pålidelige

c) udstyret med tilstrækkelig kapacitet til med nøjagtighed at behandle de data, der er nødvendige for udførelsen af aktiviteterne og rettidig levering af tjenesterne, og til at håndtere spidsbelastninger, ordre- og meddelelsesmængder eller transaktionsmængder efter behov, herunder når der indføres ny teknologi

d) teknologisk modstandsdygtige nok til i tilstrækkeligt omfang at håndtere yderligere behov for informationsbehandling som krævet under stressede markedsforhold eller i andre vanskelige situationer.

Artikel 8

Identifikation

1. Som led i den ramme for IKT-risikostyring, der er omhandlet i artikel 6, stk. 1, foretager de finansielle enheder identifikation, klassificering og tilstrækkelig dokumentering af alle IKT-understøttede forretningsfunktioner, roller og ansvarsområder, informationsaktiver og IKT-aktiver, der understøtter disse funktioner, samt deres roller og afhængigheder med hensyn til IKT-risici. De finansielle enheder vurderer efter behov og mindst én gang om året, hvorvidt denne klassificering og eventuel relevant dokumentation er tilstrækkelig.

2. De finansielle enheder identificerer løbende alle kilder til IKT-risiko, navnlig risikoeksponeringen for og fra andre finansielle enheder, og vurderer cybertrusler og IKT-sårbarheder, der er relevante for deres IKT-understøttede forretningsfunktioner, informationsaktiver og IKT-aktiver. De finansielle enheder gennemgår regelmæssigt og mindst én gang om året de risikoscenarier, der har virkninger for dem.

3. Finansielle enheder, som ikke er mikrovirksomheder, foretager en risikovurdering efter hver større ændring af infrastrukturen i net- og informationssystemerne, i de processer eller procedurer, der påvirker deres IKT-understøttede forretningsfunktioner, informationsaktiver eller IKT-aktiver.

4. De finansielle enheder identificerer alle informationsaktiver og IKT-aktiver, herunder på eksterne steder, netværksressourcer og hardwareudstyr, og kortlægger dem, der anses for kritiske. De kortlægger informationsaktivernes og IKT-aktivernes konfiguration samt forbindelserne og den indbyrdes forbundethed mellem de forskellige informationsaktiver og IKT-aktiver.

5. De finansielle enheder identificerer og dokumenterer alle processer, der er afhængige af tredjepartsudbydere af IKT-tjenester, og identificerer sammenkoblinger med tredjepartsudbydere af IKT-tjenester, der udbyder tjenester, som understøtter kritiske eller vigtige funktioner.

6. Med henblik på stk. 1, 4 og 5 opretholder finansielle enheder relevante fortegnelser og ajourfører dem regelmæssigt, og hver gang der sker større ændringer som omhandlet i stk. 3.

7. Finansielle enheder, som ikke er mikrovirksomheder, foretager regelmæssigt og mindst én gang om året en specifik IKT-risikovurdering af alle legacy-IKT-systemer og i alle tilfælde før og efter sammenkobling af teknologier, applikationer eller systemer.

Artikel 9

Beskyttelse og forebyggelse

1. Med henblik på at sikre passende beskyttelse af IKT-systemer og tilrettelægge indsatsforanstaltninger sikrer de finansielle enheder løbende overvågning af og kontrol med IKT-systemernes og -værktøjernes sikkerhed og af, hvordan de fungerer, og minimerer virkningerne af IKT-risikoen for IKT-systemer ved at indføre passende IKT-sikkerhedsværktøjer, -politikker og -procedurer.

2. De finansielle enheder udformer, indkøber og gennemfører IKT-sikkerhedspolitikker, -procedurer, -protokoller og -værktøjer, der har til formål at sikre IKT-systemernes modstandsdygtighed, stabilitet og tilgængelighed, især for dem, der understøtter kritiske eller vigtige funktioner, og at opretholde høje standarder for, tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, hvad enten dataene er inaktive, i brug eller under overførsel.

3. For at nå de i stk. 2 omhandlede mål anvender de finansielle enheder IKT-løsninger og -processer, som er hensigtsmæssige i overensstemmelse med artikel 4. Disse IKT-løsninger og -processer:

a) sikrer sikkerheden for metoderne til overførsel af data

b) minimerer risikoen for korruption eller tab af data, uautoriseret adgang og tekniske fejl, der kan hæmme erhvervsaktiviteten

c) forhindrer manglen på tilgængelighed, forringelsen af autenticiteten og integriteten, bruddene på fortroligheden og tabet af data

d) sikrer, at data beskyttes mod risici, der opstår i forbindelse med dataforvaltning, herunder dårlig administration, procesrelaterede risici og menneskelige fejl.

4. Som led i den ramme for IKT-risikostyring, der er omhandlet i artikel 6, stk. 1, skal de finansielle enheder

a) udvikle og dokumentere en informationssikkerhedspolitik, der fastlægger regler for beskyttelse af tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, informationsaktiver og IKT-aktiver, herunder deres kunders, hvis det er relevant

b) ved at følge en risikobaseret tilgang indføre en forsvarlig forvaltningsstruktur for netværk og infrastrukturer ved anvendelse af passende teknikker, metoder og protokoller, der kan omfatte gennemførelse af automatiske mekanismer til isolering af de berørte informationsaktiver i tilfælde af cyberangreb

c) gennemføre politikker, der begrænser den fysiske eller logiske adgang til informationsaktiver og IKT-aktiver udelukkende til, hvad der er påkrævet for legitime og godkendte funktioner og aktiviteter, og med henblik herpå indføre en række politikker, procedurer og kontroller, der vedrører adgangsrettigheder og sikrer forsvarlig forvaltning heraf

d) gennemføre politikker og protokoller for stærke autentificeringsmekanismer på grundlag af relevante standarder og særlige kontrolsystemer og beskyttelsesforanstaltninger for krypteringsnøgler, hvorigennem data krypteres baseret på resultaterne fra godkendt dataklassificering og godkendte IKT-risikovurderingsprocesser

e) gennemføre dokumenterede politikker, procedurer og kontroller for styring af IKT-ændringer, herunder ændringer af software, hardware, firmwarekomponenter, systemer eller sikkerhedsparametre, som er baseret på en risikovurderingstilgang og er en integreret del af den finansielle enheds samlede ændringsstyringsproces, for at sikre, at alle ændringer af IKT-systemer registreres, testes, vurderes, godkendes, gennemføres og efterprøves på en kontrolleret måde

f) sørge for, at der indføres passende og omfattende dokumenterede politikker for programrettelser og opdateringer.

Med henblik på første afsnit, litra b), udformer de finansielle enheder infrastrukturen for netværkstilslutning på en sådan måde, at den kan afbrydes eller segmenteres øjeblikkeligt for at minimere og forhindre afsmitning, navnlig i forbindelse med indbyrdes forbundne finansielle processer.

Med henblik på første afsnit, litra e), skal IKT-ændringsstyringsprocessen godkendes på passende ledelsesniveauer og omfatte specifikke protokoller.

Artikel 10

Detektion

1. De finansielle enheder indfører mekanismer til omgående detektion af anormale aktiviteter i overensstemmelse med artikel 17, herunder problemer med IKT-netværkets ydeevne og IKT-relaterede hændelser, og til identifikation af potentielt væsentlige single points of failure.

De i første afsnit omhandlede mekanismer testes regelmæssigt i overensstemmelse med artikel 25.

2. Ved de i stk. 1 omhandlede detektionsmekanismer skal det gøres muligt at anvende flere kontrollag, fastlægge varslingstærskler og -kriterier, som skal udløse og igangsætte indsatsforanstaltninger mod IKT-relaterede hændelser, herunder automatiske varslingsmekanismer for det relevante personale, som har ansvar for indsatsen mod IKT-relaterede hændelser.

3. Finansielle enheder afsætter tilstrækkelige ressourcer og kapaciteter til overvågning af brugeraktiviteter, forekomsten af IKT-anomalier og IKT-relaterede hændelser, navnlig cyberangreb.

4. Udbydere af dataindberetningstjenester indfører desuden systemer, som effektivt kan kontrollere, om handelsindberetningerne er fuldstændige, identificere udeladelser og åbenbare fejl og anmode om fornyet fremsendelse af disse indberetninger.

Artikel 11

Indsats og genopretning

1. Som led i den ramme for IKT-risikostyring, der er omhandlet i artikel 6, stk. 1, og baseret på de krav til identifikation, der er fastsat i artikel 8, indfører de finansielle enheder en omfattende politik for IKT-driftsstabilitet, som kan vedtages som en særlig specifik politik, der skal udgøre en integreret del af den finansielle enheds samlede politik for driftsstabilitet.

2. De finansielle enheder gennemfører politikken for IKT-driftsstabilitet ved hjælp af særlige, passende og veldokumenterede ordninger, planer, procedurer og mekanismer, der tager sigte mod:

a) at sikre, at den finansielle enheds kritiske eller vigtige funktioner er stabile

b) hurtigt, passende og effektivt at sætte ind over for og løse alle IKT-relaterede hændelser på en måde, der begrænser skaden og prioriterer genoptagelsen af aktiviteter og genopretningstiltag

c) omgående at aktivere særlige planer, der gør det muligt at anvende inddæmningsforanstaltninger, -processer og -teknologier, der er egnede til de enkelte typer IKT-relaterede hændelser, og som forhindrer yderligere skade, samt skræddersyede indsats- og genopretningsprocedurer, der er fastlagt i henhold til artikel 12

d) at anslå foreløbige virkninger, skader og tab

e) at indføre kommunikations- og krisestyringstiltag, der sikrer, at ajourførte oplysninger videresendes til al relevant internt personale og eksterne interessenter i overensstemmelse med artikel 14, og at de indberettes til de kompetente myndigheder i overensstemmelse med artikel 19.

3. Som led i den ramme for IKT-risikostyring, der er omhandlet i artikel 6, stk. 1, gennemfører de finansielle enheder dertil knyttede planer for IKT-indsats og -genopretning, som for finansielle enheder, der ikke er mikrovirksomheder, underkastes uafhængige interne revisionsgennemgange.

4. De finansielle enheder indfører, vedligeholder og foretager regelmæssig testning af passende planer for IKT-driftsstabilitet, navnlig med hensyn til kritiske eller vigtige funktioner, som outsources eller udliciteres gennem ordninger, der er indgået med tredjepartsudbydere af IKT-tjenester.

5. Som led i den samlede politik for driftsstabilitet foretager de finansielle enheder en forretningskonsekvensanalyse (BIA) af deres eksponering for alvorlige driftsforstyrrelser. De finansielle enheder vurderer i forbindelse med BIA'en de potentielle virkninger af alvorlige driftsforstyrrelser ved hjælp af kvantitative og kvalitative kriterier ved anvendelse af interne og eksterne data og scenarieanalyser, alt efter hvad der er relevant. BIA'en skal tage hensyn til den kritiske betydning af identificerede og kortlagte forretningsfunktioner, støtteprocesser, tredjepartsafhængighed og informationsaktiver samt deres indbyrdes afhængighed. De finansielle enheder sikrer, at IKT-aktiver og -tjenester udformes og anvendes i fuld overensstemmelse med BIA'en, navnlig med hensyn til tilstrækkeligt at sikre alle kritiske komponenters redundans.

6. Som led i den omfattende IKT-risikostyring skal de finansielle enheder

a) teste deres planer for IKT-driftsstabilitet og planer for IKT-indsats og -genopretning i forbindelse med IKT-systemer, der understøtter alle funktioner, mindst én gang om året og i tilfælde af væsentlige ændringer af IKT-systemer, der understøtter kritiske eller vigtige funktioner

b) teste de krisekommunikationsplaner, der er udarbejdet i henhold til artikel 14.

Med henblik på første afsnit, litra a), medtager finansielle enheder, som ikke er mikrovirksomheder, cyberangrebsscenarier og omstillingsscenarier mellem den primære IKT-infrastruktur og redundante kapacitet, sikkerhedskopier og de redundante faciliteter, der er nødvendige for at opfylde de i artikel 12 fastsatte forpligtelser, i testplanerne.

De finansielle enheder gennemgår regelmæssigt deres politik for IKT-driftsstabilitet og planer for IKT-indsats og -genopretning under hensyntagen til resultaterne af de test, der er gennemført i overensstemmelse med første afsnit, og henstillinger, der bygger på revisionskontrol eller tilsynsmæssige gennemgange.

7. Finansielle enheder, som ikke er mikrovirksomheder, skal have en krisestyringsfunktion, som, hvis deres planer for IKT-driftsstabilitet og planer for IKT-indsats og -genopretning aktiveres, bl.a. skal indeholde klare procedurer for forvaltning af intern og ekstern krisekommunikation i overensstemmelse med artikel 14.

8. De finansielle enheder fører let tilgængelige registre over aktiviteter før og under driftsforstyrrelser, når deres planer for IKT-driftsstabilitet og planer for IKT-indsats og -genopretning aktiveres.

9. Værdipapircentraler forelægger kopier af resultaterne af test af IKT-driftsstabiliteten eller lignende aktiviteter for de kompetente myndigheder.

10. Finansielle enheder, som ikke er mikrovirksomheder, indberetter et overslag over de samlede årlige omkostninger og tab, der opstår som følge af større IKT-relaterede hændelser, til de kompetente myndigheder på deres anmodning.

11. I overensstemmelse med artikel 16 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010, udarbejder ESA'erne via Det Fælles Udvalg senest den 17. juli 2024 fælles retningslinjer for overslaget over de samlede årlige omkostninger og tab, der er omhandlet i stk. 10.

Artikel 12

Politikker og procedurer for sikkerhedskopiering og procedurer og metoder for gendannelse og genopretning

1. Med henblik på at sikre gendannelse af IKT-systemer og data med minimal nedetid, begrænsede forstyrrelser og tab udvikler og dokumenterer de finansielle enheder som led i deres ramme for IKT-risikostyring følgende:

a) politikker og procedurer for sikkerhedskopiering, der præciserer omfanget af de data, der er genstand for sikkerhedskopiering, og minimumshyppigheden af sikkerhedskopiering baseret på oplysningernes kritiske betydning eller fortrolighedsniveauet for dataene

b) procedurer og metoder for gendannelse og genopretning.

2. De finansielle enheder etablerer systemer for sikkerhedskopiering, der kan aktiveres i overensstemmelse med politikker og procedurer for sikkerhedskopiering, og procedurer og metoder for gendannelse og genopretning. Aktiveringen af systemerne for sikkerhedskopiering må ikke sætte sikkerheden i net- og informationssystemer eller tilgængeligheden, autenticiteten, integriteten eller fortroligheden af data over styr. Der foretages regelmæssig test af procedurer for sikkerhedskopiering og procedurer og metoder for gendannelse og genopretning.

3. Når de finansielle enheder gendanner sikkerhedskopierede data ved anvendelse af egne systemer, anvender de IKT-systemer, der er fysisk og logisk adskilt fra IKT-kildesystemet. IKT-systemerne skal være sikkert beskyttet mod uautoriseret adgang eller IKT-korruption og give mulighed for rettidig gendannelse af tjenester ved hjælp af data- og systemsikkerhedskopier efter behov.

For centrale modparter skal genopretningsplaner gøre det muligt at genoptage alle transaktioner fra det tidspunkt, hvor de blev afbrudt, således at den berørte centrale modpart kan opretholde driftssikkerheden og gennemføre afviklingen på den planlagte dato.

Udbydere af dataindberetningstjenester skal desuden sørge for at råde over passende ressourcer og sikkerhedskopierings- og gendannelsesfaciliteter for til enhver tid at kunne udbyde og opretholde deres tjenester.

4. Finansielle enheder, der ikke er mikrovirksomheder, opretholder redundante IKT-kapaciteter, der er udstyret med passende ressourcer og funktioner med henblik på at sikre forretningsmæssige behov. Mikrovirksomheder vurderer behovet for at opretholde sådanne redundante IKT-kapaciteter på grundlag af deres risikoprofil.

5. Værdipapircentraler bibeholder mindst ét sekundært afviklingssted, der er udstyret med passende ressourcer, kapaciteter, funktioner og personalemæssige ordninger med henblik på at sikre forretningsmæssige behov.

Det sekundære afviklingssted skal

a) befinde sig i en geografisk afstand fra det primære afviklingssted for at sikre, at det har en særlig risikoprofil og for at forhindre, at det påvirkes af den hændelse, der har berørt det primære afviklingssted

b) kunne sikre driftsstabiliteten for kritiske eller vigtige funktioner på samme måde som det primære afviklingssted eller levere det serviceniveau, der er nødvendigt for, at den finansielle enhed kan udføre sine kritiske operationer inden for rammerne af genopretningsmålene

c) være umiddelbart tilgængeligt for den finansielle enheds personale for at sikre driftsstabilitet for kritiske eller vigtige funktioner i tilfælde af, at det primære afviklingssted ikke står til rådighed.

6. Når de finansielle enheder fastlægger målene for genopretningstid og genopretningspunkt for hver funktion, tager de hensyn til, om det er en kritisk eller vigtig funktion og de potentielle samlede virkninger for markedseffektiviteten. Sådanne tidsmål skal sikre, at de aftalte serviceniveauer overholdes i ekstreme scenarier.

7. Når de finansielle enheder foretager genopretning efter en IKT-relateret hændelse, udfører de nødvendige kontroller, herunder eventuelt flere kontroller og afstemninger, for at sikre, at dataintegriteten bevares på højeste niveau. Disse kontroller foretages også i forbindelse med rekonstruktionen af data fra eksterne interessenter for at sikre, at alle systemernes data er sammenhængende.

Artikel 13

Læring og udvikling

1. De finansielle enheder sørger for at råde over kapaciteter og personale, som kan indsamle oplysninger om sårbarheder og cybertrusler, IKT-relaterede hændelser, navnlig cyberangreb, og analysere de virkninger, de forventes at have på deres digitale operationelle modstandsdygtighed.

2. De finansielle enheder foretager gennemgange af IKT-relaterede hændelser, efter at en større IKT-relateret hændelse forstyrrer deres kerneaktiviteter, analyserer årsagerne til forstyrrelserne og identificerer nødvendige forbedringer af IKT-operationerne eller inden for rammerne af den i artikel 11 omhandlede politik for IKT-driftsstabilitet.

Finansielle enheder, som ikke er mikrovirksomheder, underretter på anmodning de kompetente myndigheder om ændringer, der er blevet gennemført efter gennemgange af IKT–relaterede hændelser som omhandlet i første afsnit.

I forbindelse med de i første afsnit omhandlede gennemgange af IKT-relaterede hændelser skal det fastslås, om de fastlagte procedurer er blevet fulgt, og om de iværksatte foranstaltninger har været effektive, herunder i forhold til følgende:

a) den hastighed, med hvilken der er blevet sat ind over for sikkerhedsvarsler, og med hvilken virkningerne af IKT-relaterede hændelser og deres omfang er blevet fastslået

b) kvaliteten og hastigheden af udførelsen af en kriminalteknisk analyse, hvor det skønnes hensigtsmæssigt

c) effektiviteten af den finansielle enheds fejlafhjælpning i forbindelse med hændelser

d) effektiviteten af den interne og eksterne kommunikation.

3. Erfaringer fra test af digital operationel modstandsdygtighed, som foretages i overensstemmelse med artikel 26 og 27, og fra faktiske IKT-relaterede hændelser, navnlig cyberangreb, samt udfordringer i forbindelse med aktiveringen af planer for IKT-driftsstabilitet og planer for IKT-indsats og -genopretning skal sammen med relevante oplysninger, der udveksles med modparter, og som vurderes i forbindelse med tilsynsmæssige gennemgange, løbende indarbejdes i IKT-risikovurderingsprocessen. Disse resultater danner grundlag for passende gennemgange af relevante komponenter i den ramme for IKT-risikostyring, der er omhandlet i artikel 6, stk. 1.

4. De finansielle enheder overvåger effektiviteten af gennemførelsen af deres strategi for digital operationel modstandsdygtighed, jf. artikel 6, stk. 8. De kortlægger IKT-risikoens udvikling over tid, analyserer hyppigheden, typerne, omfanget af og udviklingen i IKT-relaterede hændelser, navnlig cyberangreb og mønstre forbundet hermed, med henblik på at forstå graden af IKT-risikoeksponering, navnlig i forbindelse med kritiske eller vigtige funktioner, og forbedre den finansielle enheds cybermodenhed og cyberberedskab.

5. Højtstående IKT-personale skal mindst én gang om året aflægge rapport til ledelsesorganet om de i stk. 3 omhandlede resultater og fremsætte anbefalinger.

6. De finansielle enheder udvikler programmer til bevidstgørelse om IKT-sikkerhed og kurser i digital operationel modstandsdygtighed som obligatoriske moduler i deres personaleuddannelsesordninger. Disse programmer og kurser skal omfatte alle medarbejdere og den øverste ledelse og skal have en grad af kompleksitet, der svarer til deres opgavers ansvarsområde. Hvis det er relevant, inddrager finansielle enheder også tredjepartsudbydere af IKT-tjenester i deres relevante uddannelsesordninger i overensstemmelse med artikel 30, stk. 2, litra i).

7. Finansielle enheder, der ikke er mikrovirksomheder, overvåger løbende den relevante teknologiske udvikling også med henblik på at forstå den mulige virkning af indførelsen af sådanne nye teknologier for kravene til IKT-sikkerhed og digital operationel modstandsdygtighed. De skal holde sig ajour med de seneste IKT-risikostyringsprocesser for effektivt at bekæmpe aktuelle eller nye former for cyberangreb.

Artikel 14

Kommunikation

1. Som led i den ramme for IKT-risikostyring, der er omhandlet i artikel 6, stk. 1, sørger de finansielle enheder for at have krisekommunikationsplaner, der giver mulighed for ansvarlig offentliggørelse af som minimum større IKT-relaterede hændelser eller sårbarheder for kunder og modparter samt for offentligheden, alt efter hvad der er relevant.

2. Som led i rammen for IKT-risikostyring gennemfører de finansielle enheder kommunikationsplaner for internt personale og for eksterne interessenter. Kommunikationspolitikkerne for personalet skal tage hensyn til behovet for at skelne mellem personale, der er involveret i IKT-risikostyring, navnlig det personale, der er ansvarligt for indsats og genopretning, og personale, der skal underrettes.

3. Mindst én person i den finansielle enhed skal have til opgave at gennemføre kommunikationsstrategien for IKT-relaterede hændelser og til dette formål varetage funktionen vedrørende offentligheden og medierne.

Artikel 15

Yderligere harmonisering af IKT-risikostyringsværktøjer, -metoder, -processer og -politikker

ESA'erne udarbejder via Det Fælles Udvalg og i samråd med Den Europæiske Unions Agentur for Cybersikkerhed (ENISA) fælles udkast til reguleringsmæssige tekniske standarder med henblik på:

a) at præcisere, hvilke yderligere elementer der skal indgå i de IKT-sikkerhedspolitikker, -procedurer, -protokoller og -værktøjer, der er omhandlet i artikel 9, stk. 2, med henblik på at garantere netsikkerheden, sikre tilstrækkelige garantier mod indtrængen og datamisbrug, bevare tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, herunder kryptografiske teknikker, og garantere en nøjagtig og hurtig dataoverførsel uden større forstyrrelser og unødige forsinkelser

b) at videreudvikle komponenter i kontrollen med de rettigheder vedrørende adgangsforvaltning, der er omhandlet i artikel 9, stk. 4, litra c), og den dertil knyttede HR-politik med angivelse af adgangsrettigheder, procedurer for tildeling og tilbagekaldelse af rettigheder, overvågning af anormal adfærd i forbindelse med IKT-risikoen ved hjælp af passende indikatorer, herunder for mønstre vedrørende netværksbrug, tidspunkter, IT-aktivitet og ukendt udstyr

c) at videreudvikle de mekanismer, der er anført i artikel 10, stk. 1, for at muliggøre en hurtig detektion af anormale aktiviteter, og de kriterier, der er fastsat i artikel 10, stk. 2, for at udløse detektion af IKT-relaterede hændelser og indsatsforanstaltninger

d) yderligere at præcisere de komponenter, der er indeholdt i den politik for IKT-driftsstabilitet, der er omhandlet i artikel 11, stk. 1

e) yderligere at præcisere test af de planer for IKT-driftsstabilitet, der er omhandlet i artikel 11, stk. 6, for at sikre, at sådanne test tager behørigt hensyn til de scenarier, hvor kvaliteten af leveringen af en kritisk eller vigtig funktion forringes til et uacceptabelt niveau eller mislykkes, og at der tages behørigt hensyn til de potentielle virkninger af insolvens hos eller andre svigt forårsaget af eventuelle relevante tredjepartsudbydere af IKT-tjenester og, hvor det er relevant, de politiske risici i de respektive udbyderes jurisdiktioner

f) yderligere at præcisere de komponenter, der er indeholdt i de planer for IKT-indsats og -genopretning, der er omhandlet i artikel 11, stk. 3

g) yderligere at præcisere indholdet i og formatet af den rapport om gennemgangen af rammen for IKT-risikostyring, der er omhandlet i artikel 6, stk. 5.

Når ESA'erne udarbejder disse udkast til reguleringsmæssige tekniske standarder, tager de hensyn til den finansielle enheds størrelse og samlede risikoprofil og karakteren, omfanget og kompleksiteten af dens tjenester, aktiviteter og operationer og tager samtidig behørigt hensyn til eventuelle særlige kendetegn som følge af aktiviteternes særlige karakter på tværs af forskellige sektorer for finansielle tjenesteydelser.

ESA'erne forelægger disse udkast til reguleringsmæssige tekniske standarder for Kommissionen senest den 17 januar 2024 [12 måneder efter datoen for denne forordnings ikrafttræden].

Kommissionen tillægges beføjelse til supplere denne forordning ved at vedtage de i stk. 1 omhandlede reguleringsmæssige tekniske standarder i overensstemmelse med artikel 10-14 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.

Artikel 16

Forenklet ramme for IKT-risikostyring

1. Nærværende forordnings artikel 5-15 finder ikke anvendelse på små og ikke indbyrdes forbundne investeringsselskaber, betalingsinstitutter, der er undtaget i henhold til direktiv (EU) 2015/2366, institutter, der er fritaget i henhold til direktiv 2013/36/EU, og for hvilke medlemsstaterne har besluttet ikke at anvende den mulighed, der er omhandlet i nærværende forordnings artikel 2, stk. 4, e-pengeinstitutter, der er undtaget i henhold til direktiv 2009/110/EF, og små arbejdsmarkedsrelaterede pensionskasser.

Uden at det berører første afsnit skal de i første afsnit omhandlede enheder:

a) indføre og vedligeholde en robust og dokumenteret ramme for IKT-risikostyring, der beskriver de mekanismer og foranstaltninger, der skal muliggøre en hurtig, effektiv og omfattende styring af IKT-risiko, herunder vedrørende beskyttelse af relevante fysiske komponenter og infrastrukturer

b) løbende overvåge alle IKT-systemers sikkerhed og drift

c) minimere virkningen af IKT-risiko gennem anvendelse af robuste, modstandsdygtige og ajourførte IKT-systemer, -protokoller og -værktøjer, som er egnede til at understøtte udførelsen af deres aktiviteter og leveringen af tjenester og i tilstrækkelig grad beskytte tilgængeligheden, autenticiteten, integriteten og fortroligheden af data i net- og informationssystemerne

d) gøre det muligt hurtigt at konstatere og detektere IKT-risikokilder og -anomalier i net- og informationssystemerne og hurtigt at håndtere IKT-relaterede hændelser

e) konstatere stor afhængighed af tredjepartsudbydere af IKT-tjenester

f) sikre kontinuiteten af kritiske eller vigtige funktioner gennem planer for driftsstabiliteten og indsats- og genopretningsforanstaltninger, der som minimum omfatter sikkerhedskopierings- og gendannelsesforanstaltninger

g) regelmæssigt teste de planer og foranstaltninger, der er omhandlet i litra f), samt effektiviteten af de gennemførte kontroller i overensstemmelse med litra a) og c)

h) gennemføre, alt efter hvad der er relevant, de relevante operationelle konklusioner, der følger af de test, der er omhandlet i litra g), og af de efterfølgende analyser af hændelserne, i IKT-risikovurderingsprocessen og efter behov og IKT-risikoprofil udvikle programmer til bevidstgørelse om IKT-sikkerhed og kurser i digital operationel modstandsdygtighed for personale og ledelse.

2. Den i stk. 1, andet afsnit, litra a) omhandlede ramme for IKT-risikostyring skal dokumenteres og gennemgås regelmæssigt og ved forekomst af større IKT-relaterede hændelser i overensstemmelse med de tilsynsmæssige instrukser. Den skal forbedres løbende på grundlag af indhøstede erfaringer fra gennemførelse og overvågning. Der skal forelægges en rapport om gennemgangen af rammen for IKT-risikostyring for den kompetente myndighed på dennes anmodning.

3. ESA'erne udarbejder via Det Fælles Udvalg og i samråd med ENISA fælles udkast til reguleringsmæssige tekniske standarder med henblik på:

a) yderligere at præcisere de elementer, der skal indgå i rammen for IKT-risikostyring som omhandlet i stk. 1, andet afsnit, litra a)

b) yderligere at præcisere de elementer, der for så vidt angår systemer, protokoller og værktøjer mindsker virkningerne af den IKT-risiko, der er omhandlet i stk. 1, andet afsnit, litra c), med henblik på at garantere netsikkerheden, sikre tilstrækkelige garantier mod indtrængen og datamisbrug og bevare tilgængeligheden, autenticiteten, integriteten og fortroligheden af data

c) yderligere at præcisere de komponenter, der er indeholdt i de planer for IKT-driftsstabilitet, der er omhandlet i stk. 1, andet afsnit, litra f)

d) yderligere at præcisere reglerne om test af planer for driftsstabiliteten og sikre effektiviteten af de kontrolforanstaltninger, der er omhandlet i stk. 1, andet afsnit, litra g), og sikre, at der ved en sådan test tages behørigt hensyn til de scenarier, hvor kvaliteten af leveringen af en kritisk eller vigtig funktion forringes til et uacceptabelt niveau eller mislykkes

e) yderligere at præcisere indholdet og formatet af den rapport om gennemgangen af rammen for IKT-risikostyring, der er omhandlet i stk. 2.

Når ESA'erne udarbejder disse udkast til reguleringsmæssige tekniske standarder, tager de hensyn til den finansielle enheds størrelse og samlede risikoprofil og karakteren, omfanget og kompleksiteten af dens tjenester, aktiviteter og operationer.

ESA'erne forelægger disse udkast til reguleringsmæssige tekniske standarder for Kommissionen senest den 17. januar 2024.

Kommissionen tillægges beføjelse til at supplere denne forordning ved at vedtage de i første afsnit omhandlede reguleringsmæssige tekniske standarder i overensstemmelse med artikel 10-14 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.

KAPITEL III

Styring, klassificering og indberetning af IKT-relaterede hændelser

Artikel 17

Proces for styring af IKT-relaterede hændelser

1. De finansielle enheder definerer, fastlægger og gennemfører en proces for styring af IKT-relaterede hændelser for at detektere, styre og indberette IKT-relaterede hændelser.

2. De finansielle enheder registrerer alle IKT-relaterede hændelser og væsentlige cybertrusler. De finansielle enheder fastlægger passende procedurer og processer, der skal sikre en konsekvent og integreret overvågning, håndtering og opfølgning af IKT-relaterede hændelser, således at de grundlæggende årsager identificeres, dokumenteres og håndteres for at forhindre, at sådanne hændelser forekommer.

3. Som led i den proces for styring af IKT-relaterede hændelser, der er omhandlet i stk. 1:

a) indføres der tidlige advarselsindikatorer

b) fastlægges der procedurer til at identificere, spore, logge, kategorisere og klassificere IKT-relaterede hændelser alt efter deres prioritet og vigtighed og alt efter den kritiske betydning i overensstemmelse med de kriterier, der er fastlagt i artikel 18, stk. 1

c) tildeles der roller og ansvarsområder, som skal aktiveres for forskellige IKT-relaterede hændelsestyper og -scenarier

d) udarbejdes der planer for kommunikation til personale, eksterne interessenter og medier i overensstemmelse med artikel 14 og for underretning af kunder, interne fejlafhjælpningsprocedurer, herunder IKT-relaterede kundeklager, samt for indgivelse af oplysninger til finansielle enheder, der fungerer som modparter, alt efter hvad der er relevant

e) sikres det, at større IKT-relaterede hændelser som minimum indberettes til den relevante øverste ledelse, at ledelsesorganet som minimum underrettes om større IKT-relaterede hændelser, idet der redegøres for virkningerne, indsatsen og yderligere kontroller, som skal indføres som følge af sådanne IKT-relaterede hændelser

f) træffes der indsatsforanstaltninger mod IKT-relaterede hændelser, som skal afbøde virkningerne og sikre, at tjenesterne bliver operationelle og sikre på en rettidig måde.

Artikel 18

Klassificering af IKT-relaterede hændelser og cybertrusler

1. De finansielle enheder klassificerer IKT-relaterede hændelser og fastslår deres virkninger på grundlag af følgende kriterier:

a) antallet og/eller relevansen af kunder eller finansielle modparter, som er berørt, og, hvis det er relevant, beløbet på eller antallet af de transaktioner, som er berørt af den IKT-relaterede hændelse, og hvorvidt den IKT-relaterede hændelse har haft indvirkning på omdømmet

b) varigheden af den IKT-relaterede hændelse, herunder tjenestens nedetid

c) den geografiske udbredelse med hensyn til de områder, der er berørt af den IKT-relaterede hændelse, navnlig hvis den berører mere end to medlemsstater

d) de datatab, som den IKT-relaterede hændelse medfører med hensyn til tilgængelighed, autenticitet, integritet eller fortrolighed af data

e) den kritiske betydning af de berørte tjenester, herunder den finansielle enheds transaktioner og operationer

f) de økonomiske virkninger, navnlig direkte og indirekte omkostninger og tab, af den IKT-relaterede hændelse i både absolutte og relative tal.

2. De finansielle enheder klassificerer cybertrusler som væsentlige på grundlag af de udsatte tjenesters kritiske betydning, herunder den finansielle enheds transaktioner og operationer, antallet og/eller relevansen af de kunder eller finansielle modparter, som rammes, og risikoområdernes geografiske udbredelse.

3. ESA'erne udarbejder via Det Fælles Udvalg og i samråd med ECB og ENISA fælles udkast til reguleringsmæssige tekniske standarder, som yderligere præciserer følgende:

a) kriterierne i stk. 1, herunder væsentlighedstærskler til bestemmelse af større IKT-relaterede hændelser eller, alt efter hvad der er relevant, større operationelle eller sikkerhedsmæssige betalingsrelaterede hændelser, som er omfattet af indberetningspligten i artikel 19, stk. 1

b) de kriterier, som de kompetente myndigheder skal anvende med henblik på at vurdere relevansen af større IKT-relaterede hændelser eller, alt efter hvad der er relevant, af større operationelle eller sikkerhedsmæssige betalingsrelaterede hændelser, for de relevante myndigheder i andre medlemsstater, og de nærmere oplysninger i rapporterne om større IKT-relaterede hændelser eller, alt efter hvad der er relevant, større operationelle eller sikkerhedsmæssige betalingsrelaterede hændelser, som skal udveksles med andre kompetente myndigheder i henhold til artikel 19, stk. 6 og 7

c) kriterierne i denne artikels stk. 2, herunder høje væsentlighedstærskler til bestemmelse af væsentlige cybertrusler.

4. Når ESA'erne udarbejder de i denne artikels stk. 3 omhandlede fælles udkast til reguleringsmæssige tekniske standarder, tager de hensyn til kriterierne i artikel 4, stk. 2, samt de internationale standarder, den vejledning og de specifikationer, der er udarbejdet og offentliggjort af ENISA, herunder, hvor det er relevant, specifikationer for andre økonomiske sektorer. Med henblik på anvendelse af kriterierne i artikel 4, stk. 2, tager ESA'erne behørigt hensyn til behovet for, at mikrovirksomheder og små og mellemstore virksomheder mobiliserer tilstrækkelige ressourcer og kapaciteter til at sikre, at IKT-relaterede hændelser håndteres hurtigt.

ESA'erne forelægger disse fælles udkast til reguleringsmæssige tekniske standarder for Kommissionen senest den 17. januar 2024.

Kommissionen tillægges beføjelse til at supplere denne forordning ved at vedtage de i stk. 3 omhandlede reguleringsmæssige tekniske standarder i overensstemmelse med artikel 10-14 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.

Artikel 19

Indberetning af større IKT-relaterede hændelserog frivillig underretning om væsentlige cybertrusler

1. De finansielle enheder indberetter større IKT-relaterede hændelser til den relevante kompetente myndighed som omhandlet i artikel 46 i overensstemmelse med nærværende artikels stk. 4.

Hvis en finansiel enhed er underlagt tilsyn af mere end en national kompetent myndighed som omhandlet i artikel 46, udpeger medlemsstaterne en fælles kompetent myndighed som den relevante kompetente myndighed, der er ansvarlig for at udføre de i denne artikel omhandlede funktioner og opgaver.

Kreditinstitutter, der er klassificeret som signifikante i overensstemmelse med artikel 6, stk. 4, i forordning (EU) nr. 1024/2013, indberetter større IKT-relaterede hændelser til den relevante nationale kompetente myndighed, der er udpeget i overensstemmelse med artikel 4 i direktiv 2013/36/EU, og som øjeblikkeligt videresender den pågældende rapport til ECB.

Med henblik på første afsnit udarbejder de finansielle enheder efter indsamling og analyse af alle relevante oplysninger den indledende underretning og de rapporter, der er omhandlet i denne artikels stk. 4, ved brug af de modeller, der er omhandlet i artikel 20, og indgiver dem til den kompetente myndighed. Hvis det er teknisk umuligt at indgive den indledende underretning ved brug af modellen, meddeler de finansielle enheder den kompetente myndighed den på anden vis.

Den indledende underretning og de rapporter, der er omhandlet i stk. 4, skal indeholde alle de oplysninger, der er nødvendige for, at den kompetente myndighed kan fastslå, hvorvidt den større IKT-relaterede hændelse er væsentlig, og vurdere mulige grænseoverskridende virkninger.

Med forbehold af den finansielle enheds indberetning i henhold til første afsnit til den relevante kompetente myndighed kan medlemsstaterne derudover bestemme, at visse eller alle finansielle enheder også skal indgive den indledende underretning og hver enkelt rapport som omhandlet i denne artikels stk. 4 ved brug af de modeller, der er omhandlet i artikel 20, til de kompetente myndigheder eller til de enheder, der håndterer IT-sikkerhedshændelser (CSIRT'er), som er udpeget eller oprettet i overensstemmelse med direktiv (EU) 2022/2555.

2. De finansielle enheder kan på frivillig basis underrette den relevante kompetente myndighed om væsentlige cybertrusler, når de anser truslen for at være relevant for det finansielle system, tjenestebrugere eller kunder. Den relevante kompetente myndighed kan give sådanne oplysninger til andre relevante myndigheder som omhandlet i stk. 6.

Kreditinstitutter, der er klassificeret som signifikante i overensstemmelse med artikel 6, stk. 4, i forordning (EU) nr. 1024/2013, kan på frivillig basis underrette den relevante nationale kompetente myndighed, der er udpeget i overensstemmelse med artikel 4 i direktiv 2013/36/EU, og som øjeblikkeligt videresender underretningen til ECB, om væsentlige cybertrusler.

Medlemsstaterne kan bestemme, at disse finansielle enheder, som på frivillig basis indgiver en underretning, jf. først afsnit, også kan videresende den pågældende underretning til de CSIRT'er, der er udpeget eller oprettet i overensstemmelse med direktiv (EU) 2022/2555

3. Hvis en større IKT-relateret hændelse indtræffer og har indflydelse på kunders finansielle interesser, underretter de finansielle enheder uden unødigt ophold, så snart de får kendskab til den, deres kunder om den større IKT-relaterede hændelse og om de foranstaltninger, der er truffet for at afbøde de negative virkninger af en sådan hændelse.

I tilfælde af en væsentlig cybertrussel underretter de finansielle enheder, hvis det er relevant, de af deres kunder, som potentielt er berørt heraf, om eventuelle passende beskyttelsesforanstaltninger, som sidstnævnte kan overveje at træffe.

4. De finansielle enheder indgiver inden for de frister, der skal fastsættes i overensstemmelse med artikel 20, stk. 1, litra a), nr. ii), følgende til den relevante kompetente myndighed:

a) en indledende underretning

b) en foreløbig rapport efter den indledende underretning, jf. litra a), så snart den oprindelige hændelses status har ændret sig betydeligt, eller håndteringen af den større IKT-relaterede hændelse har ændret sig på grundlag af nye tilgængelige oplysninger, efterfulgt, alt efter hvad der er relevant, af ajourførte underretninger, hver gang der foreligger en relevant ajourføring af status, samt efter en specifik anmodning fra den kompetente myndighed

c) en endelig rapport, når den grundlæggende årsagsanalyse er afsluttet, uanset om der allerede er gennemført afbødende foranstaltninger, og når tallene for de faktiske virkninger foreligger og kan erstatte skøn.

5. De finansielle enheder kan i overensstemmelse med EU- og national sektorspecifik ret outsource opfyldelsen af indberetningsforpligtelserne i henhold til denne artikel til en tredjepartstjenesteudbyder. I tilfælde af en sådan outsourcing er den finansielle enhed fortsat fuldt ud ansvarlig for at opfylde kravene vedrørende indberetning af hændelser.

6. Når den kompetente myndighed modtager den indledende underretning og hver enkelt rapport som omhandlet i stk. 4, forelægger den rettidigt nærmere oplysninger om den større IKT-relaterede hændelse for følgende modtagere på grundlag af deres respektive kompetencer, alt efter hvad der er relevant:

a) EBA, ESMA eller EIOPA

b) ECB i tilfælde af finansielle enheder som omhandlet i artikel 2, stk. 1, litra a), b) og d)

c) de kompetente myndigheder, de centrale kontaktpunkter eller CSIRT'er, der er udpeget eller oprettet i overensstemmelse med direktiv (EU) 2022/2555

d) afviklingsmyndighederne som omhandlet i artikel 3 i direktiv 2014/59/EU og Den Fælles Afviklingsinstans (SRB) for så vidt angår de enheder, der er omhandlet i artikel 7, stk. 2, i Europa-Parlamentets og Rådets forordning (EU) nr. 806/2014 ([37]), og for så vidt angår de enheder og koncerner, der er omhandlet i artikel 7, stk. 4, litra b), og artikel 7, stk. 5, i forordning (EU) nr. 806/2014, hvis sådanne oplysninger vedrører hændelser, der udgør en risiko for sikringen af kritiske funktioner, jf. artikel 2, stk. 1, nr. 35), i direktiv 2014/59/EU, og

e) andre relevante offentlige myndigheder i henhold til national ret.

7. Efter modtagelse af oplysningerne i overensstemmelse med stk. 6 vurderer EBA, ESMA eller EIOPA og ECB i samråd med ENISA og i samarbejde med den relevante kompetente myndighed, om den større IKT-relaterede hændelse er relevant for kompetente myndigheder i andre medlemsstater. Efter denne vurdering underretter EBA, ESMA eller EIOPA så hurtigt som muligt de relevante kompetente myndigheder i andre medlemsstater herom. ECB underretter medlemmerne af Det Europæiske System af Centralbanker om spørgsmål, der er relevante for betalingssystemet. De kompetente myndigheder træffer på grundlag af underretningen, hvis det er hensigtsmæssigt, alle nødvendige foranstaltninger for at beskytte det finansielle systems umiddelbare stabilitet.

([37]) Europa-Parlamentets og Rådets forordning (EU) nr. 806/2014 af 15. juli 2014 om ensartede regler og en ensartet procedure for afvikling af kreditinstitutter og visse investeringsselskaber inden for rammerne af en fælles afviklingsmekanisme og en fælles afviklingsfond og om ændring af forordning (EU) nr. 1093/2010 (EUT L 225 af 30.7.2014, s. 1).

8. Den underretning, som ESMA skal indgive i henhold til denne artikels stk. 7, berører ikke den kompetente myndigheds ansvar for hurtigt at videresende nærmere oplysninger om den større IKT-relaterede hændelse til den relevante myndighed i værtslandet, hvis en værdipapircentral har betydelige grænseoverskridende aktiviteter i værtslandet, den større IKT-relaterede hændelse forventes at have alvorlige konsekvenser for de finansielle markeder i værtslandet, og hvis der er samarbejdsordninger mellem de kompetente myndigheder med hensyn til tilsyn med finansielle enheder.

Artikel 20

Harmonisering af indholdet af og modeller for indberetninger

ESA'erne udarbejder via Det Fælles Udvalg og i samråd med ENISA og ECB følgende:

a) fælles udkast til reguleringsmæssige tekniske standarder med henblik på:

   i) at fastlægge indholdet af indberetningerne om større IKT-relaterede hændelser for at afspejle de kriterier, der er fastsat i artikel 18, stk. 1, og indarbejde yderligere elementer såsom nærmere oplysninger til fastlæggelse af relevansen af indberetningerne for andre medlemsstater og om, hvorvidt hændelsen udgør en større operationel eller sikkerhedsmæssig betalingsrelateret hændelse

   ii) at fastsætte fristerne for den indledende underretning og for hver enkelt rapport som omhandlet i artikel 19, stk. 4

   iii) at fastlægge indholdet af underretningen om væsentlige cybertrusler.

   Når ESA'erne udarbejder disse udkast til reguleringsmæssige tekniske standarder, tager de hensyn til den finansielle enheds størrelse og samlede risikoprofil og karakteren, omfanget og kompleksiteten af dens tjenester, aktiviteter og operationer, navnlig med henblik på at sikre, at forskellige frister, jf. dette stykkes litra a), nr. ii), alt efter hvad der er relevant, kan afspejle særlige forhold i de finansielle sektorer, uden at det berører opretholdelsen af en konsekvent tilgang til indberetning af IKT-relaterede hændelser i henhold til denne forordning og til direktiv (EU) 2022/2555 ESA'erne skal, alt efter hvad der er relevant, begrunde, hvis de afviger fra de tilgange, der er anlagt i forbindelse med nævnte direktiv

b) fælles udkast til gennemførelsesmæssige tekniske standarder for at fastlægge standardformularer, -modeller og -procedurer, som de finansielle enheder skal bruge til indberetning af en større IKT-relateret hændelse og til underretning om en væsentlig cybertrussel.

ESA'erne forelægger det fælles udkast til reguleringsmæssige tekniske standarder, der er omhandlet i stk. 1, litra a), og det fælles udkast til gennemførelsesmæssige tekniske standarder, der er omhandlet stk. 1, litra b), for Kommissionen senest den 17. juli 2024.

Kommissionen tillægges beføjelse til at supplere denne forordning ved at vedtage de fælles reguleringsmæssige tekniske standarder, der er omhandlet i stk. 1, litra a), i overensstemmelse med artikel 10-14 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.

Kommissionen tillægges beføjelse til at vedtage de fælles gennemførelsesmæssige tekniske standarder, der er omhandlet i stk. 1, litra b), i overensstemmelse med artikel 15 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.

Artikel 21

Centralisering af indberetninger af større IKT-relaterede hændelser

1. ESA'erne udarbejder via Det Fælles Udvalg og i samråd med ECB og ENISA en fælles rapport med en vurdering af den praktiske mulighed for yderligere centralisering af indberetningen af hændelser gennem oprettelse af et fælles EU-knudepunkt for finansielle enheders indberetning af større IKT-relaterede hændelser. I den fælles rapport skal det undersøges, hvordan man kan fremme strømmen af indberetninger af IKT-relaterede hændelser, reducere de dermed forbundne omkostninger og understøtte tematiske analyser med henblik på at øge den tilsynsmæssige konvergens.

2. Den i stk. 1 omhandlede fælles rapport skal mindst omfatte følgende elementer:

a) forudsætninger for oprettelsen af et fælles EU-knudepunkt

b) fordele, begrænsninger og risici, herunder risici forbundet med den høje koncentration af følsomme oplysninger

c) den nødvendige kapacitet til at sikre interoperabilitet med andre relevante indberetningsordninger

d) elementer af den operationelle styring

e) betingelser for medlemskab

f) tekniske vilkår for finansielle enheders og nationale kompetente myndigheders adgang til det fælles EU-knudepunkt

g) en foreløbig vurdering af de finansielle omkostninger, der er forbundet med oprettelse af en operationel platform, der understøtter det fælles EU-knudepunkt, herunder den nødvendige ekspertise.

3. ESA'erne forelægger den i stk. 1 omhandlede rapport for Europa-Parlamentet, Rådet og Kommissionen senest den 17. januar 2025.

Artikel 22

Tilsynsmæssig feedback

1. Med forbehold af teknisk input, rådgivning eller afhjælpende foranstaltninger og efterfølgende opfølgning herpå, som CSIRT'erne, hvis det er relevant, i overensstemmelse med national ret kan tilvejebringe i henhold til direktiv (EU) 2022/2555, kvitterer den kompetente myndighed, når den modtager den indledende underretning og hver enkelt rapport, jf. artikel 19, stk. 4, for modtagelse heraf og kan, hvis det er praktisk muligt, rettidigt give den finansielle enhed relevant og forholdsmæssig feedback eller vejledning på højt niveau, navnlig ved at stille alle relevante anonymiserede oplysninger og efterretninger om lignende trusler til rådighed, og kan drøfte, hvilke afhjælpende foranstaltninger der har fundet anvendelse over for den finansielle enhed, og måder, hvorpå negative virkninger kan minimeres og afbødes på tværs af den finansielle sektor. Med forbehold af den modtagne tilsynsmæssige feedback er de finansielle enheder fortsat fuldt ud ansvarlige for håndteringen og konsekvenserne af de IKT-relaterede hændelser, der er indberettet i henhold til artikel 19, stk. 1.

2. ESA'erne aflægger via Det Fælles Udvalg baseret på et anonymiseret og samlet grundlag årligt rapport om større IKT-relaterede hændelser, hvis nærmere indhold stilles til rådighed af de kompetente myndigheder i overensstemmelse med artikel 19, stk. 6, og der som minimum angiver antallet af større IKT-relaterede hændelser, deres karakter og indvirkning på finansielle enheders eller kunders operationer samt de afhjælpende foranstaltninger, der er truffet, og de omkostninger, der er afholdt.

ESA'erne udsteder advarsler og udarbejder statistikker på højt niveau for at understøtte IKT-trussels- og sårbarhedsvurderinger.

Artikel 23

Operationelle eller sikkerhedsmæssige betalingsrelaterede hændelser vedrørende kreditinstitutter, betalingsinstitutter, kontooplysningstjenesteudbydere og e-pengeinstitutter

De krav, der er fastlagt i dette kapitel, finder også anvendelse på operationelle eller sikkerhedsmæssige betalingsrelaterede hændelser og større operationelle eller sikkerhedsmæssige betalingsrelaterede hændelser, hvis de vedrører kreditinstitutter, betalingsinstitutter, kontooplysningstjenesteudbydere og e-pengeinstitutter.

KAPITEL IV

Test af digital operationel modstandsdygtighed

Artikel 24

Generelle krav til gennemførelsen af test af digital operationel modstandsdygtighed

1. Med henblik på at vurdere beredskabet i forhold til håndtering af IKT-relaterede hændelser, identificere svagheder, mangler og huller i den digitale operationelle modstandsdygtighed og straks træffe korrigerende foranstaltninger udarbejder, opretholder og gennemgår de finansielle enheder, der ikke er mikrovirksomheder, under hensyntagen til kriterierne i artikel 4, stk. 2, et forsvarligt og omfattende program for test af digital operationel modstandsdygtighed som en integrerende del af den i artikel 6 omhandlede ramme for IKT-risikostyring.

2. Programmet for test af digital operationel modstandsdygtighed skal omfatte en række vurderinger, test, metodologier, fremgangsmåder og værktøjer, der skal anvendes i overensstemmelse med artikel 25 og 26.

3. Når de finansielle enheder, der ikke er mikrovirksomheder, gennemfører det i denne artikels stk. 1 omhandlede program for test af digital operationel modstandsdygtighed, følger de en risikobaseret tilgang, idet de tager hensyn til kriterierne i artikel 4, stk. 2, under behørig hensyntagen til et IKT-risikomiljø i udvikling, eventuelle specifikke risici, som den berørte finansielle enhed udsættes for eller kan blive udsat for, informationsaktivernes og de leverede tjenesters kritiske betydning samt alle andre faktorer, som den finansielle enhed finder relevante.

4. De finansielle enheder, der ikke er mikrovirksomheder, sikrer, at test gennemføres af uafhængige parter, hvad enten de er interne eller eksterne. Hvis en intern tester gennemfører test, skal de finansielle enheder afsætte tilstrækkelige ressourcer og sikre, at interessekonflikter undgås under testens udformnings- og gennemførelsesfaser.

5. De finansielle enheder, der ikke er mikrovirksomheder, fastlægger procedurer og politikker med henblik på at prioritere, klassificere og afhjælpe alle problemer, der identificeres i forbindelse med gennemførelsen af test, og fastlægger interne valideringsmetoder for at sikre, at alle konstaterede svagheder, mangler eller huller afhjælpes fuldt ud.

6. De finansielle enheder, der ikke er mikrovirksomheder, sikrer, at der gennemføres passende test af alle IKT-systemer og -applikationer, der understøtter kritiske eller vigtige funktioner, mindst én gang om året.

Artikel 25

Test af IKT-værktøjer og -systemer

1. Det i artikel 24 omhandlede program for test af den digitale operationelle modstandsdygtighed skal i overensstemmelse med kriterierne i artikel 4, stk. 2, indeholde bestemmelser om gennemførelse af relevante test såsom sårbarhedsvurderinger og -scanninger, open source-analyser, vurderinger af netsikkerheden, mangelanalyser, fysiske sikkerhedsgennemgange, spørgeskemaer og scanningssoftwareløsninger, gennemgange af kildekoder, når det er praktisk muligt, scenariebaserede test, kompatibilitetstest, præstationstest, end-to-end-test og penetrationstest.

2. Værdipapircentraler og centrale modparter foretager sårbarhedsvurderinger inden indførelse eller genindførelse af nye eller eksisterende applikationer og infrastrukturkomponenter og IKT-tjenester, der understøtter den finansielle enheds kritiske eller vigtige funktioner.

3. Mikrovirksomheder gennemfører de i stk. 1 omhandlede test ved at kombinere en risikobaseret tilgang med strategisk planlægning af IKT-test under behørig hensyntagen til behovet for at opretholde en afbalanceret tilgang mellem omfanget af ressourcer og den tid, der skal afsættes til IKT-test som omhandlet i denne artikel, på den ene side og den hastende karakter, risikotype og informationsaktivernes og de leverede tjenesters kritiske betydning samt alle andre relevante faktorer, herunder den finansielle enheds evne til at tage kalkulerede risici, på den anden side.

Artikel 26

Avancerede test af IKT-værktøjer, -systemer og -processer baseret på TLPT

1. Finansielle enheder, der hverken er enheder som omhandlet i artikel 16, stk. 1, første afsnit, eller mikrovirksomheder, og som er identificeret i overensstemmelse med nærværende artikels stk. 8, tredje afsnit, foretager mindst hvert tredje år avancerede test ved hjælp af TLPT. På grundlag af den finansielle enheds risikoprofil og under hensyntagen til de operationelle omstændigheder kan den kompetente myndighed om nødvendigt anmode den finansielle enhed om at reducere eller øge denne hyppighed.

2. Hver trusselsbaseret penetrationstest skal omfatte flere eller samtlige kritiske eller vigtige funktioner hos en finansiel enhed og foretages på live-produktionssystemer, der understøtter sådanne funktioner.

De finansielle enheder identificerer alle relevante underliggende IKT-systemer, -processer og -teknologier, der understøtter kritiske eller vigtige funktioner og alle relevante IKT-tjenester, herunder dem, der understøtter kritiske eller vigtige funktioner og tjenester, der er blevet outsourcet eller udliciteret til tredjepartsudbydere af IKT-tjenester.

De finansielle enheder vurderer, hvilke kritiske eller vigtige funktioner, der skal være omfattet af TLPT. Resultatet af denne vurdering bestemmer det nøjagtige omfang af TLPT og valideres af de kompetente myndigheder.

3. Hvis tredjepartsudbydere af IKT-tjenester medtages i TLPT's anvendelsesområde, træffer den finansielle enhed de nødvendige foranstaltninger og sikkerhedsforanstaltninger for at sikre deltagelse af sådanne tredjepartsudbydere af IKT-tjenester i TLPT, og den har til enhver tid det fulde ansvar for at sikre overholdelse af denne forordning.

4. Uden at det berører stk. 2, første og andet afsnit, kan den finansielle enhed og tredjepartsudbyderen af IKT-tjenester, hvis deltagelse af en tredjepartsudbyder af IKT-tjenester i TLPT som omhandlet i stk. 3 med rimelighed kan forventes at have en negativ indvirkning på kvaliteten eller sikkerheden af de tjenester, som tredjepartsudbyderen af IKT-tjenester leverer til kunder, der er enheder, som ikke henhører under denne forordnings anvendelsesområde, eller på fortroligheden af data forbundet med sådanne tjenester, skriftligt aftale, at tredjepartsudbyderen af IKT-tjenester direkte indgår kontraktlige ordninger med en ekstern tester med henblik på under ledelse af en udpeget finansiel enhed at foretage en samlet TLPT, der omfatter flere finansielle enheder (samlet test), som tredjepartsudbyderen af IKT-tjenester leverer IKT-tjenester til.

Denne samlede test skal omfatte en relevant vifte af IKT-tjenester, der understøtter kritiske eller vigtige funktioner, som de finansielle enheder har udliciteret til den pågældende tredjepartsudbyder af IKT-tjenester. Den samlede test betragtes som en TLPT, som gennemføres af de finansielle enheder, der deltager i den samlede test.

Antallet af finansielle enheder, der deltager i den samlede test, afpasses behørigt under hensyntagen til kompleksiteten og typen af de involverede tjenester.

5. De finansielle enheder anvender i samarbejde med tredjepartsudbydere af IKT-tjenester og andre involverede parter, herunder testere, men med undtagelse af de kompetente myndigheder, effektive risikostyringskontroller for at mindske risici for potentielle virkninger på data, skade på aktiver og forstyrrelser af kritiske eller vigtige funktioner, tjenester eller operationer i den finansielle enhed selv, hos dens modparter eller i den finansielle sektor.

6. Efter afslutning af testen, og efter at der er opnået enighed om rapporter og udbedringsplaner, forelægger den finansielle enhed og, hvor det er relevant, de eksterne testere den myndighed, der er udpeget i overensstemmelse med stk. 9 eller 10, en sammenfatning af de relevante resultater, udbedringsplanerne og den dokumentation, som viser, at TLPT er blevet gennemført i overensstemmelse med kravene.

7. Myndighederne forelægger de finansielle enheder en erklæring, der bekræfter, at testen er blevet gennemført i overensstemmelse med de krav, der fremgår af dokumentationen, for at give mulighed for gensidig anerkendelse af trusselsbaserede penetrationstest mellem de kompetente myndigheder. Den finansielle enhed underretter den relevante kompetente myndighed om erklæringen, sammenfatningen af de relevante resultater og udbedringsplanerne.

Med forbehold af denne erklæring har de finansielle enheder til enhver tid fortsat det fulde ansvar for virkningen af de i stk. 4 omhandlede test.

8. De finansielle enheder indgår en kontrakt med testere med henblik på at gennemføre TLPT i overensstemmelse med artikel 27. Hvis de finansielle enheder anvender interne testere med henblik på at gennemføre TLPT, skal de indgå kontrakt med eksterne testere ved hver tredje test.

Kreditinstitutter, som er klassificeret som signifikante i overensstemmelse med artikel 6, stk. 4, i forordning (EU) nr. 1024/2013, må kun anvende eksterne testere i overensstemmelse med artikel 27, stk. 1, litra a)-e).

De kompetente myndigheder identificerer finansielle enheder, som pålægges at gennemføre TLPT under hensyntagen til kriterierne i artikel 4, stk. 2, på grundlag af en vurdering af følgende:

a) virkningsrelaterede faktorer, navnlig i hvilket omfang de tjenester, der leveres, og de aktiviteter, der udføres af den finansielle enhed, indvirker på den finansielle sektor

b) eventuelle betænkeligheder vedrørende finansiel stabilitet, herunder den finansielle enheds systemiske karakter på EU-plan eller nationalt plan, alt efter hvad der er relevant

c) den finansielle enheds specifikke IKT-risikoprofil, grad af IKT-modenhed eller de teknologiske kendetegn, der er involveret.

9. Medlemsstaterne kan udpege en fælles offentlig myndighed i den finansielle sektor til at være ansvarlig for TLPT-relaterede spørgsmål i den finansielle sektor på nationalt plan og overdrager den alle kompetencer og opgaver med henblik herpå.

10. I tilfælde af manglende udpegelse, jf. denne artikels stk. 9, og med forbehold af beføjelserne til at identificere de finansielle enheder, der skal gennemføre TLTP, kan en kompetent myndighed delegere udførelsen af visse eller alle de opgaver, der er omhandlet i denne artikel og artikel 27, til en anden national myndighed i den finansielle sektor.

11. ESA'erne udarbejder efter aftale med ECB fælles udkast til reguleringsmæssige tekniske standarder i overensstemmelse med TIBER-EU-rammen med henblik på yderligere at præcisere følgende:

a) de kriterier, der anvendes med henblik på anvendelsen af stk. 8, andet afsnit

b) krav til og standarder for anvendelsen af interne testere

c) kravene vedrørende:

   i) omfanget af de i stk. 2 omhandlede TLPT

   ii) den testmetode og -tilgang, der skal følges for hver specifik fase af testprocessen

   iii) resultaterne af testen, testens afslutnings- og udbedringsfaser

d) den type tilsynsmæssigt og andet relevant samarbejde, der er nødvendigt for at gennemføre TLPT, og for at lette den gensidige anerkendelse af den pågældende test, i forbindelse med finansielle enheder, der opererer i mere end én medlemsstat, således at der sikres et passende niveau af tilsynsmæssig deltagelse og en fleksibel gennemførelse for at tage højde for særlige forhold i finansielle delsektorer eller lokale finansielle markeder.

Når ESA'erne udarbejder disse udkast til reguleringsmæssige tekniske standarder, tager de behørigt hensyn til eventuelle særlige kendetegn, der opstår som følge af aktiviteternes særlige karakter på tværs af forskellige sektorer for finansielle tjenesteydelser.

ESA'erne forelægger disse udkast til reguleringsmæssige tekniske standarder for Kommissionen senest den 17. juli 2024.

Kommissionen tillægges beføjelse til at supplere denne forordning ved at vedtage de i første afsnit omhandlede reguleringsmæssige tekniske standarder i overensstemmelse med artikel 10-14 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.

Artikel 27

Krav til testere vedrørende gennemførelsen af TLPT

1. De finansielle enheder må kun anvende testere til gennemførelsen af TLPT, som:

a) er de mest egnede, og som har det bedste omdømme

b) er i besiddelse af tekniske og organisatoriske kapaciteter og har specifik ekspertise med hensyn til trusselsefterretning, penetrationstest og red team-test

c) er certificerede af et akkrediteringsorgan i en medlemsstat eller har overholdt formelle adfærdskodekser eller etiske rammer

d) afgiver en uafhængig garanti for eller en revisionsrapport vedrørende forsvarlig risikostyring i forbindelse med gennemførelsen af TLPT, herunder behørig beskyttelse af den finansielle enheds fortrolige oplysninger og afhjælpning af den finansielle enheds forretningsrisici

e) er behørigt og fuldt ud dækket af relevante erhvervsansvarsforsikringer, herunder mod risici for forseelser og forsømmelighed.

2. Når de anvender interne testere, skal de finansielle enheder i tillæg til kravene i stk. 1 sikre, at følgende betingelser er opfyldt:

a) en sådan anvendelse er blevet godkendt af den relevante kompetente myndighed eller den fælles offentlige myndighed, som er udpeget i overensstemmelse med artikel 26, stk. 9 og 10

b) den relevante kompetente myndighed har efterprøvet, at den finansielle enhed har afsat tilstrækkelige særlige ressourcer, og sikret, at interessekonflikter undgås under testens udformnings- og gennemførelsesfaser, og

c) formidleren af trusselsefterretninger er ekstern i forhold til den finansielle enhed.

3. De finansielle enheder sikrer, at der i de kontrakter, der indgås med eksterne testere, kræves en forsvarlig forvaltning af resultaterne af TLPT, og at enhver databehandling heraf, herunder enhver form for generering, lagring, aggregering, udkast, rapportering, kommunikation eller destruktion, ikke medfører risici for den finansielle enhed.

KAPITEL V

Styring af IKT-tredjepartsrisici

Afdeling I

Centrale principper for forsvarlig styring af IKT-tredjepartsrisici

Artikel 28

Generelle principper

1. De finansielle enheder styrer IKT-tredjepartsrisiko som en integreret del af IKT-risiko inden for deres ramme for IKT-risikostyring som omhandlet i artikel 6, stk. 1, og i overensstemmelse med følgende principper:

a) Finansielle enheder, der har indgået kontraktlige ordninger for brugen af IKT-tjenester til drift af deres forretningsaktiviteter, har til enhver tid det fulde ansvar for at overholde og opfylde alle forpligtelser i henhold til denne forordning og gældende finansiel tjenesteydelsesret

b) De finansielle enheders styring af IKT-tredjepartsrisiko skal gennemføres under hensyntagen til proportionalitetsprincippet, idet følgende tages i betragtning:

i) karakteren, omfanget, kompleksiteten og betydningen af den IKT-relaterede afhængighed

ii) de risici, der opstår som følge af kontraktlige ordninger for brugen af IKT-tjenester, der er indgået med tredjepartsudbydere af IKT-tjenester, under hensyntagen til den kritiske betydning eller vigtighed af den pågældende tjeneste, proces eller funktion og til de potentielle virkninger for driftsstabiliteten og tilgængeligheden af finansielle tjenesteydelser og aktiviteter på individuelt plan og koncernniveau.

2. Finansielle enheder, der hverken er enheder som omhandlet i artikel 16, stk. 1, første afsnit, eller er mikrovirksomheder, vedtager og gennemgår regelmæssigt en strategi for IKT-tredjepartsrisiko som led i deres ramme for IKT-risikostyring, idet de tager hensyn til den strategi med flere udbydere, der er omhandlet i artikel 6, stk. 9, hvor det er relevant. Strategien for IKT-tredjepartsrisiko skal omfatte en politik for brugen af IKT-tjenester, der understøtter kritiske eller vigtige funktioner, og som leveres af tredjepartsudbydere af IKT-tjenester, og skal gælde på individuelt grundlag og, hvor det er relevant, på delkonsolideret og konsolideret grundlag. Ledelsesorganet gennemgår på grundlag af en vurdering af den finansielle enheds samlede risikoprofil og omfanget og kompleksiteten af forretningstjenesterne regelmæssigt de risici, der er konstateret i forbindelse med kontraktlige ordninger for brugen af IKT-tjenester, der understøtter kritiske eller vigtige funktioner.

3. Som led i deres ramme for IKT-risikostyring opretholder og ajourfører de finansielle enheder på enhedsniveau, og på delkonsolideret og konsolideret niveau, et register over oplysninger om alle kontraktlige ordninger for brugen af IKT-tjenester, der leveres af tredjepartsudbydere af IKT-tjenester.

De i første afsnit omhandlede kontraktlige ordninger skal være behørigt dokumenteret, idet der skelnes mellem dem, der dækker IKT-tjenester, der understøtter kritiske eller vigtige funktioner, og dem, der ikke gør.

De finansielle enheder indberetter mindst én gang om året antallet af nye ordninger for brugen af IKT-tjenester, kategorierne af tredjepartsudbydere af IKT-tjenester, typen af kontraktlige ordninger og de IKT-tjenester og funktioner, der leveres, til de kompetente myndigheder.

De finansielle enheder stiller efter anmodning det fulde register over oplysninger eller, som anmodet, nærmere angivne afsnit heraf til rådighed for den kompetente myndighed sammen med eventuelle oplysninger, som anses for nødvendige for at muliggøre et effektivt tilsyn med den finansielle enhed.

De finansielle enheder underretter rettidigt den kompetente myndighed om enhver planlagt kontraktlig ordning for brugen af IKT-tjenester, der understøtter kritiske eller vigtige funktioner, og når en funktion er blevet kritisk eller vigtig.

4. Inden de finansielle enheder indgår en kontraktlig ordning for brugen af IKT-tjenester, skal de:

a) vurdere, om den kontraktlige ordning omfatter brugen af IKT-tjenester, der understøtter en kritisk eller vigtig funktion

b) vurdere, om de tilsynsmæssige betingelser for udlicitering er opfyldt

c) identificere og vurdere alle relevante risici i forbindelse med den kontraktlige ordning, herunder muligheden for, at sådanne kontraktlige ordninger kan bidrage til at øge IKT-koncentrationsrisikoen, jf. artikel 29

d) foretage fornøden due diligence over for potentielle tredjepartsudbydere af IKT-tjenester og under alle udvælgelses- og vurderingsprocesserne sikre, at den pågældende tredjepartsudbyder af IKT-tjenester er egnet

e) identificere og vurdere interessekonflikter, som de kontraktlige ordninger kan give anledning til.

5. De finansielle enheder må kun indgå kontraktlige ordninger med tredjepartsudbydere af IKT-tjenester, der overholder passende standarder for informationssikkerhed. Når disse kontraktlige ordninger vedrører kritiske eller vigtige funktioner, tager de finansielle enheder, inden de indgår ordningerne, behørigt hensyn til tredjepartsudbydere af IKT-tjenesters brug af de seneste informationssikkerhedsstandarder af højeste kvalitet.

6. Når finansielle enheder udøver adgangs-, inspektions- og revisionsrettigheder over for tredjepartsudbyderen af IKT-tjenester, foretager de på grundlag af en risikobaseret tilgang en forudgående fastsættelse af hyppigheden af revisioner og inspektioner samt af de områder, der skal underkastes revision, idet de overholder almindeligt accepterede revisionsstandarder i overensstemmelse med eventuelle tilsynsmæssige instrukser vedrørende anvendelse og indarbejdelse af sådanne revisionsstandarder.

Hvis de kontraktlige ordninger, der indgås med tredjepartsudbydere af IKT-tjenester for brugen af IKT-tjenester, indebærer en høj grad af teknisk kompleksitet, efterprøver den finansielle enhed, om revisorerne, hvad enten de er interne, eksterne eller en pulje af revisorer, besidder de nødvendige færdigheder og den nødvendige viden til effektivt at udføre de relevante revisioner og vurderinger.

7. De finansielle enheder sikrer, at de kontraktlige ordninger for brugen af IKT-tjenester som minimum kan opsiges i enhver af følgende situationer:

a) væsentlig overtrædelse begået af tredjepartsudbyderen af IKT-tjenester af gældende love, administrative bestemmelser eller kontraktvilkår

b) forhold, der er identificeret under overvågningen af IKT-tredjepartsrisiko, og som anses for at kunne ændre udførelsen af de funktioner, der er leveret gennem den kontraktlige ordning, herunder væsentlige ændringer, der påvirker ordningen eller situationen for tredjepartsudbyderen af IKT-tjenester

c) dokumenterede svagheder hos tredjepartsudbyderen af IKT-tjenester, som vedrører dennes samlede IKT-risikostyring, og navnlig i den måde, hvorpå denne garanterer tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, hvad enten det drejer sig om personoplysninger eller på anden måde følsomme data eller andre oplysninger end personoplysninger

d) hvis den kompetente myndighed ikke længere kan føre effektivt tilsyn med den finansielle enhed som følge af betingelserne eller omstændighederne vedrørende de respektive kontraktlige ordninger.

8. For så vidt angår IKT-tjenester, der understøtter kritiske eller vigtige funktioner, indfører de finansielle enheder exitstrategier. Exitstrategierne skal tage højde for de risici, der kan opstå hos tredjepartsudbydere af IKT-tjenester, navnlig mulige svigt fra deres side, en forringelse af kvaliteten af de leverede IKT-tjenester, eventuelle driftsforstyrrelser som følge af uhensigtsmæssig eller manglende levering af IKT-tjenester eller eventuelle væsentlige risici i forbindelse med en passende og løbende anvendelse af de pågældende IKT-tjenester eller opsigelse af kontraktlige ordninger med tredjepartsudbydere af IKT-tjenester i en af de i stk. 7 anførte situationer.

De finansielle enheder sikrer, at de kan opsige kontraktlige ordninger, uden:

a) at deres forretningsaktiviteter afbrydes

b) at efterlevelsen af de forskriftsmæssige krav begrænses

c) at kontinuiteten og kvaliteten af de leverede tjenester til kunder lider skade.

Exitplanerne skal være omfattende, veldokumenterede og, i overensstemmelse med kriterierne i artikel 4, stk. 2, testet i tilstrækkeligt omfang samt gennemgået regelmæssigt.

De finansielle enheder identificerer alternative løsninger og udarbejder overgangsplaner, således at de kan fratage tredjepartsudbyderen af IKT-tjenester de udliciterede IKT-tjenester og de relevante data og sikkert og fuldstændigt kan overføre disse til alternative udbydere eller på ny indarbejde dem internt.

De finansielle enheder indfører passende beredskabsforanstaltninger for at opretholde driftsstabiliteten i tilfælde af de i første afsnit omhandlede omstændigheder.

9. ESA'erne udarbejder via Det Fælles Udvalg udkast til gennemførelsesmæssige tekniske standarder for at fastlægge standardmodeller med henblik på det i stk. 3 omhandlede register over oplysninger, herunder oplysninger, som er fælles for alle kontraktlige ordninger for brugen af IKT-tjenester. ESA'erne forelægger disse udkast til gennemførelsesmæssige tekniske standarder for Kommissionen senest den 17. januar 2024.

Kommissionen tillægges beføjelse til at vedtage de i første afsnit omhandlede gennemførelsesmæssige tekniske standarder i overensstemmelse med artikel 15 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.

10. ESA'erne udarbejder via Det Fælles Udvalg udkast til reguleringsmæssige tekniske standarder for yderligere at præcisere det detaljerede indhold af den i stk. 2 omhandlede politik vedrørende de kontraktlige ordninger for brugen af IKT-tjenester, der understøtter kritiske eller vigtige funktioner, som leveres af tredjepartsudbydere af IKT-tjenester.

Når ESA'erne udarbejder disse udkast til reguleringsmæssige tekniske standarder, tager de hensyn til den finansielle enheds størrelse og samlede risikoprofil og karakteren, omfanget og kompleksiteten af dens tjenester, aktiviteter og operationer. ESA'erne forelægger disse udkast til reguleringsmæssige tekniske standarder for Kommissionen senest den 17. januar 2024.

Kommissionen tillægges beføjelse til at supplere denne forordning ved at vedtage de i første afsnit omhandlede reguleringsmæssige tekniske standarder i overensstemmelse med artikel 10-14 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.

Artikel 29

Foreløbig vurdering af IKT-koncentrationsrisiko på enhedsniveau

1. Når finansielle enheder foretager identifikation og vurdering af de risici, der er omhandlet i artikel 28, stk. 4, litra c), tager de også hensyn til, hvorvidt den påtænkte indgåelse af en kontraktlig ordning i forbindelse med IKT-tjenester, der understøtter kritiske eller vigtige funktioner, vil føre til et af følgende forhold:

a) udlicitering til en tredjepartsudbyder af IKT-tjenester, som ikke er let at erstatte, eller

b) indgåelse af flere kontraktlige ordninger om levering af IKT-tjenester, der understøtter kritiske eller vigtige funktioner, med den samme tredjepartsudbyder af IKT-tjenester eller med tredjepartsudbydere af IKT-tjenester, som har tætte forbindelser til denne.

De finansielle enheder afvejer fordele og omkostninger ved alternative løsninger såsom brug af forskellige tredjepart-sudbydere af IKT-tjenester under hensyntagen til, hvorvidt og hvordan de påtænkte løsninger svarer til de forretningsmæssige behov og mål, der er fastsat i deres strategi for digital modstandsdygtighed.

2. Hvis de kontraktlige ordninger for brugen af IKT-tjenester, der understøtter kritiske eller vigtige funktioner, omfatter muligheden for, at en tredjepartsudbyder af IKT-tjenester giver IKT-tjenester, der understøtter en kritisk eller vigtig funktion, videre i underentreprise til andre tredjepartsudbydere af IKT-tjenester, afvejer de finansielle enheder de fordele og risici, der kan opstå i forbindelse med en sådan underentreprise, navnlig hvis der er tale om en IKT-underleverandør med hjemsted i et tredjeland.

Hvis de kontraktlige ordninger vedrører IKT-tjenester, der understøtter kritiske eller vigtige funktioner, tager de finansielle enheder behørigt hensyn til de bestemmelser i insolvensretten, som finder anvendelse, hvis tredjepartsudbyderen af IKT-tjenester går konkurs, samt eventuelle begrænsninger, der kan opstå i forbindelse med en hastende genopretning af den finansielle enheds data.

Hvis der er indgået kontraktlige ordninger for brug af IKT-tjenester, der understøtter kritiske eller vigtige funktioner, med en tredjepartsudbyder af IKT-tjenester med hjemsted i et tredjeland, tager de finansielle enheder ud over til de i andet afsnit omhandlede forhold også hensyn til overholdelsen af Unionens databeskyttelsesregler og en effektiv håndhævelse af retten i det pågældende tredjeland.

Hvis de kontraktlige ordninger for brugen af IKT-tjenester, der understøtter kritiske eller vigtige funktioner, indeholder bestemmelser om underentreprise, vurderer de finansielle enheder, hvorvidt og hvordan potentielt lange eller komplekse underentreprisekæder kan påvirke deres evne til fuldt ud at overvåge de udliciterede funktioner og den kompetente myndigheds evne til i denne henseende at føre effektivt tilsyn med den finansielle enhed.

Artikel 30

Centrale kontraktbestemmelser

1. Rettigheder og forpligtelser for den finansielle enhed og for tredjepartsudbyderen af IKT-tjenester skal fordeles klart og fastlægges skriftligt. Den samlede kontrakt skal omfatte serviceniveauaftaler og dokumenteres i ét skriftligt dokument, som parterne skal have adgang til på papir, eller i et dokument i et andet varigt og tilgængeligt format, som kan downloades.

2. De kontraktlige ordninger for brugen af IKT-tjenester skal mindst omfatte følgende elementer:

a) en klar og fuldstændig beskrivelse af alle funktioner og IKT-tjenester, som tredjepartsudbyderen af IKT-tjenester skal levere, med angivelse af, om underentreprise af en IKT-tjeneste, der understøtter en kritisk eller vigtig funktion eller væsentlige dele heraf er tilladt, og, hvis det er tilfældet, de betingelser, der gælder for en sådan underentreprise

b) de steder, navnlig de regioner eller lande, hvor de udliciterede funktioner og IKT-tjenester eller funktionerne og IKT-tjenesterne i underentreprise skal leveres, og hvor data skal behandles, herunder lagringsstedet, og kravet om, at tredjepartsudbyderen af IKT-tjenester på forhånd skal underrette den finansielle enhed, hvis den har planer om at ændre disse steder

c) bestemmelser om tilgængelighed, autenticitet, integritet og fortrolighed med hensyn til databeskyttelse, herunder personoplysninger

d) bestemmelser om sikring af adgang, genopretning og tilbagesendelse i et lettilgængeligt format af personoplysninger og andre data end personoplysninger, der behandles af den finansielle enhed, i tilfælde af insolvens, afvikling eller afbrydelse af de forretningsaktiviteter, som tredjepartsudbyderen af IKT-tjenester varetager, eller i tilfælde af opsigelse af de kontraktlige ordninger

e) beskrivelser af serviceniveauet, herunder ajourføringer og revisioner heraf

f) forpligtelsen for tredjepartsudbyderen af IKT-tjenester til at yde bistand til den finansielle enhed uden yderligere omkostninger eller til en omkostning, der fastsættes på forhånd, hvis der opstår en IKT-hændelse, der vedrører den IKT-tjeneste, som leveres til den finansielle enhed

g) forpligtelsen for tredjepartsudbyderen af IKT-tjenester til at samarbejde fuldt ud med den finansielle enheds kompetente myndigheder og afviklingsmyndigheder, herunder personer, som de har udpeget

h) opsigelsesrettigheder og dertil knyttet minimumsfrister for opsigelse af de kontraktlige ordninger i overensstemmelse med de kompetente myndigheders og afviklingsmyndighedernes forventninger

i) betingelserne for deltagelse af tredjepartsudbydere af IKT-tjenester i de finansielle enheders programmer til bevidstgørelse om IKT-sikkerhed og kurser i digital operationel modstandsdygtighed, jf. artikel 13, stk. 6.

3. De kontraktlige ordninger for brugen af IKT-tjenester, der understøtter kritiske eller vigtige funktioner, skal ud over de elementer, der er omhandlet i stk. 2, mindst omfatte følgende:

a) en fuldstændig beskrivelse af serviceniveauer, herunder ajourføringer og revisioner heraf, med præcise kvantitative og kvalitative præstationsmål inden for de aftalte serviceniveauer, således at den finansielle enhed kan foretage en effektiv overvågning af IKT-tjenester, og således at der uden unødigt ophold kan træffes passende afhjælpende foranstaltninger, når de aftalte serviceniveauer ikke overholdes

b) opsigelsesfrister og indberetningsforpligtelser for tredjepartsudbyderen af IKT-tjenester over for den finansielle enhed, herunder underretning om enhver udvikling, som kan have væsentlig indvirkning på, hvorvidt tredjepartsudbyderen af IKT-tjenester har evnen til effektivt at levere IKT-tjenester, der understøtter kritiske eller vigtige funktioner i overensstemmelse med de aftalte serviceniveauer

c) krav til tredjepartsudbyderen af IKT-tjenester om at gennemføre og teste beredskabsplaner og indføre IKT-sikkerhedsforanstaltninger, -værktøjer og -politikker, som giver et passende niveau af sikkerhed for, at den finansielle enhed kan foretage levering af tjenester i overensstemmelse med dens reguleringsramme

d) forpligtelsen for tredjepartsudbyderen af IKT-tjenester til at deltage i og fuldt ud samarbejde om den finansielle enheds TLPT som omhandlet i artikel 26 og 27

e) retten til løbende at overvåge det præstationsniveau, som tredjepartsudbyderen af IKT-tjenester leverer, hvilket indebærer følgende:

i) den finansielle enheds eller en udpeget tredjeparts og den kompetente myndigheds uindskrænkede ret til adgang, inspektion og revision og ret til at tage kopier af relevant dokumentation på stedet, hvis denne har afgørende betydning for tredjepartsudbyderen af IKT-tjenesters operationer, hvis faktiske udøvelse ikke hindres eller begrænses af andre kontraktlige ordninger eller gennemførelsespolitikker

ii) retten til at nå til enighed om alternative sikkerhedsniveauer, hvis andre kunders rettigheder påvirkes

iii) forpligtelsen for tredjepartsudbyderen af IKT-tjenester til fuldt ud at samarbejde under de inspektioner og revisioner på stedet, som de kompetente myndigheder, den ledende tilsynsførende, den finansielle enhed eller en udpeget tredjepart udfører, og

iv) forpligtelsen til at give nærmere oplysninger om omfanget af, de procedurer, som skal følges, og hyppigheden af sådanne inspektioner og revisioner

f) exitstrategier, navnlig indførelse af en obligatorisk passende overgangsperiode:

i) i løbet af hvilken tredjepartsudbyderen af IKT-tjenester fortsat leverer de respektive funktioner eller IKT-tjenester med henblik på at mindske risikoen for forstyrrelser i den finansielle enhed eller sikre en effektiv afvikling eller omstrukturering heraf

ii) som giver den finansielle enhed mulighed for at migrere til en anden tredjepartsudbyder af IKT-tjenester eller skifte til interne løsninger, der stemmer overens med den leverede tjenestes kompleksitet.

Uanset litra e) kan tredjepartsudbyderen af IKT-tjenester og den finansielle enhed, som er en mikrovirksomhed, beslutte, at den finansielle enheds ret til adgang, inspektion og revision kan delegeres til en uafhængig tredjepart, som udpeges af tredjepartsudbyderen af IKT-tjenester, og at den finansielle enhed til enhver tid kan anmode tredjeparten om oplysninger og garantier vedrørende de resultater, som tredjepartsudbyderen af IKT-tjenester opnår.

4. Når finansielle enheder og tredjepartsudbydere af IKT-tjenester forhandler om kontraktlige ordninger, overvejer de anvendelsen af standardkontraktbestemmelser, som de offentlige myndigheder har udviklet til specifikke tjenester.

5. ESA'erne udarbejder via Det Fælles Udvalg udkast til reguleringsmæssige tekniske standarder med henblik på yderligere at præcisere de i stk. 2, litra a), omhandlede elementer, som en finansiel enhed skal fastlægge og vurdere, når den giver IKT-tjenester, der understøtter kritiske eller vigtige funktioner, i underentreprise.

Når ESA'erne udarbejder disse udkast til reguleringsmæssige tekniske standarder, tager de hensyn til den finansielle enheds størrelse og samlede risikoprofil og karakteren, omfanget og kompleksiteten af dens tjenester, aktiviteter og operationer.

ESA'erne forelægger disse udkast til reguleringsmæssige tekniske standarder for Kommissionen senest den 17. juli 2024.

Kommissionen tillægges beføjelse til supplere denne forordning ved at vedtage de i første afsnit omhandlede reguleringsmæssige tekniske standarder i overensstemmelse med artikel 10-14 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.

Afdeling II

Tilsynsramme for kritiske tredjepartsudbydere af IKT-tjenester

Artikel 31

Udpegelse af kritiske tredjepartsudbydere af IKT-tjenester

1. ESA'erne skal via Det Fælles Udvalg og efter henstilling fra det tilsynsforum, der er oprettet i henhold til artikel 32, stk. 1,

a) udpege de tredjepartsudbydere af IKT-tjenester, der er kritiske for finansielle enheder efter en vurdering, der tager hensyn til kriterierne i stk. 2

b) som ledende tilsynsførende for hver kritisk tredjepartsudbyder af IKT-tjenester udpege den ESA, der i overensstemmelse med forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 eller (EU) nr. 1095/2010 er ansvarlig for de finansielle enheder, der tilsammen besidder den største andel samlede aktiver ud af værdien af de samlede aktiver for alle de finansielle enheder, der benytter sig af tjenester fra den pågældende kritiske tredjepartsudbyder af IKT-tjenester, således som det fremgår af summen af de individuelle balancer for disse finansielle enheder.

2. Den udpegelse, der er omhandlet i stk. 1, litra a), skal i forbindelse med IKT-tjenester, der leveres af tredjepartsudbyderen af IKT-tjenester, baseres på samtlige følgende kriterier:

a) den systemiske indvirkning på stabiliteten, kontinuiteten eller kvaliteten af leveringen af finansielle tjenesteydelser i tilfælde af, at den pågældende tredjepartsudbyder af IKT-tjenester udsættes for et stort operationelt svigt, således at denne ikke kan levere sine tjenester, idet der tages hensyn til antallet af finansielle enheder og den samlede værdi af aktiverne hos de finansielle enheder, som den pågældende tredjepartsudbyder af IKT-tjenester leverer tjenester til

b) den systemiske karakter eller betydning af de finansielle enheder, der er afhængige af den pågældende tredjepartsudbyder af IKT-tjenester, vurderet i overensstemmelse med følgende parametre:

   i) antallet af globale systemisk vigtige institutter (G-SII'er) eller andre systemisk vigtige institutter (O-SII'er), som er afhængige af den pågældende tredjepartsudbyder af IKT-tjenester

   ii) den indbyrdes afhængighed mellem de i nr. i) omhandlede G-SII'er eller O-SII'er og andre finansielle enheder, herunder situationer, hvor G-SII'erne eller O-SII'erne leverer finansielle infrastrukturtjenester til andre finansielle enheder

c) finansielle enheders afhængighed af de tjenester, der leveres af de pågældende tredjepartsudbydere af IKT-tjenester, i forbindelse med kritiske eller vigtige funktioner i finansielle enheder, som i sidste ende involverer den samme tredjepartsudbyder af IKT-tjenester, uanset om de benytter sig af disse tjenester direkte eller indirekte, gennem underentrepriseordninger

d) i hvilket omfang tredjepartsudbyderen af IKT-tjenester kan erstattes under hensyntagen til følgende parametre:

   i) manglen på reelle alternativer, selv delvist, på grund af det begrænsede antal tredjepartsudbydere af IKT-tjenester, der er aktive på et specifikt marked, eller den pågældende tredjepartsudbyder af IKT-tjenesters markedsandel, eller den involverede tekniske kompleksitet eller finesse, herunder i forbindelse med eventuelle egne teknologier, eller de særlige kendetegn ved tredjepartsudbyderen af IKT-tjenesters organisation eller aktivitet

   ii) vanskeligheder i forbindelse med helt eller delvist at migrere de relevante data og arbejdsbyrden fra den pågældende tredjepartsudbyder af IKT-tjenester til en anden tredjepartsudbyder af IKT-tjenester, enten på grund af betydelige finansielle omkostninger, tid eller andre ressourcer, som migreringen kan kræve, eller en øget IKT-risiko eller andre operationelle risici, som den finansielle enhed kan blive eksponeret for ved en sådan migrering.

3. Hvis tredjepartsudbyderen af IKT-tjenester indgår i en koncern, tages kriterierne i stk. 2 i betragtning i forhold til de IKT-tjenester, der leveres af koncernen som helhed.

4. Kritiske tredjepartsudbydere af IKT-tjenester, som indgår i en koncern, udpeger én juridisk person som koordineringspunkt for at sikre en passende repræsentation og kommunikation med den ledende tilsynsførende.

5. Den ledende tilsynsførende underretter tredjepartsudbyderen af IKT-tjenester om resultatet af den vurdering, der fører til udpegelsen, jf. stk. 1, litra a). Senest seks uger efter datoen for underretningen kan tredjepartsudbyderen af IKT-tjenester forelægge den ledende tilsynsførende en begrundet erklæring med alle relevante oplysninger med henblik på vurderingen. Den ledende tilsynsførende tager den begrundede erklæring i betragtning og kan anmode om, at der forelægges yderligere oplysninger inden for 30 kalenderdage efter modtagelsen af en sådan erklæring.

Efter at have udpeget en tredjepartsudbyder af IKT-tjenester som kritisk underretter ESA'erne gennem Det Fælles Udvalg tredjepartsudbyderen af IKT-tjenester om en sådan udpegelse og om startdatoen for, hvornår de reelt vil være omfattet af tilsynsaktiviteter. Denne startdato må ikke være senere end en måned efter underretningen. Tredjepartsudbyderen af IKT-tjenester underretter de finansielle enheder, som de leverer tjenester til, om deres udpegelse som kritiske.

6. Kommissionen tillægges beføjelser til at vedtage en delegeret retsakt i overensstemmelse med artikel 57 for at supplere denne forordning ved yderligere at præcisere de kriterier, der er omhandlet i nærværende artikels stk. 2, senest den 17. juli 2024.

7. Den udpegelse, der er omhandlet i stk. 1, litra a), må først anvendes, når Kommissionen har vedtaget en delegeret retsakt i overensstemmelse med stk. 6.

8. Den udpegelse, der er omhandlet i stk. 1, litra a), finder ikke anvendelse på følgende:

i) finansielle enheder, der leverer IKT-tjenester til andre finansielle enheder

ii) tredjepartsudbydere af IKT-tjenester, som er underlagt tilsynsrammer, der er etableret med henblik på at understøtte de opgaver, der er omhandlet i artikel 127, stk. 2, i traktaten om Den Europæiske Unions funktionsmåde

iii) koncerninterne udbydere af IKT-tjenester

iv) tredjepartsudbydere af IKT-tjenester, der udelukkende leverer IKT-tjenester i én medlemsstat til finansielle enheder, der kun er aktive i den pågældende medlemsstat.

9. ESA'erne udarbejder, offentliggør og ajourfører årligt via Det Fælles Udvalg listen over kritiske tredjepartsudbydere af IKT-tjenester på EU-plan.

10. Med henblik på stk. 1, litra a), videregiver de kompetente myndigheder på et årligt og aggregeret grundlag de rapporter, der er omhandlet i artikel 28, stk. 3, tredje afsnit, til det tilsynsforum, der er oprettet i henhold til artikel 32. Tilsynsforummet vurderer finansielle enheders afhængighed af tredjepartsudbydere af IKT-tjenester på grundlag af oplysninger, som det modtager fra de kompetente myndigheder.

11. De tredjepartsudbydere af IKT-tjenester, der ikke er opført på den i stk. 9 omhandlede liste, kan anmode om at blive udpeget som kritiske i overensstemmelse med stk. 1, litra a).

Med henblik på første afsnit indgiver tredjepartsudbyderen af IKT-tjenester en begrundet anmodning til EBA, ESMA eller EIOPA, som via Det Fælles Udvalg træffer afgørelse, om den pågældende tredjepartsudbyder af IKT-tjenester skal udpeges som kritisk i overensstemmelse med stk. 1, litra a).

Den i andet afsnit omhandlede afgørelse vedtages og meddeles tredjepartsudbyderen af IKT-tjenester senest 6 måneder efter modtagelsen af anmodningen.

12. Finansielle enheder benytter kun tjenester, der udbydes af en tredjepartsudbyder af IKT-tjenester med hjemsted i et tredjeland, der er udpeget som kritisk i overensstemmelse med stk. 1, litra a), hvis sidstnævnte har etableret en dattervirksomhed i Unionen senest 12 måneder efter udpegelsen.

13. Den i stk. 12 omhandlede kritiske tredjepartsudbyder af IKT-tjenester underretter den ledende tilsynsførende om eventuelle ændringer af ledelsesstrukturen i den dattervirksomhed, der er etableret i Unionen.

Artikel 32

Tilsynsrammens struktur

1. Det Fælles Udvalg opretter i overensstemmelse med artikel 57, stk. 1, i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010 tilsynsforummet som et underudvalg med henblik på at støtte det arbejde, der udføres i Det Fælles Udvalg og af den ledende tilsynsførende, der er omhandlet i artikel 31, stk. 1, litra b), med hensyn til IKT-tredjepartsrisiko på tværs af finansielle sektorer. Tilsynsforummet udarbejder udkast til fælles holdninger og udkast til fælles retsakter vedtaget af Det Fælles Udvalg inden for dette område.

Tilsynsforummet drøfter regelmæssigt relevante udviklingstendenser vedrørende IKT-risiko og -sårbarheder og fremmer en konsekvent tilgang til overvågning af IKT-tredjepartsrisiko på EU-plan.

2. Tilsynsforummet foretager på årsbasis en kollektiv vurdering af resultaterne og konklusionerne fra de tilsynsaktiviteter, der udføres for alle kritiske tredjepartsudbydere af IKT-tjenester, og fremmer koordineringsforanstaltninger for at øge finansielle enheders digitale operationelle modstandsdygtighed, fremme bedste praksis for håndtering af IKT-koncentrationsrisiko og undersøge foranstaltninger til modvirkning af risikoafsmitning på tværs af sektorer.

3. Tilsynsforummet forelægger omfattende benchmarks for kritiske tredjepartsudbydere af IKT-tjenester, som skal vedtages af Det Fælles Udvalg som ESA'ernes fælles holdninger i overensstemmelse med artikel 56, stk. 1, i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.

4. Tilsynsforummet er sammensat af:

a) formændene for ESA'erne

b) én repræsentant på højt niveau fra det nuværende personale i den relevante kompetente myndighed, jf. artikel 46, fra hver medlemsstat

c) de administrerende direktører for hver ESA og en repræsentant fra henholdsvis Kommissionen, ESRB, ECB og ENISA som observatører

d) hvor det er hensigtsmæssigt, yderligere en repræsentant for en kompetent myndighed, jf. artikel 46, fra hver medlemsstat som observatør

e) hvor det er relevant, en repræsentant for de kompetence myndigheder udpeget eller oprettet i overensstemmelse med direktiv (EU) 2022/2555, som har ansvar for tilsynet med en væsentlig eller vigtig enhed, der er omfattet af nævnte direktiv og er blevet udpeget som en kritisk tredjepartsudbyder af IKT-tjenester, som observatør

Tilsynsforummet kan, hvor det er hensigtsmæssigt, rådføre sig med uafhængige eksperter, der er udpeget i overensstemmelse med stk. 6.

5. Hver medlemsstat udpeger den relevante kompetente myndighed, hvis ansatte skal være den repræsentant på højt niveau, der er omhandlet i stk. 4, første afsnit, litra b), og underretter den ledende tilsynsførende herom.

ESA'erne offentliggør på deres websted listen over højtstående repræsentanter fra det nuværende personale i den relevante kompetente myndighed udpeget af medlemsstaterne.

6. De uafhængige eksperter, der er omhandlet i stk. 4, andet afsnit, udpeges af tilsynsforummet fra en pulje af eksperter, der udvælges efter en offentlig og gennemsigtig ansøgningsproces.

De uafhængige eksperter udpeges for en toårig periode på grundlag af deres ekspertise i finansiel stabilitet, digital operationel modstandsdygtighed og IKT-sikkerhedsspørgsmål. De handler uafhængigt og objektivt udelukkende i Unionens interesse som helhed og må ikke søge eller modtage instrukser fra EU-institutioner eller -organer, medlemsstaters regeringer eller noget andet offentligt eller privat organ.

7. I overensstemmelse med artikel 16 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010 udsteder ESA'erne senest den 17. juli 2024 med henblik på denne afdeling retningslinjer for samarbejdet mellem ESA'erne og de kompetente myndigheder om de nærmere procedurer og betingelser for tildelingen og varetagelsen af opgaver mellem de kompetente myndigheder og ESA'erne samt nærmere oplysninger om den informationsudveksling, der er nødvendig for, at de kompetente myndigheder kan sikre opfølgning af henstillinger, jf. artikel 35, stk. 1, litra d), rettet til kritiske tredjepartsudbydere af IKT-tjenester.

8. Kravene i denne afdeling berører ikke anvendelsen af direktiv (EU) 2022/2555 og af andre EU-regler om tilsyn, som finder anvendelse på udbydere af cloudcomputingtjenester.

9. ESA'erne forelægger gennem Det Fælles Udvalg og på grundlag af det forberedende arbejde, der udføres af tilsynsforummet, årligt en rapport om anvendelsen af denne afdeling for Europa-Parlamentet, Rådet og Kommissionen.

Artikel 33

Den ledende tilsynsførendes opgaver

1. Den ledende tilsynsførende, der er udpeget i overensstemmelse med artikel 31, stk. 1, litra b), fører tilsyn med de tildelte kritiske tredjepartsudbydere af IKT-tjenester og er med henblik på alle spørgsmål vedrørende tilsynet det primære kontaktpunkt for disse kritiske tredjepartsudbydere af IKT-tjenester.

2. Den ledende tilsynsførende vurderer med henblik på stk. 1, om hver enkelt kritisk tredjepartsudbyder af IKT-tjenester har indført omfattende, robuste og effektive regler, procedurer, mekanismer og ordninger til styring af den IKT-risiko, som den kan udsætte finansielle enheder for.

Den vurdering, der er omhandlet i første afsnit, skal primært fokusere på de IKT-tjenester, som leveres af den kritiske tredjepartsudbyder af IKT-tjenester, og som understøtter finansielle enheders kritiske eller vigtige funktioner. Hvis det er nødvendigt for at imødegå alle relevante risici, skal denne vurdering omfatte IKT-tjenester, der understøtter andre funktioner end dem, der er kritiske eller vigtige.

3. Den i stk. 2 omhandlede vurdering dækker følgende:

a) IKT-krav, som navnlig skal garantere sikkerhed, tilgængelighed, kontinuitet, skalerbarhed og kvalitet for de tjenester, som den kritiske tredjepartsudbyder af IKT-tjenester leverer til finansielle enheder, samt at der til enhver tid kan opretholdes høje standarder for tilgængelighed, autenticitet, integritet eller fortrolighed

b) fysisk sikkerhed, som bidrager til at garantere IKT-sikkerheden, herunder sikkerheden i lokaler, faciliteter og datacentre

c) risikostyringsprocesser, herunder politikker for IKT-risikostyring, politik for IKT-driftsstabilitet og planer for IKT-indsats og -genopretning

d) forvaltningsordninger, herunder en organisatorisk struktur med en klar, gennemsigtig og konsekvent ansvarsfordeling og regler om ansvarliggørelse, som muliggør effektiv IKT-risikostyring

e) identifikation, overvågning og hurtig indberetning af væsentlige IKT-relaterede hændelser til de finansielle enheder samt håndtering og afvikling af disse hændelser, navnlig cyberangreb

f) mekanismer for dataportabilitet, applikationsportabilitet og interoperabilitet, som sikrer en effektiv udøvelse af opsigelsesrettighederne for de finansielle enheder

g) test af IKT-systemer, -infrastruktur og -kontrolfunktioner

h) IKT-revisioner

i) anvendelse af relevante nationale og internationale standarder, som gælder for levering af IKT-tjenester til finansielle enheder.

4. På grundlag af den i stk. 2 omhandlede vurdering og i samordning med det fælles tilsynsnetværk, der er omhandlet i artikel 34, stk. 1, vedtager den ledende tilsynsførende en klar, detaljeret og begrundet individuel tilsynsplan, der beskriver de årlige tilsynsmål og de vigtigste tilsynstiltag, der er planlagt for hver enkelt kritisk tredjepartsudbyder af IKT-tjenester. Denne plan skal hvert år meddeles den kritiske tredjepartsudbyder af IKT-tjenester.

Forud for vedtagelsen af tilsynsplanen skal den ledende tilsynsførende meddele udkastet til tilsynsplan til den kritiske tredjepartsudbyder af IKT-tjenester.

Efter modtagelsen af udkastet til tilsynsplan kan den kritiske tredjepartsudbyder af IKT-tjenester inden for 15 kalenderdage indsende en begrundet erklæring, der dokumenterer den forventede virkning på kunder, som er enheder, der ikke er omfattet af denne forordnings anvendelsesområde, og, hvis det er relevant, udarbejde løsninger til at afbøde risici.

5. Når de i stk. 4 omhandlede årlige tilsynsplaner er blevet vedtaget og meddelt de kritiske tredjepartsudbydere af IKT-tjenester, kan de kompetente myndigheder kun træffe foranstaltninger, som vedrører sådanne kritiske tredjepartsudbydere af IKT-tjenester, efter aftale med den ledende tilsynsførende.

Artikel 34

Operationel koordinering mellem ledende tilsynsførende

1. For at sikre en konsekvent tilgang til tilsynsaktiviteter og med henblik på at muliggøre koordinerede generelle tilsynsstrategier og sammenhængende operationelle tilgange og arbejdsmetoder opretter de tre ledende tilsynsførende, der er udpeget i overensstemmelse med artikel 31, stk. 1, litra b), et fælles tilsynsnetværk, der skal koordinere indbyrdes i forbindelse med de forberedende faser og koordinere udførelsen af tilsynsaktiviteter med hensyn til deres respektive kritiske tredjepartsudbydere af IKT-tjenester, der føres tilsyn med, og i forbindelse med eventuelle tiltag, der måtte være nødvendige i henhold til artikel 42.

2. Med henblik på stk. 1 udarbejder de ledende tilsynsførende en fælles tilsynsprotokol, der præciserer de nærmere procedurer, der skal følges for at gennemføre den daglige koordinering og sikre hurtige udvekslinger og reaktioner. Protokollen revideres regelmæssigt for at afspejle de operationelle behov, navnlig de praktiske tilsynsordningers udvikling.

3. De ledende tilsynsførende kan på ad hoc-basis anmode ECB og ENISA om at yde teknisk rådgivning, udveksle praktiske erfaringer eller deltage i specifikke koordineringsmøder i det fælles tilsynsnetværk.

Artikel 35

Den ledende tilsynsførendes beføjelser

1. Med henblik på varetagelsen af de i denne afdeling omhandlede opgaver tillægges den ledende tilsynsførende følgende beføjelser med hensyn til de kritiske tredjepartstjenesteudbydere af IKT-tjenester:

a) at anmode om alle relevante oplysninger og dokumentation i overensstemmelse med artikel 37

b) at foretage generelle undersøgelser og inspektioner i overensstemmelse med henholdsvis artikel 38 og 39

c) efter afslutningen af tilsynsaktiviteterne at anmode om rapporter med angivelse af de tiltag, der er iværksat, eller de afhjælpende foranstaltninger, som de kritiske tredjepartsudbydere af IKT-tjenester har truffet i forbindelse med de i litra d) omhandlede henstillinger

d) at udstede henstillinger vedrørende de områder, der er omhandlet i artikel 33, stk. 3, og navnlig følgende:

   i) anvendelse af specifikke IKT-relaterede sikkerheds- og kvalitetskrav eller -processer, navnlig i forbindelse med udrulningen af programrettelser, opdateringer, kryptering og andre sikkerhedsforanstaltninger, som den ledende tilsynsførende betragter som relevante for at garantere IKT-sikkerheden for tjenester, der leveres til finansielle enheder

   ii) anvendelse af betingelser og vilkår, herunder den tekniske gennemførelse heraf, i henhold til hvilke de kritiske tredjepartsudbydere af IKT-tjenester leverer tjenester til finansielle enheder, og som den ledende tilsynsførende skønner relevante for at forhindre, at der genereres single points of failure, eller at disse forstærkes, eller for at minimere de eventuelle systemiske virkninger på tværs af Unionens finansielle sektor i tilfælde af IKT-koncentrationsrisici

   iii) eventuelle planlagte underentrepriser, hvor den ledende tilsynsførende på baggrund af undersøgelsen af de oplysninger, der er indhentet i overensstemmelse med artikel 37 og 38, skønner, at videregivelse i underentreprise, herunder ordninger for underentrepriser, som de kritiske tredjepartsudbydere af IKT-tjenester planlægger at indgå med tredjepartsudbydere af IKT-tjenester eller med IKT-underleverandører med hjemsted i et tredjeland, kan udløse risici for den finansielle enheds levering af tjenester eller risici for den finansielle stabilitet

   iv) at afholde sig fra at indgå en ordning om videregivelse i underentreprise, når følgende kumulative betingelser er opfyldt:

      — den påtænkte underleverandør er en tredjepartsudbyder af IKT-tjenester eller en IKT-underleverandør med hjemsted i et tredjeland

      — underentreprisen vedrører kritiske eller vigtige funktion for den finansielle enhed, og

— den ledende tilsynsførende vurderer, at anvendelsen af en sådan underentreprise udgør en klar og alvorlig risiko for den finansielle stabilitet i Unionen eller for finansielle enheder, herunder finansielle enheders evne til at overholde tilsynskravene.

Tredjepartsudbydere af IKT-tjenester videregiver med henblik på dette litras nr. iv) ved brug af den model, der er omhandlet i artikel 41, stk. 1, litra b), oplysninger om underentrepriser til den ledende tilsynsførende.

2. Ved udøvelsen af de beføjelser, der er omhandlet i denne artikel, skal den ledende tilsynsførende:

a) sikre regelmæssig koordinering inden for det fælles tilsynsnetværk og navnlig tilstræbe konsekvente tilgange, alt efter hvad der er relevant, med hensyn til tilsynet med kritiske tredjepartsudbydere af IKT-tjenester

b) tage behørigt hensyn til den ramme, der er fastsat ved direktiv (EU) 2022/2555, og om nødvendigt høre de relevante kompetente myndigheder, der er udpeget eller oprettet i overensstemmelse med nævnte direktiv, for at undgå overlapning af tekniske og organisatoriske foranstaltninger, som kan finde anvendelse på kritiske tredjepartsudbydere af IKT-tjenester i henhold til nævnte direktiv

c) så vidt muligt tilstræbe at minimere risikoen for forstyrrelser i tjenester, som kritiske tredjepartsudbydere af IKT-tjenester leverer til kunder, der er enheder, som ikke er omfattet af denne forordnings anvendelsesområde.

3. Den ledende tilsynsførende hører tilsynsforummet forud for udøvelsen af de i stk. 1 omhandlede beføjelser.

Inden den ledende tilsynsførende udsteder henstillinger i overensstemmelse med stk. 1, litra d), giver den tredjepartsudbyderen af IKT-tjenester mulighed for inden for 30 kalenderdage at fremlægge relevante oplysninger, der dokumenterer den forventede virkning på kunder, som er enheder, der ikke er omfattet af denne forordnings anvendelsesområde, og, hvis det er relevant, udarbejde løsninger til at afbøde risici.

4. Den ledende tilsynsførende underretter det fælles tilsynsnetværk om resultatet af udøvelsen af de beføjelser, der er omhandlet i stk. 1, litra a) og b). Den ledende tilsynsførende videregiver uden unødig forsinkelse de rapporter, der er omhandlet i stk. 1, litra c), til det fælles tilsynsnetværk og til de kompetente myndigheder for de finansielle enheder, der anvender IKT-tjenester leveret af den pågældende kritiske tredjepartsudbyder af IKT-tjenester.

5. Kritiske tredjepartsudbydere af IKT-tjenester samarbejder i god tro med den ledende tilsynsførende og bistår den ledende tilsynsførende med hensyn til varetagelsen af dennes opgaver.

6. I tilfælde af hel eller delvis manglende overholdelse af de foranstaltninger, der skal træffes i henhold til udøvelsen af beføjelserne i stk. 1, litra a), b) og c), og efter udløbet af en periode på mindst 30 kalenderdage fra den dato, hvor den kritiske tredjepartsudbyder af IKT-tjenester har modtaget underretning om de respektive foranstaltninger, vedtager den ledende tilsynsførende en afgørelse, der pålægger en tvangsbøde for at tvinge den kritiske tredjepartsudbyder af IKT-tjenester til at efterleve disse foranstaltninger.

7. De i stk. 6 omhandlede tvangsbøder pålægges dagligt, indtil der er opnået efterlevelse, og i højst seks måneder efter meddelelsen af afgørelsen om at pålægge den kritiske tredjepartsudbyder af IKT-tjenester en tvangsbøde.

8. Størrelsen af tvangsbøderne, der beregnes fra den dato, der er anført i afgørelsen om pålæggelse af tvangsbøder, udgør op til 1 % af den kritiske tredjepartsudbyder af IKT-tjenesters gennemsnitlige daglige omsætning på verdensplan i det foregående regnskabsår. Ved fastsættelsen af tvangsbødens størrelse tager den ledende tilsynsførende hensyn til følgende kriterier vedrørende manglende overholdelse af de foranstaltninger, der er omhandlet i stk. 6:

a) den manglende overholdelses grovhed og varighed

b) hvorvidt den manglende overholdelse er forsætlig eller skyldes uagtsomhed

c) niveauet af samarbejde mellem tredjepartsudbyderen af IKT-tjenester og den ledende tilsynsførende.

Med henblik på første afsnit skal den ledende tilsynsførende for at sikre en konsekvent tilgang deltage i samråd inden for det fælles tilsynsnetværk.

9. Tvangsbøder er af administrativ karakter og skal kunne tvangsfuldbyrdes. Tvangsfuldbyrdelsen sker efter den borgerlige retsplejes regler i den medlemsstat, på hvis område inspektioner og adgang skal finde sted. Domstole i den pågældende medlemsstat har kompetence til at træffe afgørelse om klager vedrørende uregelmæssigheder i forbindelse med tvangsfuldbyrdelsen. Beløbene for tvangsbøderne overføres til Den Europæiske Unions almindelige budget.

10. Den ledende tilsynsførende offentliggør alle de pålagte tvangsbøder, medmindre en sådan offentliggørelse vil være til alvorlig skade for de finansielle markeder eller forvolde de involverede parter uforholdsmæssig stor skade.

11. Inden der pålægges tvangsbøder i henhold til stk. 6, giver den ledende tilsynsførende repræsentanter for den kritiske tredjepartsudbyder af IKT-tjenester, som er genstand for proceduren, mulighed for at blive hørt om de konstaterede forhold og baserer sine afgørelser udelukkende på forhold, som den kritiske tredjepartsudbyder af IKT-tjenester, der er genstand for proceduren, har haft lejlighed til at fremsætte bemærkninger til.

Retten til forsvar for de personer, som er genstand for proceduren, skal respekteres fuldt ud under procedureforløbet. Den kritiske tredjepartsudbyder af IKT-tjenester, der er genstand for proceduren, har ret til aktindsigt i dossieret med forbehold af andre personers berettigede interesse i, at deres forretningshemmeligheder ikke afsløres. Retten til aktindsigt omfatter ikke fortrolige oplysninger eller den ledende tilsynsførendes interne forberedende dokumenter.

Artikel 36

Den ledende tilsynsførendes udøvelse af beføjelser uden for Unionen

1. Når tilsynsmålene ikke kan nås ved at interagere med den dattervirksomhed, der er oprettet med henblik på artikel 31, stk. 12, eller ved at udøve tilsynsaktiviteter i lokaler i Unionen, kan den ledende tilsynsførende udøve de i de følgende bestemmelser omhandlede beføjelser i ethvert lokale i et tredjeland, som med henblik på levering af tjenester til finansielle enheder i Unionen ejes eller på nogen måde anvendes af en kritisk tredjepartsudbyder af IKT-tjenester i forbindelse med dennes forretningsaktiviteter, funktioner eller tjenester, herunder alle administrative, forretningsmæssige eller operationelle kontorer, lokaler, arealer, bygninger eller andre ejendomme:

a) i artikel 35, stk. 1, litra a), og

b) i artikel 35, stk. 1, litra b), i overensstemmelse med artikel 38, stk. 2, litra a), b) og d), og artikel 39, stk. 1, og artikel 39, stk. 2, litra a).

De i første afsnit omhandlede beføjelser kan udøves med forbehold af overholdelse af alle følgende betingelser:

i) den ledende tilsynsførende anser det for nødvendigt, at der foretages inspektion i et tredjeland, for at denne fuldt ud og effektivt kan udføre sine opgaver i henhold til denne forordning

ii) inspektionen i et tredjeland er direkte knyttet til leveringen af IKT-tjenester til finansielle enheder i Unionen

iii) den pågældende kritiske tredjepartsudbyder af IKT-tjenester giver sit samtykke til, at der foretages en inspektion i et tredjeland, og

iv) den relevante myndighed i det pågældende tredjeland er blevet officielt underrettet af den ledende tilsynsførende og har ikke gjort indsigelse herimod.

2. Uden at det berører EU-institutionernes og medlemsstaternes respektive beføjelser, indgår EBA, ESMA eller EIOPA med henblik på stk. 1 administrative samarbejdsordninger med den relevante myndighed i tredjelandet med henblik på at gøre det muligt for den ledende tilsynsførende og det team, den har udpeget til opgaven i det pågældende tredjeland, at foretage gnidningsløse inspektioner i det pågældende tredjeland. Disse samarbejdsordninger må ikke skabe retlige forpligtelser for Unionen og dens medlemsstater og heller ikke forhindre medlemsstaterne og deres kompetente myndigheder i at indgå bilaterale eller multilaterale aftaler med disse tredjelande og deres relevante myndigheder.

Disse samarbejdsordninger præciserer som minimum følgende elementer:

a) procedurerne for koordinering af de tilsynsaktiviteter, der udføres i henhold til denne forordning, og enhver tilsvarende overvågning af IKT-tredjepartsrisiko i den finansielle sektor, der udøves af den relevante myndighed i det pågældende tredjeland, herunder nærmere oplysninger om videreformidling af sidstnævntes samtykke til, at den ledende tilsynsførende og dens udpegede team kan foretage generelle undersøgelser og inspektioner på stedet som omhandlet i stk. 1, første afsnit, på det område, der hører under dens jurisdiktion

b) mekanismen for overførsel af relevante oplysninger mellem EBA, ESMA eller EIOPA og den relevante myndighed i det pågældende tredjeland, navnlig i forbindelse med oplysninger, som den ledende tilsynsførende kan anmode om i henhold til artikel 37

c) mekanismerne for øjeblikkelig underretning fra den relevante myndighed i det pågældende tredjeland til EBA, ESMA eller EIOPA om tilfælde, hvor en tredjepartsudbyder af IKT-tjenester med hjemsted i et tredjeland, der er udpeget som kritisk i henhold til artikel 31, stk. 1, litra a), anses for at have overtrådt de krav, som den er forpligtet til at opfylde i henhold til det pågældende tredjelands gældende ret, når den leverer tjenester til finansieringsinstitutter i det pågældende tredjeland, samt de anvendte afhjælpende foranstaltninger og sanktioner

d) regelmæssig overførsel af opdateringer om regulerings- eller tilsynsmæssig udvikling vedrørende overvågning af IKT-tredjepartsrisiko for finansieringsinstitutter i det pågældende tredjeland

e) nærmere oplysninger, der om nødvendigt gør det muligt for én repræsentant for den relevante tredjelandsmyndighed at deltage i de inspektioner, der foretages af den ledende tilsynsførende og det udpegede team.

3. Når den ledende tilsynsførende ikke er i stand til at udføre tilsynsaktiviteter uden for Unionen, jf. stk. 1 og 2, skal denne

a) udøve sine beføjelser i henhold til artikel 35 på grundlag af alle de kendsgerninger og dokumenter, den råder over

b) dokumentere og redegøre for eventuelle konsekvenser af, at den ikke er i stand til at udføre de påtænkte tilsynsaktiviteter som omhandlet i denne artikel.

Der tages hensyn til de potentielle konsekvenser, der er omhandlet i dette stykkes litra b), i den ledende tilsynsførendes henstillinger fremsat i henhold til artikel 35, stk. 1, litra d).

Artikel 37

Anmodning om oplysninger

1. Den ledende tilsynsførende kan efter simpel anmodning eller ved en afgørelse kræve, at kritiske tredjepartsudbydere af IKT-tjenester fremlægger alle de oplysninger, der er nødvendige for, at den ledende tilsynsførende kan varetage sine opgaver i henhold til denne forordning, herunder alle relevante forretningsdokumenter eller operationelle dokumenter, kontrakter, politikker, dokumentation, rapporter om IKT-sikkerhedsrevision, indberetninger af IKT-relaterede hændelser samt oplysninger om parter, som den kritiske tredjepartsudbyder af IKT-tjenester har outsourcet operationelle funktioner eller aktiviteter til.

2. Når den ledende tilsynsførende sender en simpel anmodning om oplysninger i henhold til stk. 1, skal denne

a) henvise til denne artikel som retsgrundlag for anmodningen

b) angive formålet med anmodningen

c) præcisere, hvilke oplysninger der kræves

d) fastsætte en frist for fremlæggelsen af oplysningerne

e) meddele repræsentanten for den kritiske tredjepartsudbyder af IKT-tjenester, som anmodes om oplysningerne, at vedkommende ikke er forpligtet til at fremlægge oplysningerne, men at oplysningerne, såfremt vedkommende frivilligt fremlægger dem, ikke må være ukorrekte eller vildledende.

3. Når den ledende tilsynsførende ved afgørelse kræver udlevering af oplysninger i henhold til stk. 1, skal denne

a) henvise til denne artikel som retsgrundlag for anmodningen

b) angive formålet med anmodningen

c) præcisere, hvilke oplysninger der kræves

d) fastsætte en frist for fremlæggelsen af oplysningerne

e) angive de tvangsbøder, der er omhandlet i artikel 35, stk. 6, og som finder anvendelse, hvis de ønskede oplysninger er ufuldstændige, eller hvis de ikke fremlægges inden for den tidsfrist, som er omhandlet i dette stykkes litra d)

f) oplyse om retten til at appellere afgørelsen til ESA'ernes klagenævn og om retten til at indbringe en klage over afgørelsen for Den Europæiske Unions Domstol (Domstolen) i overensstemmelse med artikel 60 og 61 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.

4. De oplysninger, der anmodes om, udleveres af repræsentanterne for de kritiske tredjepartsudbydere af IKT-tjenester. Behørigt befuldmægtigede advokater kan udlevere oplysningerne på deres klienters vegne. Den kritiske tredjepartsudbyder af IKT-tjenester bærer det fulde ansvar, hvis oplysningerne er ufuldstændige, ukorrekte eller vildledende.

5. Den ledende tilsynsførende videregiver straks en kopi af afgørelsen om at udlevere oplysninger til de kompetente myndigheder for de finansielle enheder, der benytter sig af de tjenester, som de relevante kritiske tredjepartsudbydere af IKT-tjenester leverer, og til det fælles tilsynsnetværk.

Artikel 38

Generelle undersøgelser

1. For at varetage sine opgaver i henhold til denne forordning kan den ledende tilsynsførende, som bistås af det fælles undersøgelsesteam, der er omhandlet i artikel 40, stk. 1, om nødvendigt foretage undersøgelser af kritiske tredjepart-sudbydere af IKT-tjenester.

2. Den ledende tilsynsførende har beføjelse til:

a) at undersøge optegnelser, data, procedurer og andet materiale, som har betydning for varetagelsen af dennes opgaver, uanset det medium, hvorpå de er lagret

b) at tage eller erhverve bekræftede genparter eller udskrifter af sådanne optegnelser, data, dokumenterede procedurer og ethvert andet materiale

c) at indkalde repræsentanter for den kritiske tredjepartsudbyder af IKT-tjenester med henblik på mundtlige eller skriftlige redegørelser for forhold eller dokumenter, der vedrører undersøgelsens genstand og formål, og at optage svarene

d) at udspørge enhver anden fysisk eller juridisk person, der indvilliger heri, med det formål at indsamle oplysninger om undersøgelsens genstand

e) at anmode om optegnelser over telefonsamtaler og datatrafik.

3. De embedsmænd og andre personer, som den ledende tilsynsførende har bemyndiget til at foretage de i stk. 1 omhandlede undersøgelser, udøver deres beføjelser efter fremlæggelse af en skriftlig tilladelse, som angiver genstanden for undersøgelsen og formålet hermed.

Denne tilladelse skal også indeholde oplysninger om de tvangsbøder, der er omhandlet i artikel 35, stk. 6, hvis de krævede optegnelser, data, dokumenterede procedurer eller ethvert andet materiale eller svarene på de spørgsmål, der stilles til repræsentanter for tredjepartsudbyderne af IKT-tjenester, ikke fremlægges eller er ufuldstændige.

4. Repræsentanterne for de kritiske tredjepartsudbydere af IKT-tjenester skal lade sig underkaste undersøgelserne på grundlag af en afgørelse truffet af den ledende tilsynsførende. Afgørelsen skal angive undersøgelsens genstand og formål, de tvangsbøder, der er omhandlet i artikel 35, stk. 6, de retsmidler, der er tilgængelige i henhold til forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010, og retten til at indbringe en klage over afgørelsen for Domstolen.

5. Den ledende tilsynsførende underretter i god tid før indledningen af undersøgelsen de kompetente myndigheder for de finansielle enheder, som anvender IKT-tjenesterne fra den pågældende kritiske tredjepartsudbyder af IKT-tjenester, om den påtænkte undersøgelse og om de bemyndigede personers identitet.

Den ledende tilsynsførende meddeler det fælles tilsynsnetværk alle oplysninger, der er videregivet i henhold til første afsnit.

Artikel 39

Inspektioner

1. For at varetage sine opgaver i henhold til denne forordning kan den ledende tilsynsførende, som bistås af de fælles undersøgelsesteams, der er omhandlet i artikel 40, stk. 1, betræde og foretage alle nødvendige inspektioner på stedet i alle forretningslokaler, arealer eller ejendomme, som tilhører tredjepartsudbyderne af IKT-tjenester, f.eks. hovedkontorer, operationscentraler og sekundære lokaler, samt foretage eksterne inspektioner.

Med henblik på udøvelsen af de beføjelser, der er omhandlet i første afsnit, hører den ledende tilsynsførende det fælles tilsynsnetværk.

2. De embedsmænd og andre personer, som den ledende tilsynsførende har bemyndiget til at foretage inspektion på stedet, har beføjelse til at

a) betræde alle sådanne forretningslokaler, arealer eller ejendomme, og

b) forsegle alle sådanne forretningslokaler, regnskaber eller registre i det for inspektionen nødvendige tidsrum og omfang.

De embedsmænd og andre personer, som den ledende tilsynsførende har bemyndiget, udøver deres beføjelser efter fremlæggelse af en skriftlig tilladelse, der angiver genstanden for og formålet med inspektionen og de tvangsbøder, der er omhandlet i artikel 35, stk. 6, hvis repræsentanterne for de berørte kritiske tredjepartsudbydere af IKT-tjenester ikke lader sig underkaste inspektionen.

3. Den ledende tilsynsførende underretter i god tid før indledningen af inspektionen de kompetente myndigheder for de finansielle enheder, som anvender den pågældende tredjepartsudbyder af IKT-tjenester.

4. Inspektioner skal omfatte hele viften af relevante IKT-systemer, netværk, udstyr, oplysninger og data, der enten anvendes til eller bidrager til leveringen af IKT-tjenester til finansielle enheder.

5. Den ledende tilsynsførende underretter kritiske tredjepartsudbydere af IKT-tjenester i rimelig tid før enhver planlagt inspektion på stedet, medmindre en sådan underretning ikke er mulig på grund af en nød- eller krisesituation, eller hvis det vil føre til en situation, hvor inspektionen eller revisionen ikke længere vil være effektiv.

6. Den kritiske tredjepartsudbyder af IKT-tjenester skal lade sig underkaste inspektioner på stedet, som er påbudt i henhold til en afgørelse truffet af den ledende tilsynsførende. Afgørelsen skal angive inspektionens genstand og formål, fastsætte tidspunktet for inspektionens påbegyndelse og oplyse om de tvangsbøder, der er omhandlet i artikel 35, stk. 6, de retsmidler, der er tilgængelige i henhold til forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010, og om retten til at indbringe en klage over afgørelsen for Domstolen.

7. Hvis de embedsmænd og andre personer, der er bemyndiget af den ledende tilsynsførende, konstaterer, at en kritisk tredjepartsudbyder af IKT-tjenester gør indsigelse mod en inspektion, der er påbudt i henhold til denne artikel, underretter den ledende tilsynsførende den kritiske tredjepartsudbyder af IKT-tjenester om konsekvenserne af en sådan indsigelse, herunder muligheden for, at de kompetente myndigheder for de relevante finansielle enheder kan kræve, at de finansielle enheder opsiger de kontraktlige ordninger, der er indgået med den pågældende kritiske tredjepartsudbyder af IKT-tjenester.

Artikel 40

Løbende tilsyn

1. Når den ledende tilsynsførende udfører tilsynsaktiviteter, navnlig generelle undersøgelser eller inspektioner, bistås denne af et fælles undersøgelsesteam, som er oprettet for hver af de kritiske tredjepartsudbydere af IKT-tjenester.

2. Det fælles undersøgelsesteam, der er omhandlet i stk. 1, skal bestå af medarbejdere fra:

a) ESA'erne

b) de relevante kompetente myndigheder, der fører tilsyn med de finansielle enheder, som den kritiske tredjepartsudbyder af IKT-tjenester leverer IKT-tjenester til

c) den nationale kompetente myndighed, der er omhandlet i artikel 32, stk. 4, litra e), på frivillig basis

d) én national kompetent myndighed fra den medlemsstat, hvor den kritiske tredjepartsudbyder af IKT-tjenester har hjemsted, på frivillig basis.

Medlemmerne af det fælles undersøgelsesteam skal have ekspertise med hensyn til IKT-anliggender og operationel risiko. Arbejdet i det fælles undersøgelsesteam koordineres af en udpeget medarbejder under den ledende tilsynsførende (»koordinatoren for den ledende tilsynsførende«).

3. Inden for 3 måneder fra fuldførelsen af en undersøgelse eller en inspektion og efter at have hørt tilsynsforummet vedtager den ledende tilsynsførende henstillinger, som skal fremsættes over for den berørte kritiske tredjepartsudbyder af IKT-tjenester, i henhold til de i artikel 35 omhandlede beføjelser.

4. De i stk. 3 omhandlede henstillinger meddeles omgående den kritiske tredjepartsudbyder af IKT-tjenester og de kompetente myndigheder for de finansielle enheder, som den leverer IKT-tjenester til.

Med henblik på at varetage tilsynsaktiviteterne kan den ledende tilsynsførende tage hensyn til eventuelle relevante tredjepartscertificeringer og IKT-tredjeparters interne eller eksterne revisionsrapporter, som den kritiske tredjepartsudbyder af IKT-tjenester har stillet til rådighed.

Artikel 41

Harmonisering af de betingelser, der muliggør udførelsen af tilsynsaktiviteter

1. ESA'erne udarbejder via Det Fælles Udvalg udkast til reguleringsmæssige tekniske standarder for at præcisere følgende:

a) de oplysninger, som en tredjepartsudbyder af IKT-tjenester skal fremlægge i sin ansøgning om frivillig anmodning om at blive udpeget som kritisk, jf. artikel 31, stk. 11

b) indholdet, strukturen og formatet af de oplysninger, som tredjepartsudbydere af IKT-tjenester skal indgive, offentliggøre eller aflægge rapport om i henhold til artikel 35, stk. 1, herunder modellen for afgivelse af oplysninger om underentrepriseordninger

c) kriterierne for fastlæggelse af sammensætningen af det fælles undersøgelsesteam, der sikrer en afbalanceret deltagelse af medarbejdere fra ESA'erne og fra de relevante kompetente myndigheder, deres udpegelse, opgaver og arbejdsordninger

d) de nærmere oplysninger om de kompetente myndigheders vurdering af de foranstaltninger, som kritiske tredjepartsudbydere af IKT-tjenester har truffet på grundlag af henstillinger fra den ledende tilsynsførende, jf. artikel 42, stk. 3.

2. ESA'erne forelægger disse udkast til reguleringsmæssige tekniske standarder for Kommissionen senest den 17. juli 2024.

Kommissionen tillægges beføjelse til supplere denne forordning ved at vedtage de i stk. 1 omhandlede reguleringsmæssige tekniske standarder i overensstemmelse med den procedure, der er fastsat i artikel 10-14 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.

Artikel 42

De kompetente myndigheders opfølgning

1. Senest 60 kalenderdage efter modtagelsen af de henstillinger, der er fremsat af den ledende tilsynsførende i henhold til artikel 35, stk. 1, litra d), underretter de kritiske tredjepartsudbydere af IKT-tjenester enten den ledende tilsynsførende om, at de agter at følge henstillingerne, eller de giver en begrundet redegørelse for, hvorfor de agter ikke at følge henstillingerne. Den ledende tilsynsførende videregiver straks disse oplysninger til de kompetente myndigheder for de pågældende finansielle enheder.

2. Den ledende tilsynsførende offentliggør det, hvis en kritisk tredjepartsudbyder af IKT-tjenester undlader at underrette den ledende tilsynsførende i overensstemmelse med stk. 1, eller hvis den redegørelse, som den kritiske tredjepartsudbyder af IKT-tjenester har givet, ikke anses for at være tilstrækkelig. De offentliggjorte oplysninger skal oplyse om identiteten af den kritiske tredjepartsudbyder af IKT-tjenester og om typen og arten af den manglende overholdelse. Sådanne oplysninger begrænses til, hvad der er relevant og forholdsmæssigt med henblik på at sikre offentlighedens bevidsthed, medmindre en sådan offentliggørelse vil kunne forvolde de involverede parter uforholdsmæssig stor skade eller i alvorlig grad bringe de finansielle markeders velordnede funktion og integritet eller stabiliteten af hele eller dele af Unionens finansielle system i fare.

Den ledende tilsynsførende underretter tredjepartsudbyderen af IKT-tjenester om den pågældende offentliggørelse.

3. De kompetente myndigheder informerer de relevante finansielle enheder om de risici, der er identificeret i de henstillinger, som er fremsat over for kritiske tredjepartsudbydere af IKT-tjenester i overensstemmelse med artikel 35, stk. 1, litra d).

Når de finansielle enheder styrer IKT-tredjepartsrisici tager de hensyn til de risici, der er omhandlet i første afsnit.

4. Hvis en kompetent myndighed vurderer, at en finansiel enhed ikke tager hensyn til eller ikke i tilstrækkelig grad i sin styring af IKT-tredjepartsrisiko imødegå de specifikke risici, der er identificeret i henstillingerne, underretter den den finansielle enhed om muligheden for, at der inden for 60 kalenderdage efter modtagelsen af en sådan underretning træffes en afgørelse i henhold til stk. 6, i fravær af passende kontraktlige ordninger, der tager sigte på at imødegå sådanne risici.

5. De kompetente myndigheder kan efter at have modtaget rapporterne omhandlet i artikel 35, stk. 1, litra c), og inden de træffer en afgørelse som omhandlet i nærværende artikels stk. 6, på frivillig basis høre de kompetente myndigheder, der er udpeget eller oprettet overensstemmelse med direktiv (EU) 2022/2555, som har ansvar for tilsynet med en væsentlig eller vigtig enhed opført, der er omfattet af nævnte direktiv og er blevet udpeget som en kritisk tredjepartsudbyder af IKT-tjenester.

6. De kompetente myndigheder kan, som en sidste udvej, efter underretningen og eventuelt høringen som fastsat i nærværende artikels stk. 4 og 5, i henhold til artikel 50 træffe en afgørelse, der kræver, at finansielle enheder midlertidigt, enten helt eller delvist, suspenderer anvendelsen eller udrulningen af en tjeneste, som den kritiske tredjepartsudbyder af IKT-tjenester leverer, indtil de risici, der er identificeret i de henstillinger, der er fremsat over for de kritiske tredjepartsudbydere af IKT-tjenester, er blevet imødegået. De kan om nødvendigt kræve, at finansielle enheder helt eller delvist opsiger de relevante kontraktlige ordninger, der er indgået med de kritiske tredjepartsudbydere af IKT-tjenester.

7. Hvis en kritisk tredjepartsudbyder af IKT-tjenester på grundlag af en tilgang, der divergerer fra den, som den ledende tilsynsførende anbefaler, nægter at tilslutte sig henstillinger, og en sådan divergerende tilgang kan have negativ indvirkning på et stort antal finansielle enheder eller en betydelig del af den finansielle sektor, og individuelle advarsler fra de kompetente myndigheder ikke har resulteret i konsekvente tilgange, der afbøder den potentielle risiko for den finansielle stabilitet, kan den ledende tilsynsførende efter at have hørt tilsynsforummet afgive ikkebindende og ikkeoffentlige udtalelser til de kompetente myndigheder for at fremme konsekvente og konvergerende tilsynsmæssige opfølgningsforanstaltninger, alt efter hvad der er relevant.

8. Efter at have modtaget rapporterne omhandlet i artikel 35, stk. 1, litra c), tager de kompetente myndigheder, når de træffer en afgørelse som omhandlet i nærværende artikels stk. 6, hensyn til typen og omfanget af den risiko, som ikke imødegås af den kritiske tredjepartsudbyder af IKT-tjenester, samt alvoren af den manglende overholdelse, under hensyntagen til følgende kriterier:

a) den manglende overholdelses grovhed og varighed

b) hvorvidt den manglende overholdelse har afsløret alvorlige svagheder i de procedurer, de forvaltningssystemer, den risikostyring og de interne kontroller, som den kritiske tredjepartsudbyder af IKT-tjenester varetager

c) om en økonomisk forbrydelse er blevet fremmet eller foranlediget af eller på anden måde kan tilskrives den manglende overholdelse

d) hvorvidt den manglende overholdelse er forsætlig eller skyldes uagtsomhed

e) hvorvidt suspensionen eller opsigelsen af de kontraktlige ordninger skaber en risiko for kontinuiteten af den finansielle enheds forretningsaktiviteter, uanset den finansielle enheds bestræbelser på at undgå afbrydelser af leveringen af dens tjenester

f) når det er relevant, den udtalelse, som på frivillig basis i overensstemmelse med denne artikels stk. 5 er indhentet fra de kompetente myndigheder, der er udpeget eller oprettet i overensstemmelse med direktiv (EU) 2022/2555, og som har ansvar for tilsynet med en væsentlig eller vigtig enhed, der er omfattet af nævnte direktiv og er blevet udpeget som en kritisk tredjepartsudbyder af IKT-tjenester.

De kompetente myndigheder giver de finansielle enheder den nødvendige tid for dem til at tilpasse de kontraktlige ordninger med kritiske tredjepartsudbydere af IKT-tjenester for at undgå skadelige virkninger for deres digitale operationelle modstandsdygtighed og for dem til at indføre exitstrategier og overgangsplaner som omhandlet i artikel 28.

9. Den afgørelse, der er omhandlet i denne artikels stk. 6, meddeles medlemmerne af tilsynsforummet, jf. artikel 32, stk. 4, litra a), b) og c), og det fælles tilsynsnetværk.

De kritiske tredjepartsudbydere af IKT-tjenester, der er berørt af de i stk. 6 omhandlede afgørelser, samarbejder fuldt ud med de påvirkede finansielle enheder, navnlig i forbindelse med suspension eller opsigelse af deres kontraktlige ordninger.

10. De kompetente myndigheder orienterer regelmæssigt den ledende tilsynsførende om de tilgange og foranstaltninger, de har iværksat i forbindelse med deres tilsynsopgaver vedrørende finansielle enheder, samt om de kontraktlige ordninger, som de finansielle enheder har indgået, når kritiske tredjepartsudbydere af IKT-tjenester kun delvist eller slet ikke har tilsluttet sig de henstillinger, som den ledende tilsynsførende har fremsat over for dem.

11. Den ledende tilsynsførende kan efter anmodning fremkomme med yderligere præciseringer vedrørende de udstedte henstillinger for at vejlede de kompetente myndigheder om opfølgningsforanstaltningerne.

Artikel 43

Tilsynsgebyrer

1. Den ledende tilsynsførende opkræver i overensstemmelse med den delegerede retsakt, der er omhandlet i denne artikels stk. 2, gebyrer hos kritiske tredjepartsudbydere af IKT-tjenester, som fuldt ud dækker den ledende tilsynsførendes nødvendige udgifter i forbindelse med varetagelsen af tilsynsopgaver i henhold til denne forordning, herunder godtgørelse af eventuelle omkostninger, der kan opstå som følge af det arbejde, der udføres af det fælles undersøgelsesteam, som er omhandlet i artikel 40, samt omkostningerne til rådgivning ydet af de uafhængige eksperter som omhandlet i artikel 32, stk. 4, andet afsnit, i forbindelse med forhold, der hører under området for de direkte tilsynsaktiviteter.

Det gebyrbeløb, der opkræves hos en kritisk tredjepartsudbyder af IKT-tjenester, skal dække alle omkostninger, der opstår som følge af udførelsen af de i denne afdeling fastsatte opgaver, og skal stå i et rimeligt forhold til dennes omsætning.

2. Kommissionen tillægges beføjelser til at vedtage en delegeret retsakt i overensstemmelse med artikel 57 for at supplere denne forordning ved at fastsætte gebyrbeløbene og den måde, hvorpå de skal betales, senest den 17. juli 2024.

Artikel 44

Internationalt samarbejde

1. Med forbehold af artikel 36 kan EBA, ESMA og EIOPA i overensstemmelse med artikel 33 i henholdsvis forordning (EU) nr. 1093/2010, (EU) nr. 1095/2010 og (EU) nr. 1094/2010 indgå administrative ordninger med tredjelandes regulerings- og tilsynsmyndigheder for at fremme det internationale samarbejde om IKT-tredjepartsrisiko på tværs af forskellige finansielle sektorer, navnlig ved at udvikle bedste praksis for gennemgang af praksis og kontroller forbundet med IKT-risikostyring, afhjælpende foranstaltninger og indsatsen i forbindelse med hændelser.

2. ESA'erne forelægger hvert femte år via Det Fælles Udvalg en fælles fortrolig rapport for Europa-Parlamentet, Rådet og Kommissionen med en sammenfatning af resultaterne af de relevante drøftelser, der er ført med de i stk. 1 omhandlede tredjelandsmyndigheder, med fokus på udviklingen inden for IKT-tredjepartsrisiko og konsekvenserne for den finansielle stabilitet, markedets integritet, investorbeskyttelsen og det indre markeds funktionsmåde.

KAPITEL VI

Ordninger for informationsudveksling

Artikel 45

Ordninger for informationsudveksling af oplysninger og efterretninger om cybertrusler

1. De finansielle enheder kan indbyrdes udveksle oplysninger og efterretninger om cybertrusler, herunder kompromitteringsindikatorer, taktikker, teknikker og procedurer, cybersikkerhedsvarsler og konfigurationsværktøjer, i det omfang en sådan udveksling af oplysninger og efterretninger:

a) har til formål at forbedre finansielle enheders digitale operationelle modstandsdygtighed, navnlig ved at øge bevidstheden om cybertrusler, begrænse eller hindre cybertruslernes spredningsevne, understøtte forsvarskapaciteter, teknikker til detektion af trusler, strategier for afbødning eller indsats- og genopretningsfaser

b) finder sted inden for betroede fællesskaber af finansielle enheder

c) gennemføres gennem ordninger for informationsudveksling, der beskytter de udvekslede oplysningers potentielt sensitive karakter, og som er omfattet af adfærdsregler med fuld respekt for forretningshemmeligheder, beskyttelse af personoplysninger i overensstemmelse med forordning (EU) 2016/679 og retningslinjer for konkurrencepolitikken.

2. Med henblik på stk. 1, litra c), fastlægger ordningerne for informationsudveksling betingelserne for deltagelse og fastsætter, hvor det er relevant, de nærmere bestemmelser om inddragelse af offentlige myndigheder og om den egenskab, i hvilken de kan indgå i ordninger for informationsudveksling, om inddragelse af tredjepartsudbydere af IKT-tjenester og om operationelle elementer, herunder anvendelsen af særlige IT-platforme.

3. De finansielle enheder underretter de kompetente myndigheder om deres deltagelse i de i stk. 1 omhandlede ordninger for informationsudveksling efter validering af deres medlemskab eller, alt efter hvad der er relevant, ophør af deres medlemskab, når det træder i kraft.

KAPITEL VII

Kompetente myndigheder

Artikel 46

Kompetente myndigheder

Uden at dette berører bestemmelserne i denne forordnings kapitel V, afdeling II, om tilsynsrammen for kritiske tredjepart-sudbydere af IKT-tjenester, sikrer følgende kompetente myndigheder overholdelse af denne forordning, i overensstemmelse med de beføjelser, som tillægges dem ved de respektive retsakter:

a) for kreditinstitutter og for institutter, der er fritaget i henhold til direktiv 2013/36/EU: den kompetente myndighed, der er udpeget i henhold til nævnte direktivs artikel 4, og for kreditinstitutter, der er klassificeret som signifikante i henhold til artikel 6, stk. 4, i forordning (EU) nr. 1024/2013: ECB i overensstemmelse med de ved nævnte forordning tillagte beføjelser og opgaver

b) for betalingsinstitutter, herunder betalingsinstitutter, der er undtaget i henhold til direktiv (EU) 2015/2366, e-pengeinstitutter, herunder dem, der er undtaget i henhold til direktiv 2009/110/EF, og kontooplysningstjene-steudbydere som omhandlet i artikel 33, stk. 1, i direktiv (EU) 2015/2366: den kompetente myndighed, der er udpeget i henhold til artikel 22 i direktiv (EU) 2015/2366

c) for investeringsselskaber: den kompetente myndighed, der er udpeget i henhold til artikel 4 i Europa-Parlamentets og Rådets direktiv (EU) 2019/2034 ([38])

d) for udbydere af kryptoaktivtjenester, der er meddelt tilladelse i henhold til forordningen om markeder for kryptoaktiver, og udstedere af aktivbaserede tokens: den kompetente myndighed, der er udpeget i overensstemmelse med den relevante bestemmelse i nævnte forordning

e) for værdipapircentraler: den kompetente myndighed, der er udpeget i henhold til artikel 11 i forordning (EU) nr. 909/2014

f) for centrale modparter: den kompetente myndighed, der er udpeget i henhold til artikel 22 i forordning (EU) nr. 648/2012

g) for markedspladser og udbydere af dataindberetningstjenester: den kompetente myndighed, der er udpeget i henhold til artikel 67 i direktiv 2014/65/EU, og den kompetente myndighed som defineret i artikel 2, stk. 1, nr. 18), i forordning (EU) nr. 600/2014

h) for transaktionsregistre: den kompetente myndighed, der er udpeget i henhold til artikel 22 i forordning (EU) nr. 648/2012

i) for forvaltere af alternative investeringsfonde: den kompetente myndighed, der er udpeget i henhold til artikel 44 i direktiv 2011/61/EU

j) for administrationsselskaber: den kompetente myndighed, der er udpeget i henhold til artikel 97 i direktiv 2009/65/EF

k) for forsikrings- og genforsikringsselskaber: den kompetente myndighed, der er udpeget i henhold til artikel 30 i direktiv 2009/138/EF

l) for forsikringsformidlere, genforsikringsformidlere og accessoriske forsikringsformidlere: den kompetente myndighed, der er udpeget i henhold til artikel 12 i direktiv (EU) 2016/97

m) for arbejdsmarkedsrelaterede pensionskasser: den kompetente myndighed, der er udpeget i henhold til artikel 47 i direktiv (EU) 2016/2341

n) for kreditvurderingsbureauer: den kompetente myndighed, der er udpeget i henhold til artikel 21 i forordning (EF) nr. 1060/2009

o) for administratorer af kritiske benchmarks: den kompetente myndighed, der er udpeget i henhold til artikel 40 og 41 i forordning (EU) 2016/1011

([38]) Europa-Parlamentets og Rådets direktiv (EU) 2019/2034 af 27. november 2019 om tilsyn med investeringsselskaber og om ændring af direktiv 2002/87/EF, 2009/65/EF, 2011/61/EU, 2013/36/EU, 2014/59/EU og 2014/65/EU (EUT L 314 af 5.12.2019, s. 64).

p) for udbydere af crowdfundingtjenester: den kompetente myndighed, der er udpeget i henhold til artikel 29 i forordning (EU) 2020/1503

q) for securitiseringsregistre: den kompetente myndighed, der er udpeget i henhold til artikel 10 og artikel 14, stk. 1, i forordning (EU) 2017/2402.

Artikel 47

Samarbejde med strukturer og myndigheder, der er oprettet ved direktiv (EU) 2022/2555

1. For at fremme samarbejde og muliggøre tilsynsmæssig udveksling mellem de kompetente myndigheder, der er udpeget i henhold til denne forordning, og den samarbejdsgruppe, der er nedsat ved artikel 14 i direktiv (EU) 2022/2555, kan ESA'erne og de kompetente myndigheder deltage i samarbejdsgruppens aktiviteter for så vidt angår spørgsmål, der vedrører deres tilsynsaktiviteter i forbindelse med finansielle enheder. ESA'erne og de kompetente myndigheder kan anmode om at blive indbudt til at deltage i samarbejdsgruppens aktiviteter for så vidt angår spørgsmål i forbindelse med væsentlige eller vigtige enheder, der er omfattet af direktiv (EU) 2022/2555 og desuden er blevet udpeget som kritiske tredjepartsudbydere af IKT-tjenester i henhold til denne forordnings artikel 31.

2. Hvis det er relevant, kan de kompetente myndigheder rådføre sig og dele oplysninger med henholdsvis de centrale kontaktpunkter og de CSIRT'er, der er udpeget eller oprettet i overensstemmelse med direktiv (EU) 2022/2555.

3. Hvis det er relevant, kan de kompetente myndigheder anmode om relevant teknisk rådgivning og bistand fra de kompetente myndigheder, der er udpeget eller oprettet i overensstemmelse med direktiv (EU) 2022/2555, og etablere samarbejdsordninger, således at der kan oprettes effektive og hurtige koordineringsmekanismer.

4. De ordninger, der er omhandlet i denne artikels stk. 3, kan bl.a. præcisere procedurerne for koordinering af tilsynsaktiviteter i forbindelse med væsentlige eller vigtige enheder, der er omfattet af direktiv (EU) 2022/2555 og er udpeget som kritiske tredjepartsudbydere af IKT-tjenester i henhold til denne forordnings artikel 31, herunder med henblik på i overensstemmelse med national ret at gennemføre undersøgelser og inspektioner på stedet samt med henblik på mekanismer til udveksling af oplysninger mellem de kompetente myndigheder i henhold til denne forordning og de kompetente myndigheder, der er udpeget eller oprettet i overensstemmelse med nævnte direktiv, hvilket omfatter adgang til oplysninger, som sidstnævnte myndigheder har anmodet om.

Artikel 48

Samarbejde mellem myndigheder

1. De kompetente myndigheder arbejder tæt sammen indbyrdes og, hvis det er relevant, med den ledende tilsynsførende.

2. De kompetente myndigheder og den ledende tilsynsførende udveksler rettidigt alle de relevante oplysninger om kritiske tredjepartsudbydere af IKT-tjenester, som er nødvendige for, at de kan udføre deres respektive opgaver i henhold til denne forordning, navnlig i forbindelse med identificerede risici, tilgange og foranstaltninger, der træffes som led i den ledende tilsynsførendes tilsynsopgaver.

Artikel 49

Simuleringsøvelser på tværs af sektorer, kommunikation og samarbejde inden for finans

1. ESA'erne kan via Det Fælles Udvalg og i samarbejde med de kompetente myndigheder, afviklingsmyndigheder som omhandlet i artikel 3 i direktiv 2014/59/EU, ECB, Den Fælles Afviklingsinstans for så vidt angår oplysninger vedrørende enheder, der er omfattet af anvendelsesområdet for forordning (EU) nr. 806/2014, ESRB og ENISA, alt efter hvad der er relevant, indføre mekanismer, der gør det muligt at udveksle effektive fremgangsmåder på tværs af finansielle sektorer for at forbedre situationskendskabet og identificere fælles cybersårbarheder og risici på tværs af sektorer.

De kan udvikle simuleringsøvelser for krisestyring og beredskab, der omfatter cyberangrebsscenarier, med henblik på at udvikle kommunikationskanaler og gradvist muliggøre en effektiv koordineret indsats på EU-plan i tilfælde af en større grænseoverskridende IKT-relateret hændelse eller dermed forbundet trussel, som har systemiske virkninger for Unionens finansielle sektor som helhed.

Simuleringsøvelserne kan, alt efter hvad der er relevant, også tjene til at teste den finansielle sektors afhængighed af andre økonomiske sektorer.

2. De kompetente myndigheder, ESA'erne og ECB samarbejder tæt med hinanden og udveksler oplysninger med henblik på at varetage deres opgaver i henhold til artikel 47-54. De koordinerer deres tilsyn tæt for at identificere og afhjælpe overtrædelser af denne forordning, udvikle og fremme bedste praksis, lette samarbejdet, fremme en konsekvent fortolkning og tilvejebringe vurderinger på tværs af jurisdiktioner i tilfælde af eventuelle tvister.

Artikel 50

Administrative sanktioner og afhjælpende foranstaltninger

1. De kompetente myndigheder tillægges alle de nødvendige tilsynsmæssige beføjelser, undersøgelses- og sanktionsbeføjelser, således at de kan opfylde deres forpligtelser i henhold til denne forordning.

2. De i stk. 1 omhandlede beføjelser skal mindst omfatte følgende beføjelser til at:

a) have adgang til ethvert dokument eller data i enhver form, som den kompetente myndighed anser for relevante for varetagelsen af sine opgaver, og modtage eller tage en kopi deraf

b) gennemføre inspektioner eller undersøgelser på stedet, som omfatter, men ikke er begrænset til:

   i) at indkalde repræsentanter for de finansielle enheder med henblik på mundtlige eller skriftlige redegørelser for forhold eller dokumenter, der vedrører undersøgelsens genstand og formål, og at optage svarene

   ii) at udspørge enhver anden fysisk eller juridisk person, der indvilliger heri, med det formål at indsamle oplysninger om undersøgelsens genstand

c) kræve korrigerende og afhjælpende foranstaltninger for overtrædelser af kravene i denne forordning.

3. Uden at dette berører medlemsstaternes ret til at pålægge strafferetlige sanktioner i overensstemmelse med artikel 52, fastsætter medlemsstaterne bestemmelser om passende administrative sanktioner og afhjælpende foranstaltninger for overtrædelser af denne forordning og sikrer en effektiv gennemførelse heraf.

Disse sanktioner eller foranstaltninger skal være effektive, stå i rimeligt forhold til overtrædelsen og have afskrækkende virkning.

4. Medlemsstaterne tillægger de kompetente myndigheder beføjelse til at anvende mindst følgende administrative sanktioner eller afhjælpende foranstaltninger for overtrædelser af denne forordning:

a) at udstede et påbud om, at den fysiske eller juridiske person bringer den adfærd, der udgør en overtrædelse af denne forordning, til ophør og afholder sig fra at gentage en sådan adfærd

b) at kræve midlertidigt eller permanent ophør med en praksis eller adfærd, som den kompetente myndighed anser for at stride mod bestemmelserne i denne forordning, og forhindre, at en sådan praksis eller adfærd gentager sig

c) at træffe enhver form for foranstaltning, herunder af pekuniær karakter, for at sikre, at de finansielle enheder fortsat overholder de retlige krav

d) i det omfang national ret tillader det, at kræve udlevering af eksisterende optegnelser over datatrafik, som en telekommunikationsoperatør er i besiddelse af, når der foreligger en rimelig mistanke om en overtrædelse af denne forordning, og når sådanne optegnelser kan være relevante for en undersøgelse af overtrædelser af denne forordning og

e) at udsende offentlige meddelelser, herunder offentlige erklæringer, der angiver den fysiske eller juridiske persons identitet og overtrædelsens art.

5. Såfremt stk. 2, litra c), og stk. 4, finder anvendelse på juridiske personer, giver medlemsstaterne de kompetente myndigheder beføjelse til i overensstemmelse med betingelserne i national ret at anvende de administrative sanktioner og afhjælpende foranstaltninger på medlemmer af ledelsesorganet samt andre personer, som i henhold til national ret er ansvarlige for overtrædelsen.

6. Medlemsstaterne sikrer, at enhver afgørelse om pålæggelse af administrative sanktioner eller afhjælpende foranstaltninger som omhandlet i stk. 2, litra c), er behørigt begrundet og kan påklages.

Artikel 51

Udøvelse af beføjelsen til at pålægge administrative sanktioner og afhjælpende foranstaltninger

1. De kompetente myndigheder udøver, hvis det er relevant, beføjelsen til at pålægge de administrative sanktioner og afhjælpende foranstaltninger, der er omhandlet i artikel 50, i overensstemmelse med deres nationale lovrammer på følgende måde:

a) direkte

b) i samarbejde med andre myndigheder

c) under eget ansvar ved delegation til andre myndigheder eller

d) ved anmodning til de kompetente judicielle myndigheder.

2. De kompetente myndigheder tager ved valget af arten af og niveauet for en administrativ sanktion eller afhjælpende foranstaltning, der pålægges i henhold til artikel 50, hensyn til, i hvilken grad overtrædelsen er forsætlig eller skyldes uagtsomhed, og alle andre relevante omstændigheder, herunder følgende, hvis det er relevant:

a) overtrædelsens væsentlighed, grovhed og varighed

b) graden af ansvar hos den fysiske eller juridiske person, der er ansvarlig for overtrædelsen

c) den ansvarlige fysiske eller juridiske persons finansielle styrke

d) omfanget af den ansvarlige fysiske eller juridiske persons opnåede fortjeneste eller undgåede tab, såfremt disse beløb kan beregnes

e) de tab for tredjeparter, som skyldes overtrædelsen, såfremt disse beløb kan beregnes

f) i hvilken grad den fysiske eller juridiske person samarbejder med den kompetente myndighed, uden at det dog berører kravet om tilbagebetaling af den pågældende fysiske eller juridiske persons opnåede fortjeneste eller undgåede tab

g) overtrædelser, som den ansvarlige fysiske eller juridiske person tidligere har begået.

Artikel 52

Strafferetlige sanktioner

1. Medlemsstaterne kan beslutte ikke at fastsætte bestemmelser om administrative sanktioner eller afhjælpende foranstaltninger for overtrædelser, der er omfattet af strafferetlige sanktioner i henhold til national ret.

2. Hvis medlemsstaterne har valgt at fastsætte strafferetlige sanktioner for overtrædelser af denne forordning, sikrer de, at der er truffet passende foranstaltninger, således at de kompetente myndigheder har alle de nødvendige beføjelser til at holde kontakt til de judicielle, retsforfølgende eller strafferetlige myndigheder inden for deres jurisdiktion for at indhente specifikke oplysninger om strafferetlige efterforskninger eller straffesager, der er indledt for overtrædelser af denne forordning, og til at give andre kompetente myndigheder samt EBA, ESMA eller EIOPA de samme oplysninger, således at disse kan opfylde deres forpligtelser til at samarbejde med henblik på anvendelsen af denne forordning.

Artikel 53

Meddelelsespligt

Medlemsstaterne giver senest den 17. januar 2025 Kommissionen, ESMA, EBA, og EIOPA meddelelse om de love og administrative bestemmelser, herunder relevante strafferetlige bestemmelser, som gennemfører dette kapitel. Medlemsstaterne meddeler uden unødigt ophold Kommissionen, ESMA, EBA, og EIOPA eventuelle senere ændringer heraf.

Artikel 54

Offentliggørelse af administrative sanktioner

1. De kompetente myndigheder offentliggør uden unødigt ophold på deres officielle websteder enhver afgørelse om pålæggelse af en administrativ sanktion, som ikke kan påklages, efter at modtageren af sanktionen er blevet underrettet om afgørelsen.

2. Den i stk. 1 omhandlede offentliggørelse omfatter oplysninger om overtrædelsens type og art, de ansvarlige personers identitet samt de pålagte sanktioner.

3. Hvis den kompetente myndighed efter en vurdering i det enkelte tilfælde finder, at offentliggørelse af identiteten, hvis der er tale om juridiske personer, eller af identiteten og personoplysninger, hvis der er tale om fysiske personer, vil være uforholdsmæssig, herunder omfatte risici i forbindelse med beskyttelsen af personoplysninger, vil bringe de finansielle markeders stabilitet eller gennemførelsen af en igangværende strafferetlig efterforskning i fare eller, i det omfang skaden kan fastslås, vil forvolde uforholdsmæssig stor skade på den involverede person, tager den en af følgende løsninger i anvendelse med hensyn til afgørelsen om at pålægge en administrativ sanktion:

a) udsætte offentliggørelsen heraf, indtil enhver begrundelse for at undlade offentliggørelse er bortfaldet

b) offentliggøre den anonymt i overensstemmelse med national ret eller

c) undlade at offentliggøre den, hvis mulighederne i litra a) og b) enten anses for at være utilstrækkelige til at sikre, at de finansielle markeders stabilitet ikke på nogen måde bringes i fare, eller hvis en sådan offentliggørelse ikke står i et rimeligt forhold til den pålagte sanktions mildhed.

4. I tilfælde af en afgørelse om at offentliggøre en administrativ sanktion anonymt i overensstemmelse med stk. 3, litra b), kan offentliggørelsen af de relevante oplysninger udskydes.

5. Hvis en kompetent myndighed offentliggør en afgørelse om at pålægge en administrativ sanktion, der kan indbringes for de relevante judicielle myndigheder, lægger de kompetente myndigheder straks denne oplysning på deres officielle websted sammen med eventuelle efterfølgende oplysninger om resultatet af denne indbringelse på et senere tidspunkt. En judiciel afgørelse, som annullerer en afgørelse om at pålægge en administrativ sanktion, skal også offentliggøres.

6. Kompetente myndigheder sikrer, at enhver offentliggørelse som omhandlet i stk. 1-4 kun er tilgængelig på deres officielle websted i den periode, der er nødvendig af hensyn til denne artikel. Denne periode må ikke overstige fem år efter offentliggørelsen.

Artikel 55

Tavshedspligt

1. Enhver fortrolig oplysning, der modtages, udveksles eller videregives i henhold til denne forordning, er underlagt de i stk. 2 omhandlede betingelser vedrørende tavshedspligt.

2. Tavshedspligten gælder for alle personer, der arbejder eller har arbejdet for de kompetente myndigheder i henhold til denne forordning eller for en myndighed, en markedsdeltager eller en fysisk eller juridisk person, som disse kompetente myndigheder har overdraget sine beføjelser til, herunder revisorer og sagkyndige, der har indgået en kontrakt med disse.

3. Oplysninger, der er omfattet af tavshedspligt, herunder udveksling af oplysninger mellem kompetente myndigheder i henhold til denne forordning og kompetente myndigheder, der er udpeget eller oprettet i overensstemmelse med direktiv (EU) 2022/2555, må ikke videregives til nogen anden person eller myndighed, medmindre der er hjemmel dertil i bestemmelser fastsat i EU-ret eller national ret;

4. Alle oplysninger, der udveksles mellem de kompetente myndigheder i henhold til denne forordning, og som vedrører forretnings- eller driftsmæssige betingelser og andre økonomiske eller personlige anliggender, betragtes som fortrolige og er underlagt krav om tavshedspligt, undtagen når den kompetente myndighed på det tidspunkt, hvor oplysningerne blev meddelt, har erklæret, at disse oplysninger kan videregives, eller når videregivelse er nødvendig i forbindelse med en eventuel retsforfølgning.

Artikel 56

Databeskyttelse

1. ESA'erne og de kompetente myndigheder må kun behandle personoplysninger, hvis det er nødvendigt for, at de kan opfylde deres respektive forpligtelser og udføre deres opgaver i henhold til denne forordning, navnlig med hensyn til undersøgelse, inspektion, anmodning om oplysninger, kommunikation, offentliggørelse, evaluering, efterprøvning, vurdering og udarbejdelse af tilsynsplaner. Personoplysninger behandles i overensstemmelse med forordning (EU) 2016/679 eller (EU) 2018/1725, alt efter hvilken der finder anvendelse.

2. Medmindre andet er fastsat i andre sektorspecifikke retsakter, opbevares de personoplysninger, der er omhandlet i stk. 1, indtil de relevante tilsynsopgaver er udført, og under alle omstændigheder i en periode på højst 15 år, undtagen i tilfælde af verserende retssager, der kræver yderligere opbevaring af sådanne oplysninger.

KAPITEL VIII

Delegerede retsakter

Artikel 57

Udøvelse af de delegerede beføjelser

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

2. Beføjelsen til at vedtage delegerede retsakter, jf. artikel 31, stk. 6, og artikel 43, stk. 2, tillægges Kommissionen for en periode på fem år fra den 17. januar 2024. Kommissionen udarbejder en rapport vedrørende delegationen af beføjelser senest ni måneder inden udløbet af femårsperioden. Delegationen af beføjelser forlænges stiltiende for perioder af samme varighed, medmindre Europa-Parlamentet eller Rådet modsætter sig en sådan forlængelse senest tre måneder inden udløbet af hver periode.

3. Den i artikel 31, stk. 6, og artikel 43, stk. 2, omhandlede delegation af beføjelser kan til enhver tid tilbagekaldes af Europa-Parlamentet eller Rådet. En afgørelse om tilbagekaldelse bringer delegationen af de beføjelser, der er angivet i den pågældende afgørelse, til ophør. Den får virkning dagen efter offentliggørelsen af afgørelsen i *Den Europæiske Unions Tidende* eller på et senere tidspunkt, der angives i afgørelsen. Den berører ikke gyldigheden af delegerede retsakter, der allerede er i kraft.

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

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

6. En delegeret retsakt vedtaget i henhold til artikel 31, stk. 6, og artikel 43, stk. 2, træder kun i kraft, hvis hverken Europa-Parlamentet eller Rådet har gjort indsigelse inden for en frist på tre måneder fra meddelelsen af den pågældende retsakt til Europa-Parlamentet og Rådet, eller hvis Europa-Parlamentet og Rådet inden udløbet af denne frist begge har underrettet Kommissionen om, at de ikke agter at gøre indsigelse. Fristen forlænges med tre måneder på Europa-Parlamentets eller Rådets initiativ.

KAPITEL IX

Overgangsbestemmelser og afsluttende bestemmelser

Afdeling I

Artikel 58

Revisionsklausul

1. Senest den 17. januar 2028 foretager Kommissionen efter høring af ESA'erne og ESRB, alt efter hvad der er relevant, en gennemgang og forelægger en rapport for Europa-Parlamentet og Rådet, eventuelt ledsaget af et lovgivningsmæssigt forslag. Gennemgangen skal som minimum omfatte følgende:

a) kriterierne for udpegelse af kritiske tredjepartsudbydere af IKT-tjenester i overensstemmelse med artikel 31, stk. 2

b) den frivillige karakter af underretningen om væsentlige cybertrusler, der er omhandlet i artikel 19

c) den ordning, der er omhandlet i artikel 31, stk. 12, og de beføjelser, som tillægges den ledende tilsynsførende, som er fastsat i artikel 35, stk. 1, litra d), nr. iv), første led, med henblik på at evaluere nævnte bestemmelsers effektivitet med hensyn til at sikre effektivt tilsyn med kritiske tredjepartsudbydere af IKT-tjenester med hjemsted i et tredjeland og nødvendigheden af at etablere en dattervirksomhed i Unionen.

   Med henblik på dette litras første afsnit skal gennemgangen indeholde en analyse af den ordning, der er omhandlet i artikel 31, stk. 12, herunder for så vidt angår adgang for Unionens finansielle enheder til tjenester fra tredjelande og tilgængeligheden af sådanne tjenester på Unionens marked, og den skal tage hensyn til den yderligere udvikling på markederne for tjenester, der er omfattet af denne forordning, de finansielle enheders og de finansielle tilsynsmyndigheders praktiske erfaring med hensyn til henholdsvis brugen af og tilsynet med nævnte ordning og enhver relevant reguleringsmæssig og tilsynsmæssig udvikling, der finder sted på internationalt plan.

d) det hensigtsmæssige i at lade de finansielle enheder, der er omhandlet i artikel 2, stk. 3, litra e), og som gør brug af automatiske salgssystemer, være omfattet af denne forordnings anvendelsesområde i lyset af den fremtidige markedsudvikling i brugen af sådanne systemer

e) det fælles tilsynsnetværks funktion og effektivitet med hensyn til at støtte tilsynets konsekvens og informationsudvekslingens effektivitet inden for tilsynsrammen.

2. I forbindelse med revisionen af direktiv (EU) 2015/2366 vurderer Kommissionen behovet for øget cyberrobusthed i betalingssystemer og betalingsbehandlingsaktiviteter og hensigtsmæssigheden af at udvide denne forordnings anvendelsesområde til operatører af betalingssystemer og enheder, der er involveret i betalingsbehandlingsaktiviteter. I lyset af denne vurdering forelægger Kommissionen som led i revisionen af direktiv (EU) 2015/2366 en rapport for Europa-Parlamentet og Rådet senest den 17. juli 2023.

På grundlag af denne revisionsrapport og efter høring af ESA'erne, ECB og ESRB kan Kommissionen, hvor det er relevant og som led i det lovgivningsmæssige forslag, som den kan vedtage i henhold til artikel 108, stk. 2, i direktiv (EU) 2015/2366, forelægge et forslag, der sikrer, at alle operatører af betalingssystemer og enheder, der er involveret i betalingsbehandlingsaktiviteter, er omfattet af passende tilsyn, samtidig med at der tages hensyn til centralbankens eksisterende tilsyn.

3. Senest den 17. januar 2026 foretager Kommissionen efter høring af ESA'erne og Udvalget af Europæiske Revisionstilsynsmyndigheder en gennemgang og forelægger en rapport for Europa-Parlamentet og Rådet, eventuelt ledsaget af et lovgivningsmæssigt forslag vedrørende det hensigtsmæssige i skærpede krav til lovpligtige revisorer og revisionsfirmaer for så vidt angår digital operationel modstandsdygtighed ved at lade revisorer og revisionsfirmaer blive omfattet af denne forordnings anvendelsesområde eller gennem ændringer af Europa-Parlamentets og Rådets direktiv 2006/43/EF ([39]).

Afdeling II

Ændringer

Artikel 59

Ændringer af forordning (EF) nr. 1060/2009

I forordning (EF) nr. 1060/2009 foretages følgende ændringer:

1) Bilag I, afsnit A, punkt 4, første afsnit, affattes således:

»Et kreditvurderingsbureau skal have passende administrative og regnskabsmæssige procedurer, interne kontrolmekanismer, effektive procedurer til risikovurdering og effektive kontrol- og sikkerhedsforanstaltninger med henblik på styring af sine IKT-systemer i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) 2022/2554 (*).

(*) 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).«

2) Bilag III, punkt 12, affattes således:

»12. Kreditvurderingsbureauet overtræder artikel 6, stk. 2, sammenholdt med bilag I, afsnit A, punkt 4, ved at undlade at have passende administrative og regnskabsmæssige procedurer, interne kontrolmekanismer, effektive procedurer til risikovurdering og effektive kontrol- og sikkerhedsforanstaltninger med henblik på styring af sine IKT-systemer i overensstemmelse med forordning (EU) 2022/2554, eller ved at undlade at gennemføre eller opretholde beslutningsprocedurer eller organisatoriske strukturer som påkrævet i henhold til nævnte punkt.«

Artikel 60

Ændringer af forordning (EU) nr. 648/2012

I forordning (EU) nr. 648/2012 foretages følgende ændringer:

1) I artikel 26 foretages følgende ændringer:

a) Stk. 3 affattes således:

»3. En CCP opretholder og anvender en sådan organisatorisk struktur, som er nødvendig til at sikre kontinuitet og regelmæssighed i leveringen af dens tjenesteydelser og udøvelsen af dens aktiviteter. Den anvender med henblik herpå hensigtsmæssige og forholdsmæssigt afpassede systemer, ressourcer og procedurer, herunder IKT-systemer, som styres i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) 2022/2554 (*).

(*) 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).«

([39]) Europa-Parlamentets og Rådets direktiv 2006/43/EF af 17. maj 2006 om lovpligtig revision af årsregnskaber og konsoliderede regnskaber, om ændring af Rådets direktiv 78/660/EØF og 83/349/EØF og om ophævelse af Rådets direktiv 84/253/EØF (EUT L 157 af 9.6.2006, s. 87).

b) Stk. 6 udgår.

2) I artikel 34 foretages følgende ændringer:

a) Stk. 1 affattes således:

»1. En CCP udarbejder, gennemfører og opretholder en passende forretningskontinuitetsplan og en katastrofeberedskabsplan, som omfatter en politik for IKT-driftsstabilitet og planer for IKT-indsats og -genopretning, der indføres og gennemføres i overensstemmelse med forordning (EU) 2022/2554, og som har til formål at sikre opretholdelsen af dens funktioner, sikre rettidig genopretning af transaktioner og opfyldelse af CCP'ens forpligtelser.«

b) Stk. 3, første afsnit, affattes således:

»3. For at sikre ensartet anvendelse af denne artikel udarbejder ESMA efter høring af medlemmerne af ESCB udkast til reguleringsmæssige tekniske standarder, der præciserer de elementer og krav, som forretningskontinuitetspolitikken og katastrofeberedskabsplanen mindst skal indeholde, eksklusive en politik for IKT-driftsstabilitet og IKT-katastrofeberedskabsplaner.«

3) Artikel 56, stk. 3, første afsnit, affattes således:

»3. For at sikre den ensartede anvendelse af denne artikel udarbejder ESMA udkast til reguleringsmæssige tekniske standarder, som præciserer oplysningerne i ansøgningen om registrering, jf. stk. 1, dog ikke oplysningerne om krav til IKT-risikostyring.«

4) Artikel 79, stk. 1 og 2, affattes således:

»1. Et transaktionsregister skal identificere kilderne til operationelle risici og desuden reducere dem ved at udvikle passende systemer, kontroller og procedurer, herunder IKT-systemer, der styres i overensstemmelse med forordning (EU) 2022/2554.

2. Et transaktionsregister udarbejder, gennemfører og opretholder en hensigtsmæssig forretningskontinuitetsplan og en katastrofeberedskabsplan, herunder en politik for IKT-driftsstabilitet og planer for IKT-indsats og -genopretning udarbejdet i overensstemmelse med forordning (EU) 2022/2554, som har til formål at sikre opretholdelsen af registrets funktioner og sikre rettidig genopretning af transaktioner og opfyldelse af transaktionsregistrets forpligtelser.«

5) Artikel 80, stk. 1, udgår.

6) Bilag I, afsnit II, ændres således:

a) Litra a) og b) affattes således:

»a) et transaktionsregister overtræder bestemmelserne i artikel 79, stk. 1, ved at undlade at identificere kilder til operationelle risici eller ved at undlade at reducere disse risici ved at udvikle passende systemer, kontroller og procedurer, herunder IKT-systemer, der styres i overensstemmelse med forordning (EU) 2022/2554

b) et transaktionsregister overtræder bestemmelserne i artikel 79, stk. 2, ved at undlade at udarbejde, gennemføre eller opretholde en hensigtsmæssig forretningskontinuitetsplan og en katastrofeberedskabsplan udarbejdet i overensstemmelse med forordning (EU) 2022/2554, som har til formål at sikre opretholdelse af registrets funktioner, sikre rettidig genopretning af transaktioner og opfyldelse af transaktionsregistrets forpligtelser«.

b) Litra c) udgår.

7) Bilag III ændres således:

a) Afsnit II ændres således:

i) litra c) affattes således:

»c) en niveau 2-CCP overtræder artikel 26, stk. 3, ved at undlade at opretholde eller anvende en organisatorisk struktur, som sikrer kontinuitet og regelmæssighed i leveringen af dens tjenesteydelser og udøvelsen af dens aktiviteter, eller ved at undlade at anvende hensigtsmæssige og forholdsmæssigt afpassede systemer, ressourcer og procedurer, herunder IKT-systemer, der styres i overensstemmelse med forordning (EU) 2022/2554«.

ii) litra f) udgår.

b) Afsnit III, litra a), affattes således:

»a) en niveau 2-CCP overtræder artikel 34, stk. 1, ved at undlade at udarbejde, gennemføre eller opretholde en passende forretningskontinuitetsplan og en indsats- og genopretningsplan udarbejdet i overensstemmelse med forordning (EU) 2022/2554, som har til formål at sikre opretholdelsen af CCP'ens funktioner, sikre rettidig genopretning af alle transaktioner og opfyldelse af CCP'ens forpligtelser, og som mindst giver mulighed for at genoptage alle transaktioner fra det tidspunkt, hvor de blev afbrudt, for at give den pågældende CCP mulighed for at opretholde driftssikkerheden og gennemføre afvikling på den planlagte dato«.

Artikel 61

Ændringer af forordning (EU) nr. 909/2014

I artikel 45 i forordning (EU) nr. 909/2014 foretages følgende ændringer:

1) Stk. 1 affattes således:

»1. CSD'er skal identificere kilder til operationelle risici, både interne og eksterne, og ligeledes begrænse deres indvirkning ved at anvende passende IKT-værktøjer, kontroller og procedurer, som er oprettet og styres i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) 2022/2554 (*), samt ved anvende eventuelle andre relevante værktøjer, kontroller og procedurer for andre typer af operationelle risici, herunder for alle de værdipapirafviklingssystemer, som de driver.

(*) 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).«

2) Stk. 2 udgår.

3) Stk. 3 og 4 affattes således:

»3. CSD'er udarbejder, gennemfører og opretholder for tjenesteydelser, som de leverer, samt for hvert af de værdipapirafviklingssystemer, som de driver, en passende forretningskontinuitetspolitik og en katastrofeberedskabsplan, herunder en politik for IKT-driftsstabilitet og planer for IKT-indsats og -genopretning udarbejdet i overensstemmelse med forordning (EU) 2022/2554, som har til formål at sikre opretholdelsen af deres tjenesteydelser, rettidig genopretning af transaktioner og opfyldelse af deres forpligtelser i tilfælde af hændelser, som i høj grad risikerer at afbryde transaktioner.

4. Planerne i stk. 3 skal give mulighed for at genoptage alle transaktioner og deltageres positioner fra det tidspunkt, hvor de blev afbrudt, for at give deltagerne i en CSD mulighed for at opretholde driftssikkerheden og foretage afvikling på den planlagte dato, bl.a. ved at sikre, at kritiske IT-systemer kan genoptage driften fra det tidspunkt, hvor de blev afbrudt som fastsat i artikel 12, stk. 5 og 7, i forordning (EU) 2022/2554.«

4) Stk. 6 affattes således:

»6. CSD'er identificerer, overvåger og forvalter de risici, som de vigtigste deltagere i de værdipapirafviklingssystemer, de driver, samt serviceydere og andre CSD'er eller andre markedsinfrastrukturer kan indebære for deres transaktioner. De giver efter anmodning de kompetente og relevante myndigheder oplysninger om sådanne risici, der identificeres. De underretter også omgående den kompetente myndighed og relevante myndigheder om eventuelle operationelle hændelser som følge af sådanne risici, dog ikke om IKT-risikoen.«

5) Stk. 7, første afsnit, affattes således:

»7. ESMA udarbejder i tæt samarbejde med medlemmerne af ESCB udkast til reguleringsmæssige tekniske standarder med henblik på at præcisere de operationelle risici i stk. 1 og 6, dog ikke IKT-risikoen, og metoderne til at teste, håndtere eller begrænse de pågældende risici, herunder forretningskontinuitetspolitikkerne og katastrofeberedskabsplanerne i stk. 3 og 4 og metoderne til vurdering deraf.«

Artikel 62

Ændringer af forordning (EU) nr. 600/2014

I forordning (EU) nr. 600/2014 foretages følgende ændringer:

1) Artikel 27g ændres således:

a) Stk. 4 affattes således:

»4. En APA skal opfylde kravene til sikkerheden i net- og informationssystemer, der er fastsat i Europa-Parlamentets og Rådets forordning (EU) 2022/2554 (*).

(*) 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).«

b) Stk. 8, litra c), affattes således:

»c) de konkrete organisatoriske krav, der er fastsat i stk. 3 og 5.«

2) Artikel 27h ændres således:

a) Stk. 5 affattes således:

»5. En CTP skal opfylde kravene til sikkerheden i net- og informationssystemer, der er fastsat i forordning (EU) 2022/2554.«

b) Stk. 8, litra e), affattes således:

»e) de konkrete organisatoriske krav, der er fastsat i stk. 4.«

3) Artikel 27i ændres således:

a) Stk. 3 affattes således:

»3. En ARM skal opfylde kravene til sikkerheden i net- og informationssystemer, der er fastsat i forordning (EU) 2022/2554«

b) Stk. 5, litra b), affattes således:

»b) de konkrete organisatoriske krav, der er fastsat i stk. 2 og 4.«

Artikel 63

Ændring af forordning (EU) 2016/1011

I artikel 6 i forordning (EU) 2016/1011 tilføjes følgende stykke:

»6. For kritiske benchmarks skal en administrator have solide administrative og regnskabsmæssige procedurer, interne kontrolmekanismer, effektive procedurer til risikovurdering og effektive kontrol- og sikkerhedsforanstaltninger med henblik på styring af sine IKT-systemer i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) 2022/2554 (*).

(*) 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).«

Artikel 64

Ikrafttræden og anvendelse

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

Den finder anvendelse fra den 17. januar 2025.

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

Udfærdiget i Strasbourg, den 14. december 2022.

På Europa-Parlamentets vegne	*På Rådets vegne*
R. METSOLA	M. BEK
Formand	*Formand*

DIREKTIVER

EUROPA-PARLAMENTETS OG RÅDETS DIREKTIV (EU) 2022/2555

af 14. december 2022

om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen, om ændring af forordning (EU) nr. 910/2014 og direktiv (EU) 2018/1972 og om ophævelse af direktiv (EU) 2016/1148 (NIS 2-direktivet)

(EØS-relevant tekst)

EUROPA-PARLAMENTET OG RÅDET FOR DEN EUROPÆISKE UNION HAR —

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

under henvisning til forslag fra Europa-Kommissionen,

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

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

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

efter høring af Regionsudvalget,

efter den almindelige lovgivningsprocedure ([3]), og

ud fra følgende betragtninger:

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

(2) Siden ikrafttrædelsen af direktiv (EU) 2016/1148 er der gjort betydelige fremskridt med hensyn til at øge Unionens niveau af cyberrobusthed. Evalueringen af nævnte direktiv har vist, at det har fungeret som katalysator for den institutionelle og lovgivningsmæssige tilgang til cybersikkerhed i Unionen og har banet vejen for en betydelig holdningsændring. Nævnte direktiv har sikret færdiggørelsen af nationale rammer for sikkerheden i net- og informationssystemer ved at fastlægge nationale strategier for sikkerheden i net- og informationssystemer og etablere nationale kapaciteter og ved at gennemføre lovgivningsmæssige foranstaltninger, der omfatter væsentlige infrastrukturer og enheder, som hver medlemsstat har identificeret. Direktiv (EU) 2016/1148 har også bidraget til samarbejdet på EU-plan gennem oprettelsen af samarbejdsgruppen og netværket af nationale enheder, der håndterer IT-sikkerhedshændelser. Uanset disse resultater har evalueringen af direktiv (EU) 2016/1148 afsløret iboende mangler, der forhindrer det i effektivt at tackle aktuelle og nye cybersikkerhedsudfordringer.

(3) Net- og informationssystemer har udviklet sig til et centralt element i hverdagen med den hurtige digitale omstilling og forbundethed i samfundet, herunder i forbindelse med grænseoverskridende udvekslinger. Denne udvikling har ført til en udvidelse af antallet og typen af cybertrusler og skabt nye udfordringer, som kræver tilpassede, koordinerede og innovative svar i alle medlemsstater. Antallet, omfanget, den avancerede karakter, hyppigheden og virkningen af hændelser er stigende og udgør en alvorlig trussel mod net- og informationssystemernes funktion. Som følge heraf kan hændelser hindre udøvelsen af økonomiske aktiviteter i det indre marked, medføre

([1]) EUT C 233 af 16.6.2022, s. 22.
([2]) EUT C 286 af 16.7.2021, s. 170.
([3]) Europa-Parlamentets holdning af 10.11.2022 (endnu ikke offentliggjort i EUT) og Rådets afgørelse af 28.11.2022.
([4]) Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (EUT L 194 af 19.7.2016, s. 1).

økonomiske tab, underminere brugernes tillid og forårsage store skader på Unionens økonomi og samfund. Cybersikkerhedsberedskab og -effektivitet er derfor mere afgørende for et velfungerende indre marked end nogensinde før. Cybersikkerhed er desuden en vigtig katalysator for, at mange kritiske sektorer kan tage den digitale omstilling til sig med et positivt resultat og fuldt ud kan udnytte de økonomiske, sociale og bæredygtige fordele ved digitalisering.

(4) Retsgrundlaget for direktiv (EU) 2016/1148 var artikel 114 i traktaten om Den Europæiske Unions funktionsmåde (TEUF), hvis formål er det indre markeds oprettelse og funktion ved at styrke foranstaltninger til indbyrdes tilnærmelse af de nationale regler. De cybersikkerhedskrav, der pålægges enheder, som leverer tjenester eller som udfører aktiviteter, der er økonomisk betydningsfulde, varierer betydeligt fra medlemsstat til medlemsstat med hensyn til typen af krav, detaljeringsgrad og tilsynsmetode. Disse forskelle medfører yderligere omkostninger og skaber vanskeligheder for enheder, der udbyder varer eller tjenester på tværs af grænserne. Krav, der stilles af en medlemsstat, og som er forskellige fra eller endog i konflikt med dem, der er pålagt af en anden medlemsstat, kan påvirke sådanne grænseoverskridende aktiviteter i væsentlig grad. Desuden har muligheden for en utilstrækkelig udformning eller gennemførelse af cybersikkerhedskravene i én medlemsstat sandsynligvis konsekvenser for cybersikkerhedsniveauet i andre medlemsstater, navnlig i betragtning af intensiteten af grænseoverskridende udvekslinger. Evalueringen af direktiv (EU) 2016/1148 har vist, at der er store forskelle i medlemsstaternes gennemførelse af det, herunder med hensyn til dets anvendelsesområde, hvis afgrænsning i vid udstrækning blev overladt til medlemsstaternes skøn. Direktiv (EU) 2016/1148 gav også medlemsstaterne meget vide skønsbeføjelser med hensyn til gennemførelsen af de sikkerheds- og hændelsesrapporteringsforpligtelser, der er fastsat deri. Disse forpligtelser blev derfor gennemført på vidt forskellige måder på nationalt plan. Der er lignende forskelle i gennemførelsen af bestemmelserne i direktiv (EU) 2016/1148 om tilsyn og håndhævelse.

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

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

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

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

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

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

(9) Medlemsstaterne bør kunne træffe de nødvendige foranstaltninger for at sikre beskyttelsen af væsentlige nationale sikkerhedsinteresser, opretholde den offentlige orden og sikkerhed samt tillade forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger. Med henblik herpå bør medlemsstater kunne undtage specifikke enheder, der udfører aktiviteter inden for national sikkerhed, offentlig sikkerhed, forsvar eller retshåndhævelse, herunder forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger, fra visse forpligtelser, der er fastsat i dette direktiv, for så vidt angår disse aktiviteter. Hvor en enhed udelukkende leverer tjenester til en offentlig forvaltningsenhed, der er udelukket fra dette direktivs anvendelsesområde, bør medlemsstater kunne undtage denne enhed fra visse forpligtelser, der er fastsat i dette direktiv, for så vidt angår disse tjenester. Endvidere bør ingen medlemsstat være forpligtet til at meddele oplysninger, hvis videregivelse efter dens opfattelse ville stride mod dens væsentlige interesser med hensyn til national sikkerhed, offentlig sikkerhed eller forsvar. Nationale regler eller EU-regler om beskyttelse af fortrolige oplysninger, hemmeligholdelsesaftaler og uformelle hemmeligholdelsesaftaler, f.eks. Traffic Light Protocol, bør tages i betragtning i denne sammenhæng. Traffic Light Protocol skal forstås som et middel til at informere om eventuelle begrænsninger for så vidt angår den videre spredning af oplysninger. Den anvendes i næsten alle enheder, der håndterer IT-sikkerhedshændelser (CSIRT'er), og i nogle informationsanalyse- og informationsdelingscentre.

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

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

([6]) Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF (EUT L 257 af 28.8.2014, s. 73).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(23) Hvor en sektorspecifik EU-retsakt indeholder bestemmelser, der kræver, at væsentlige eller vigtige enheder træffer foranstaltninger til styring af cybersikkerhedsrisici eller underretter om væsentlige hændelser, og hvor disse krav har en virkning, der mindst svarer til de forpligtelser, der er fastsat i dette direktiv, bør de pågældende bestemmelser,

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

(24) Hvor bestemmelser i en sektorspecifik EU-retsakt kræver, at væsentlige eller vigtige enheder overholder rapporteringsforpligtelser med en virkning, der mindst svarer til de rapporteringsforpligtelser, der er fastsat i dette direktiv, bør der sikres sammenhæng og effektivitet i håndteringen af hændelsesunderretninger. Med henblik herpå bør bestemmelserne vedrørende hændelsesunderretninger i den sektorspecifikke EU-retsakt give CSIRT'erne, de kompetente myndigheder eller de centrale kontaktpunkter for cybersikkerhed (det centrale kontaktpunkt) i henhold til dette direktiv øjeblikkelig adgang til de hændelsesunderretninger, der indgives i overensstemmelse med den sektorspecifikke EU-retsakt. En sådan øjeblikkelig adgang kan navnlig sikres, hvis hændelsesunderretninger uden unødigt ophold sendes til CSIRT'en, den kompetente myndighed eller det centrale kontaktpunkt i henhold til dette direktiv. Medlemsstaterne bør, hvor det er hensigtsmæssigt, indføre en automatisk og direkte rapporteringsmekanisme, der sikrer systematisk og øjeblikkelig udveksling af oplysninger med CSIRT'er, de kompetente myndigheder eller de centrale kontaktpunkter vedrørende håndtering af sådanne hændelsesunderretninger. Med henblik på at forenkle rapporteringen og gennemføre den automatiske og direkte rapporteringsmekanisme vil medlemsstaterne i overensstemmelse med den sektorspecifikke EU-retsakt kunne anvende et enkelt indgangspunkt.

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

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

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

(28) Europa-Parlamentets og Rådets forordning (EU) 2022/2554 ([10]) bør betragtes som en sektorspecifik EU-retsakt i forbindelse med dette direktiv for så vidt angår finansielle enheder. Bestemmelserne i forordning (EU) 2022/2554 om risikostyring inden for informations- og kommunikationsteknologi (IKT), styring af IKT-relaterede hændelser og navnlig indberetning af større IKT-relaterede hændelser, samt om test af digital operationel modstandsdygtighed, ordninger for udveksling af oplysninger og IKT-tredjepartsrisiko bør finde anvendelse i stedet for bestemmelserne i dette direktiv. Medlemsstaterne bør derfor ikke anvende bestemmelserne i dette direktiv om risikostyrings- og rapporterings forpligtelser vedrørende cybersikkerhed samt tilsyn og håndhævelse på finansielle enheder, der er omfattet af forordning (EU) 2022/2554. Samtidig er det vigtigt at opretholde stærke forbindelser og udveksle oplysninger med den finansielle sektor i henhold til dette direktiv. Med henblik herpå giver forordning (EU) 2022/2554 de europæiske tilsynsmyndigheder (ESA'erne) og de kompetente myndigheder i henhold til nævnte forordning mulighed for at deltage i samarbejdsgruppens aktiviteter samt udveksle oplysninger og samarbejde med de centrale kontaktpunkter såvel som CSIRT'erne og de kompetente myndigheder i henhold til dette direktiv. De kompetente myndigheder i henhold til forordning (EU) 2022/2554 bør også fremsende oplysninger om større IKT-relaterede hændelser og, hvor det er relevant, væsentlige cybertrusler til CSIRT'erne, de kompetente myndigheder eller de centrale kontaktpunkter i henhold til dette direktiv. Dette kan opnås ved at sikre øjeblikkelig adgang til hændelsesun-

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

derretninger og videresende af dem enten direkte eller via et enkelt indgangspunkt. Desuden bør medlemsstaterne fortsat medtage den finansielle sektor i deres cybersikkerhedsstrategier, og CSIRT'er kan dække den finansielle sektor i deres aktiviteter.

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

(30) I betragtning af de indbyrdes forbindelser mellem cybersikkerhed og enheders fysiske sikkerhed bør der sikres en sammenhængende tilgang mellem Europa-Parlamentets og Rådets direktiv (EU) 2022/2557 ([13]) og nærværende direktiv. Med henblik herpå bør enheder identificeret som kritiske enheder i henhold til direktiv (EU) 2022/2557 betragtes som væsentlige enheder i henhold til nærværende direktiv. Endvidere bør hver medlemsstat sikre, at dens nationale cybersikkerhedsstrategi skaber en politisk ramme for øget koordinering i nævnte medlemsstat mellem dens kompetente myndigheder i henhold til nærværende direktiv og dem i henhold til direktiv (EU) 2022/2557 i forbindelse med udveksling af oplysninger om risici, cybertrusler og hændelser samt om ikke-cyberrelaterede risici, trusler og hændelser samt om udøvelse af tilsynsopgaver. De kompetente myndigheder i henhold til nærværende direktiv og de i henhold til direktiv (EU) 2022/2557 bør samarbejde og udveksle oplysninger uden unødigt ophold, navnlig vedrørende identifikation af kritiske enheder, om risici, cybertrusler og hændelser samt om ikke-cyberrelaterede risici, trusler og hændelser, der påvirker kritiske enheder, herunder cybersikkerhedsforanstaltninger og fysiske foranstaltninger, der træffes af kritiske enheder, såvel som resultaterne af tilsynsaktiviteter, der udføres med hensyn til sådanne enheder.

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

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

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

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

([13]) Europa-Parlamentets og Rådets direktiv (EU) 2022/2557 af 14. december 2022 om kritiske enheders modstandsdygtighed og om ophævelse af Rådets direktiv 2008/114/EF (se side 164 i denne EUT).

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

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

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

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

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

(36) Forskningsaktiviteter spiller en central rolle i udviklingen af nye produkter og processer. Mange af disse aktiviteter udføres af enheder, der deler, udbreder eller udnytter resultaterne af deres forskning til kommercielle formål. Disse enheder kan derfor være vigtige led i værdikæder, hvilket gør sikkerheden af deres net- og informationssystemer til en integreret del af det indre markeds overordnede cybersikkerhed. Begrebet »forskningsorganisationer« bør forstås som omfattende enheder, der primært beskæftiger sig med anvendt forskning eller udvikling i den i Organisationen

for Økonomisk Samarbejde og Udviklings Frascati-manual fra 2015 (»Guidelines for Collecting and Reporting Data on Research and Experimental Development«) anvendte betydning med henblik på at udnytte resultaterne heraf til kommercielle formål såsom fremstilling eller udvikling af et produkt eller proces, levering af en tjeneste eller markedsføringen heraf.

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

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

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

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

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

(42) CSIRT'erne har til opgave at håndtere hændelser. Dette omfatter behandling af store mængder til tider følsomme oplysninger. Medlemsstaterne bør sikre, at CSIRT'erne har en infrastruktur til udveksling og behandling af oplysninger samt veludstyrede medarbejdere, hvilket sikrer fortroligheden og pålideligheden af deres operationer. CSIRT'erne vil også kunne vedtage adfærdskodekser i den henseende.

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

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

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

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

(47) CSIRT-netværket bør fortsat bidrage til at styrke fortroligheden og tilliden og til at fremme hurtigt og effektivt operationelt samarbejde mellem medlemsstaterne. For at styrke det operationelle samarbejde på EU-plan bør CSIRT-netværket overveje at indbyde EU-organer og -agenturer, der er involveret i cybersikkerhedspolitikken, såsom Europol, til at deltage i sit arbejde.

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

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

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

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

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

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

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

(55) Offentlig-private partnerskaber (OPP'er) inden for cybersikkerhed kan skabe en passende ramme for udveksling af viden, deling af bedste praksis og etablering af et fælles forståelsesniveau blandt interessenter. Medlemsstaterne bør fremme politikker til støtte for oprettelsen af cybersikkerhedsspecifikke OPP'er. Disse politikker bør bl.a. klarlægge anvendelsesområdet og de involverede interessenter, styringsmodellen, de tilgængelige finansieringsmuligheder og samspillet mellem de deltagende interessenter med hensyn til OPP'er. OPP'er kan udnytte ekspertisen i enheder inden for den private sektor med henblik på at bistå de kompetente myndigheder i udviklingen af tjenester og processer på det aktuelle teknologiske stade, herunder udveksling af oplysninger, tidlig varsling, cybertrussels- og -hændelsesøvelser, krisestyring og planlægning af modstandsdygtighed.

(56) Medlemsstaterne bør i deres nationale cybersikkerhedsstrategier tackle små og mellemstore virksomheders specifikke cybersikkerhedsbehov. Små og mellemstore virksomheder udgør på tværs af Unionen en stor procentdel af industri- og forretningsmarkedet og kæmper ofte med at tilpasse sig nye forretningspraksisser i en mere forbundet verden og til det digitale miljø, hvor medarbejdere arbejder hjemmefra, og forretning i stigende grad drives online. Nogle små og mellemstore virksomheder står over for specifikke cybersikkerhedsudfordringer, såsom ringe cyberbevidsthed, manglende IT-sikkerhed i forbindelse med fjernarbejde, de store omkostninger forbundet med cybersikkerhedsløsninger og et øget trusselsniveau, som f.eks. ransomware, som de bør modtage vejledning i og assistance til. Små og mellemstore virksomheder er i stigende grad mål for angreb i forsyningskæden på grund af deres mindre strenge foranstaltninger til styring af cybersikkerhedsrisici og angrebsstyring, samt det faktum at de har begrænsede sikkerhedsressourcer. Sådanne angreb i forsyningskæden har ikke kun indvirkning på små og mellemstore virksomheder og deres aktiviteter isoleret set, men kan også have en kaskadevirkning på større angreb på enheder, som de leverede varer til. Medlemsstaterne bør gennem deres nationale cybersikkerhedsstrategier hjælpe

små og mellemstore virksomheder med at tackle de udfordringer, de står over for i deres forsyningskæder. Medlemsstaterne bør have et kontaktpunkt for små og mellemstore virksomheder på nationalt eller regionalt plan, som enten yder vejledning og bistand til små og mellemstore virksomheder eller retter dem mod de relevante organer med henblik på vejledning og bistand med hensyn til cybersikkerhedsrelaterede spørgsmål. Medlemsstaterne tilskyndes også til at tilbyde tjenester såsom webstedskonfigurering og muliggørelse af logning til mikrovirksomheder og små virksomheder, der mangler disse kapaciteter.

(57) Medlemsstaterne bør som led i deres nationale cybersikkerhedsstrategier vedtage politikker til fremme af aktiv cyberbeskyttelse som led i en bredere defensiv strategi. Snarere end at svare reaktivt består aktiv cyberbeskyttelse i forebyggelse, opdagelse, overvågning, analyse og afbødning af brud på netsikkerheden på en aktiv måde kombineret med anvendelse af kapaciteter i og uden for det net, der angribes. Dette vil kunne omfatte medlemsstater, der tilbyder gratis tjenester eller værktøjer til visse enheder, herunder selvbetjeningskontrol, opdagelsesværktøjer og fjernelsestjenester. Evnen til hurtigt og automatisk at udveksle og forstå trusselsoplysninger og -analyser, cyberaktivitetsalarmer og reaktionsforanstaltninger er helt afgørende for at muliggøre en forenet indsats med hensyn til på vellykket vis at forebygge, opdage, imødegå og blokere angreb på net- og informationssystemer. Aktiv cyberbeskyttelse er baseret på en defensiv strategi, der udelukker offensive foranstaltninger.

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

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

(60) Medlemsstaterne bør i samarbejde med ENISA træffe foranstaltninger til at fremme koordineret offentliggørelse af sårbarheder ved at fastlægge en relevant national politik. Som led i deres nationale politik bør medlemsstaterne så vidt muligt tackle de udfordringer, som sårbarhedsforskere står over for, herunder deres potentielle strafansvar, i overensstemmelse med nationale ret. Eftersom fysiske og juridiske personer, der forsker i sårbarheder, i nogle medlemsstater vil kunne blive udsat for strafferetligt og civilretligt ansvar, opfordres medlemsstaterne til at vedtage retningslinjer for ikke-retsforfølgelse af informationssikkerhedsforskere og en fritagelse for civilretligt ansvar for deres aktiviteter.

(61) Medlemsstaterne bør udpege en af deres CSIRT'er som koordinator med henblik på at fungere som betroet formidler mellem de rapporterende fysiske eller juridiske personer og producenterne eller udbyderne af IKT-produkter eller -tjenester, som sandsynligvis vil blive berørt af sårbarheden, hvor det er nødvendigt. Den CSIRT, der er udpeget som koordinator, bør bl.a. have til opgave at identificere og kontakte de berørte enheder, at bistå de fysiske eller juridiske personer, der rapporterer en sårbarhed, at forhandle tidsfrister for offentliggørelse og at håndtere sårbarheder, der

påvirker flere enheder (koordineret offentliggørelse af sårbarheder med flere parter). Hvor den rapporterede sårbarhed vil kunne have væsentlig indvirkning på enheder i mere end én medlemsstat, bør de CSIRT'er, der er udpeget som koordinatorer, i givet fald samarbejde inden for CSIRT-netværket.

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

(63) Selv om der findes lignende sårbarhedsregistre eller -databaser, hostes og vedligeholdes disse af enheder, der ikke er etableret i Unionen. En europæisk sårbarhedsdatabase, der vedligeholdes af ENISA, vil give større gennemsigtighed med hensyn til offentliggørelsesprocessen, inden sårbarheden offentliggøres, og modstandsdygtighed i tilfælde af en forstyrrelse eller en afbrydelse af leveringen af tilsvarende tjenester. For i videst muligt omfang at undgå dobbeltarbejde og tilstræbe komplementaritet bør ENISA undersøge muligheden for at indgå strukturerede samarbejdsaftaler med lignende registre eller databaser, der henhører under tredjelandes jurisdiktioner. ENISA bør navnlig undersøge muligheden for et tæt samarbejde med operatørerne af det fælles sårbarheds- og eksponeringssystem (CVE).

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

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

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

oprettet ved forordning (EU) 2018/1139, og Den Europæiske Unions Agentur for Rumprogrammet, oprettet ved Europa-Parlamentets og Rådets forordning (EU) 2021/696 ([14]), til at deltage i sit arbejde.

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

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

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

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

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

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

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

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

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

(73) Unionen kan, hvor det er hensigtsmæssigt, i overensstemmelse med artikel 218 i TEUF indgå internationale aftaler med tredjelande eller internationale organisationer, som giver mulighed for og tilrettelægger disses deltagelse i bestemte aktiviteter, der foretages af samarbejdsgruppen, CSIRT-netværket og EU-CyCLONe. Sådanne aftaler bør sikre Unionens interesser og tilstrækkelig databeskyttelse. Dette bør ikke udelukke medlemsstaternes ret til at samarbejde med tredjelande om håndtering af sårbarheder og styring af cybersikkerhedsrisici og lette rapportering og generel udveksling af oplysninger i overensstemmelse med EU-retten.

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

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

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

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

(77) Ansvaret for at sikre sikkerheden i net- og informationssystemer ligger i vid udstrækning hos væsentlige og vigtige enheder. En risikostyringskultur, der indbefatter risikovurderinger og gennemførelse af foranstaltninger til styring af cybersikkerhedsrisici, som står i forhold til de foreliggende risici, bør fremmes og udvikles.

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

(79) Da trusler mod sikkerheden i net- og informationssystemer kan have forskellig oprindelse, bør foranstaltninger til styring af cybersikkerhedsrisici bygge på en tilgang, der omfatter alle farer og sigter på at beskytte net- og informationssystemer og disse systemers fysiske miljø mod enhver begivenhed såsom tyveri, brand, oversvømmelse, telekommunikations- eller strømsvigt, eller uautoriseret fysisk adgang til, beskadigelse af eller indgreb i en væsentlig eller vigtig enheds informations- og informationsbehandlingsfaciliteter, som kan kompromittere tilgængeligheden, autenticiteten, integriteten eller fortroligheden af lagrede, overførte eller behandlede data eller de tjenester, der tilbydes af eller er tilgængelige via net- og informationssystemerne. Foranstaltningerne til styring af cybersikkerhedsrisici bør derfor også adressere den fysiske og miljømæssige sikkerhed i net- og informationssystemerne ved at inkludere foranstaltninger til beskyttelse af sådanne systemer mod systemsvigt, menneskelige fejl, ondsindede handlinger eller naturfænomener i overensstemmelse med europæiske og internationale standarder såsom dem, der indgår i ISO/IEC 27000-serien. Væsentlige og vigtige enheder bør med henblik herpå som led i deres foranstaltninger til styring af cybersikkerhedsrisici også adressere sikkerheden vedrørende menneskelige ressourcer og indføre passende adgangskontrolpolitikker. Disse foranstaltninger bør være forenelige med direktiv (EU) 2022/2557.

(80) Med henblik på at påvise overensstemmelse med foranstaltninger til styring af cybersikkerhedsrisici og i mangel af passende europæiske cybersikkerhedscertificeringsordninger vedtaget i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) 2019/881 ([18]) bør medlemsstaterne i samråd med samarbejdsgruppen og Den Europæiske Cybersikkerhedscertificeringsgruppe fremme væsentlige og vigtige enheders anvendelse af relevante europæiske og internationale standarder eller kan eventuelt kræve, at enhederne anvender certificerede IKT-produkter, -tjenester og -processer.

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

(82) Foranstaltninger til styring af cybersikkerhedsrisici bør stå i et passende forhold til graden af de væsentlige eller vigtige enheders risikoeksponering og til den samfundsmæssige og økonomiske indvirkning, som en hændelse ville have. Ved fastlæggelsen af foranstaltninger til styring af cybersikkerhedsrisici, der er tilpasset væsentlige og vigtige enheder, bør der tages behørigt hensyn til væsentlige og vigtige enheders forskellige risikoeksponering, herunder enhedens kritiske betydning, de risici, herunder samfundsmæssige risici, som den er eksponeret for, enhedens størrelse og sandsynligheden for hændelser og deres alvor, herunder deres samfundsmæssige og økonomiske indvirkning.

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

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

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

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

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

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

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

(89) Væsentlige og vigtige enheder bør indføre en bred vifte af grundlæggende cyberhygiejnepraksisser såsom »zero trust«-principper, softwareopdateringer, enhedskonfiguration, netværkssegmentering, identitets- og adgangsstyring eller brugerbevidsthed, arrangere kurser for deres personale og højne bevidstheden om cybertrusler, phishing og social engineering-teknikker. Disse enheder bør desuden evaluere deres egne cybersikkerhedskapaciteter og, hvor det er hensigtsmæssigt, stræbe efter at integrere cybersikkerhedsforstærkende teknologier, såsom systemer baseret på kunstig intelligens eller maskinlæring, for at forstærke deres kapaciteter og sikkerheden i net- og informationssystemerne.

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

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

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

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

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

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

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

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

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

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

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

(99) For at beskytte sikkerheden af og forhindre misbrug af og manipulation med offentlige elektroniske kommunikationsnet og offentligt tilgængelige elektroniske kommunikationstjenester bør brugen af sikre routingstandarder fremmes for at sikre integriteten og robustheden af routingfunktionerne i hele økosystemet af udbydere af internetadgangstjenester.

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

(101) I dette direktiv fastlægges en flertrinstilgang for underretning om væsentlige hændelser med henblik på at finde den rette balance mellem på den ene side hurtig underretning, der bidrager til at afbøde den potentielle spredning af væsentlige hændelser og giver væsentlige og vigtige enheder mulighed for at søge assistance, og på den anden side dybdegående underretning, der gør det muligt at høste værdifulde erfaringer af individuelle hændelser og over tid forbedre individuelle virksomheders og hele sektorers cyberrobusthed. Direktivet bør i den henseende omfatte underretning om hændelser, som ud fra en indledende vurdering foretaget af den berørte enhed kunne forårsage alvorlige driftsmæssige forstyrrelser af tjenesterne eller økonomiske tab for denne enhed eller forvolde betydelig materiel eller immateriel skade for andre fysiske eller juridiske personer. En sådan indledende vurdering bør bl.a. tage i betragtning de berørte net- og informationssystemer, navnlig deres betydning for leveringen af enhedens tjenester, alvoren og de tekniske karakteristika af en cybertrussel, eventuelle underliggende sårbarheder, der udnyttes, samt enhedens erfaring med tilsvarende hændelser. Indikatorer såsom graden af påvirkning af tjenestens funktionsdygtighed, varigheden af en hændelse eller antallet af berørte tjenestemodtagere vil kunne spille en vigtig rolle med hensyn til at fastslå, om den driftsmæssige forstyrrelse af tjenesten er alvorlig.

(102) Hvor væsentlige og vigtige enheder bliver opmærksomme på en væsentlig hændelse, bør de være forpligtet til at indgive en tidlig varsling uden unødigt ophold og under alle omstændigheder inden for 24 timer. Denne tidlige varsling bør efterfølges af en hændelsesunderretning. De pågældende enheder bør indgive en hændelsesunderretning uden unødigt ophold og under alle omstændigheder inden for 72 timer efter, at have fået kendskab til den væsentlige hændelse, navnlig med henblik på at ajourføre de oplysninger, der blev indgivet ved den tidlige varsling, og give en indledende vurdering af den væsentlige hændelse, herunder dens alvor og indvirkning, samt kompromitteringsindikatorer, hvor sådanne foreligger. En endelig rapport bør indgives senest en måned efter hændelsesunderretningen. Den tidlige varsling bør kun indeholde de oplysninger, der er nødvendige for at gøre CSIRT'en eller i givet fald den kompetente myndighed opmærksom på den væsentlige hændelse og give den pågældende enhed mulighed for om nødvendigt at søge assistance. En sådan tidlige varsling bør, hvis det er relevant, angive, om den væsentlige hændelse mistænkes for at være forårsaget af ulovlige eller ondsindede handlinger, og om den sandsynligvis vil have grænseoverskridende virkninger. Medlemsstaterne bør sikre, at forpligtelsen til at indgive den tidlige varsling eller den efterfølgende hændelsesunderretning ikke medfører, at den underrettende enhed bruger færre ressourcer på aktiviteter vedrørende håndtering af hændelser, idet disse bør prioriteres, så det forhindres, at forpligtelser vedrørende hændelsesrapportering enten omdirigerer ressourcer fra håndtering af væsentlige hændelser eller på

anden måde kompromitterer enhedens indsats i denne henseende. I tilfælde af, at en hændelse pågår på tidspunktet for indgivelsen af den endelige rapport, bør medlemsstaterne sikre, at berørte enheder forelægger en statusrapport på det pågældende tidspunkt og en endelig rapport senest en måned efter deres håndtering af den væsentlige hændelse.

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

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

(105) En proaktiv tilgang til cybertrusler er et afgørende element i styring af cybersikkerhedsrisici, som bør sætte de kompetente myndigheder i stand til effektivt at forhindre cybertrusler i at blive til hændelser, der kan forårsage betydelige materiel eller immateriel skade. Med henblik herpå er underretning om cybertrusler af afgørende betydning. Enhederne opfordres med dette for øje til på frivillig basis at rapportere cybertrusler.

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

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

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

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

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

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

(111) For at sikre, at nøjagtige og fuldstændige domænenavnsregistreringsdata er til rådighed, bør topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester, indsamle og garantere integriteten og tilgængeligheden af domænenavnsregistreringsdata. Topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester, bør navnlig fastlægge politikker og procedurer for indsamling og vedligeholdelse af nøjagtige og fuldstændige domænenavnsregistreringsdata samt for forebyggelse og rettelse af unøjagtige registreringsdata, i overensstemmelse med EU-databeskyttelsesretten. Disse politikker og procedurer bør så vidt muligt tage hensyn til de standarder, der er udviklet af multiinteressentstyringsstrukturerne på internationalt plan. Topdomænenavneadministratorerne og de enheder, der leverer domænenavnsregistreringstjenester, bør fastlægge og indføre forholdsmæssige procedurer til verifikation af domænenavnsregistreringsdata. Disse procedurer bør afspejle den bedste praksis, der anvendes i industrien, og så vidt muligt de fremskridt, der er gjort inden for elektronisk identifikation. Verifikationsprocedurerne kan eksempelvis bestå i forudgående kontrol, der foretages på tidspunktet for registreringen, og efterfølgende kontrol, der foretages efter registreringen. Topdomænenavneadministratorerne og de enheder, der leverer domænenavnsregistreringstjenester, bør navnlig verificere mindst én kontaktmåde for registranten.

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

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

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

(114) For at tage hensyn til den grænseoverskridende karakter af de tjenester og operationer, der henholdsvis leveres og udføres af DNS-tjenesteudbydere, topdomænenavneadministratorer, enheder, der leverer domænenavnsregistreringstjenester, og udbydere af cloudcomputingtjenester, af datacentertjenester, af indholdsleveringsnetværk, af administrerede tjenester, af administrerede sikkerhedstjenester, af onlinemarkedspladser, af onlinesøgemaskiner og af platforme for sociale netværkstjenester, bør kun én medlemsstat have jurisdiktion over disse enheder. Jurisdiktionen bør tillægges den medlemsstat, hvor den pågældende enhed har sit hovedforretningssted i Unionen. For så vidt angår dette direktiv indebærer forretningsstedskriteriet i dette direktiv en faktisk udøvelse af virksomhed gennem faste ordninger. De pågældende ordningers juridiske form — hvorvidt der er tale om en filial eller et datterselskab med status som juridisk person — er ikke den afgørende faktor i denne forbindelse. Opfyldelsen af det nævnte kriterium bør ikke afhænge af, om net- og informationssystemerne fysisk befinder sig på et givent sted; tilstedeværelsen og anvendelsen af sådanne systemer udgør ikke i sig selv et sådant hovedforretningssted og er derfor ikke afgørende for fastlæggelsen af samme. Hovedforretningsstedet bør anses som værende i den medlemsstat, hvor beslutningerne vedrørende foranstaltninger til styring af cybersikkerhedsrisici overvejende træffes i Unionen. Det vil typisk være det sted, hvor enhedernes centrale administration i Unionen er placeret. Hvis en sådan medlemsstat ikke kan fastslås, eller hvis sådanne beslutninger ikke træffes i Unionen, bør hovedforretningsstedet anses for at være i den medlemsstat, hvor der udføres cybersikkerhedsoperationer. Hvis en sådan medlemsstat ikke kan fastslås, bør hovedforretningsstedet anses for at være i den medlemsstat, hvor enhedens forretningssted med det største antal ansatte i Unionen er beliggende. Hvor tjenesterne udføres af en gruppe af virksomheder, bør den kontrollerende virksomheds hovedforretningssted anses for at være hele gruppens hovedforretningssted.

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

(116) Hvor en DNS-tjenesteudbyder, en topdomænenavneadministrator, en enhed, der leverer domænenavnsregistreringstjenester eller en udbyder af cloudcomputingtjenester, af datacentertjenester, af indholdsleveringsnetværk, af administrerede tjenester, af administrerede sikkerhedstjenester, af onlinemarkedspladser, af onlinesøgemaskiner eller af platforme for sociale netværkstjenester, som ikke er etableret i Unionen, udbyder tjenester i Unionen, bør denne udpege en repræsentant i Unionen. Med henblik på at afgøre, om en sådan enhed udbyder tjenester i Unionen, bør det fastslås, om enheden har til hensigt at udbyde tjenester til personer i en eller flere medlemsstater. Det blotte faktum, at der i Unionen er adgang til enhedens eller en formidlers websted eller til en e-mailadresse og andre kontaktoplysninger, eller at der benyttes et sprog, som almindeligvis benyttes i det tredjeland, hvor enheden er etableret, bør anses for utilstrækkeligt til at fastslå en sådan hensigt. Imidlertid vil faktorer såsom anvendelse af et sprog eller en valuta, der almindeligvis anvendes i en eller flere medlemsstater, muligheden for at bestille tjenester på det pågældende sprog eller omtale af kunder eller brugere, der befinder sig i Unionen, kunne gøre det åbenbart, at enheden har til hensigt at udbyde tjenester i Unionen. Repræsentanten bør handle på vegne af enheden, og det bør være muligt for de kompetente myndigheder eller CSIRT'er at kontakte repræsentanten. Repræsentanten bør have et udtrykkeligt skriftligt mandat fra enheden til at handle på sidstnævntes vegne for så vidt angår sidstnævntes forpligtelser, der er fastsat i dette direktiv, herunder rapportering af hændelser.

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

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

(119) I takt med at cybertrusler bliver mere komplekse og sofistikerede, er evnen til at opdage sådanne trusler og træffe effektive forebyggelsesforanstaltninger mod dem i høj grad afhængig af regelmæssig udveksling af trussels- og sårbarhedsefterretninger mellem enheder. Udveksling af oplysninger bidrager til øget bevidsthed om cybertrusler, hvilket igen styrker enhedernes evne til at forhindre trusler i at blive til hændelser og sætter dem i stand til bedre at inddæmme virkningerne af hændelser og reetablere sig mere effektivt. I mangel af vejledning på EU-plan synes flere faktorer at have hæmmet en sådan udveksling af efterretninger, navnlig usikkerhed om foreneligheden med konkurrence- og ansvarsregler.

(120) Enhederne bør tilskyndes til, med bistand fra medlemsstaterne, i fællesskab at udnytte deres individuelle viden og praktiske erfaring på strategisk, taktisk og operationelt plan med henblik på at styrke deres kapacitet til i tilstrækkeligt omfang at forebygge, opdage, reagere på eller reetablere sig efter hændelser eller afbøde deres virkninger. Det er derfor nødvendigt at gøre det muligt på EU-plan at etablere frivillige ordninger for udveksling af cybersikkerhedsoplysninger. Med henblik herpå bør medlemsstaterne aktivt bistå og tilskynde enheder, såsom dem der leverer cybersikkerhedstjenester og -forskning, samt relevante enheder, der ikke er omfattet af dette direktivs anvendelsesområde til at deltage i sådanne ordninger for udveksling af cybersikkerhedsoplysninger. Disse ordninger bør etableres i overensstemmelse med EU-konkurrencereglerne og EU-databeskyttelsesretten.

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

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

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

(124) Ved udøvelsen af efterfølgende tilsyn bør de kompetente myndigheder kunne træffe afgørelse om prioriteringen af de tilsynsforanstaltninger og -midler, som de har til rådighed, på en forholdsmæssig måde. Dette indebærer, at de kompetente myndigheder kan træffe afgørelse om en sådan prioritering på grundlag af tilsynsmetoder, som bør baseres på en risikobaseret tilgang. Mere specifikt vil sådanne metoder kunne omfatte kriterier eller benchmarks for klassificering af væsentlige enheder i risikokategorier og tilsvarende anbefalede tilsynsforanstaltninger og -midler pr. risikokategori, som f.eks. brugen, hyppigheden eller typerne af kontrol på stedet, målrettede sikkerhedsaudits eller -scanninger, typen af oplysninger, der skal anmodes om, og detaljeringsgraden af disse oplysninger. Sådanne

tilsynsmetoder vil også kunne ledsages af arbejdsprogrammer og vurderes og revideres regelmæssigt, herunder vedrørende aspekter såsom ressourcefordeling og -behov. For så vidt angår offentlige forvaltningsorganer bør tilsynsbeføjelserne udøves i overensstemmelse med de nationale lovgivningsmæssige og institutionelle rammer.

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

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

(127) For at gøre håndhævelse effektiv bør der fastlægges en minimumsliste over håndhævelsesbeføjelser, der kan udøves for overtrædelse af foranstaltningerne til styring af cybersikkerhedsrisici og rapporteringskravene i dette direktiv, som opstiller en klar og konsekvent ramme for sådan håndhævelse i hele Unionen. Der bør tages behørigt hensyn til overtrædelsen af dette direktivs art, grovhed og varighed, den forvoldte materielle eller immaterielle skade, hvorvidt overtrædelsen var forsætlig eller uagtsom, tiltag truffet for at forebygge eller afbøde den materielle eller immaterielle skade, graden af ansvar eller eventuelle relevante tidligere overtrædelser, graden af samarbejde med den kompetente myndighed og enhver anden skærpende eller formildende omstændighed. Håndhævelsesforanstaltningerne, herunder administrative bøder, bør være forholdsmæssige, og pålæggelsen heraf bør være underlagt passende proceduremæssige garantier i overensstemmelse med de generelle principper i EU-retten og Den Europæiske Unions charter om grundlæggende rettigheder (chartret), herunder adgangen til effektive retsmidler og retten til en retfærdig rettergang, uskyldsformodningen og retten til et forsvar.

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

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

(130) Hvor en administrative bøde pålægges en væsentlig eller vigtig enhed, der er en virksomhed, bør der ved virksomhed i denne forbindelse forstås en virksomhed i overensstemmelse med artikel 101 og 102 i TEUF. Hvor en administrativ bøde pålægges en person, der ikke er en virksomhed, bør den kompetente myndighed ved fastsættelsen af en passende bødestørrelse tage hensyn til det generelle indkomstniveau i den pågældende medlemsstat og personens økonomiske stilling. Det bør være op til medlemsstaterne at bestemme, om og i hvilket omfang de offentlige myndigheder bør kunne pålægges administrative bøder. Pålæggelse af en administrativ bøde berører ikke de kompetente myndigheders anvendelse af andre beføjelser eller andre sanktioner, der er fastsat i de nationale regler til gennemførelse af dette direktiv.

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

(132) Hvor dette direktiv ikke harmoniserer administrative sanktioner eller hvor det i andre tilfælde er nødvendigt, f.eks. i tilfælde af en alvorlig overtrædelse af dette direktiv, bør medlemsstaterne indføre en ordning, der giver mulighed for at pålægge sanktioner, som er effektive, står i rimeligt forhold til overtrædelsen og har afskrækkende virkning. Sanktionernes art, herunder om de skal være strafferetlige eller administrative, bør fastsættes ved national ret.

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

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

(135) For at sikre effektivt tilsyn og effektiv håndhævelse, navnlig i en situation med en grænseoverskridende dimension, bør en medlemsstat, der har modtaget en anmodning om gensidig bistand, inden for rammerne af denne anmodning træffe passende tilsyns- og håndhævelsesforanstaltninger over for den enhed, der er genstand for denne anmodning, og som leverer tjenester eller har et net- og informationssystem på denne medlemsstats område.

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

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

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

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

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

(140) Kommissionen bør regelmæssigt evaluere dette direktiv efter høring af interessenter, navnlig med henblik på at afgøre, om det er hensigtsmæssigt at foreslå ændringer i lyset af skiftende samfundsmæssige, politiske eller teknologiske vilkår eller markedsvilkår. Som led i disse evalueringer bør Kommissionen vurdere relevansen af størrelsen af de berørte enheder, sektorerne, delsektorerne og typerne af enheder omhandlet i dette direktivs bilag for, hvordan økonomien og samfundet fungerer i relation til cybersikkerhed. Kommissionen bør bl.a. vurdere, hvorvidt udbydere, der er omfattet af dette direktivs anvendelsesområde og er udpeget som meget store onlineplatforme i den i artikel 33 i Europa-Parlamentets og Rådets forordning (EU) 2022/2065 ([24]) anvendte betydning, vil kunne identificeres som væsentlige enheder i henhold til dette direktiv.

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

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

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

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

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

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

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

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

VEDTAGET DETTE DIREKTIV:

KAPITEL I

GENERELLE BESTEMMELSER

Artikel 1

Genstand

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

2. Med henblik herpå fastlægger dette direktiv:

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

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

c) regler og forpligtelser vedrørende udveksling af cybersikkerhedsoplysninger

d) tilsyns- og håndhævelsesforpligtelser for medlemsstaterne.

Artikel 2

Anvendelsesområde

1. Dette direktiv finder anvendelse på offentlige eller private enheder af den type, der er omhandlet i bilag I eller II, som udgør mellemstore virksomheder i henhold til artikel 2 i bilaget til henstilling 2003/361/EF, eller overskrider tærsklerne for mellemstore virksomheder fastsat i nævnte artikels stk. 1, og som leverer deres tjenester eller udfører deres aktiviteter inden for Unionen.

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

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

a) tjenester leveres af:

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

   ii) tillidstjenesteudbydere

   iii) topdomænenavneadministratorer og udbydere af domænenavnesystemer

b) enheden er den eneste udbyder i en medlemsstat af en tjeneste, der er væsentlig for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter

c) en forstyrrelse af den tjeneste, enheden leverer, vil kunne have væsentlig indvirkning på den offentlige sikkerhed eller folkesundheden

d) en forstyrrelse af den tjeneste, enheden leverer, vil kunne medføre en væsentlig systemisk risiko, navnlig for sektorer, hvor en sådan forstyrrelse kan have en grænseoverskridende virkning

e) enheden er kritisk på grund af sin specifikke betydning på nationalt eller regionalt plan for den pågældende sektor eller type af tjeneste eller for andre indbyrdes afhængige sektorer i medlemsstaten

f) enheden er en offentlig forvaltningsenhed:

i) under den centrale forvaltning som defineret af en medlemsstat i overensstemmelse med national ret eller

ii) på regionalt plan som defineret af en medlemsstat i overensstemmelse med national ret, som efter en risikobaseret vurdering leverer tjenester, hvis forstyrrelse vil kunne have væsentlig indvirkning på kritiske samfundsmæssige eller økonomiske aktiviteter.

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

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

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

a) offentlige forvaltningsenheder på lokalt plan

b) uddannelsesinstitutioner, navnlig hvor de udfører kritiske forskningsaktiviteter.

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

7. Dette direktiv finder ikke anvendelse på offentlige forvaltningsenheder, der udfører deres aktiviteter inden for national sikkerhed, offentlig sikkerhed, forsvar eller retshåndhævelse, herunder forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger.

8. Medlemsstater kan undtage specifikke enheder, der udfører aktiviteter inden for national sikkerhed, offentlig sikkerhed, forsvar eller retshåndhævelse, herunder forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger, eller som udelukkende leverer tjenester til de offentlige forvaltningsenheder, der er omhandlet i denne artikels stk. 7, fra forpligtelserne i artikel 21 eller 23 for så vidt angår disse aktiviteter eller tjenester. I så fald finder de i kapitel VII omhandlede tilsyns- og håndhævelsesforanstaltninger ikke anvendelse i forbindelse med disse specifikke aktiviteter eller tjenester. Hvor enhederne udelukkende udfører aktiviteter eller leverer tjenester af den type, der er omhandlet i dette stykke, kan medlemsstater beslutte også at fritage disse enheder for forpligtelserne i artikel 3 og 27.

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

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

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

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

13. Uden at det berører artikel 346 i TEUF, udveksles oplysninger, der er fortrolige i henhold til EU-regler eller nationale regler, såsom regler om forretningshemmeligheder, kun med Kommissionen og andre relevante myndigheder i overensstemmelse med dette direktiv, hvor denne udveksling er nødvendig for anvendelsen af dette direktiv. De udvekslede oplysninger begrænses til, hvad der er relevant og forholdsmæssigt under hensyn til formålet med udvekslingen. Udvekslingen af oplysninger skal bevare de pågældende oplysningers fortrolighed og beskytte de berørte enheders sikkerhed og kommercielle interesser.

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

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

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

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

Artikel 3

Væsentlige og vigtige enheder

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

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

b) kvalificerede tillidstjenesteudbydere og topdomænenavneadministratorer samt DNS-tjenesteudbydere, uanset deres størrelse

c) udbydere af offentlige elektroniske kommunikationsnet eller af offentligt tilgængelige elektroniske kommunikationstjenester, der udgør mellemstore virksomheder i henhold til artikel 2, i bilaget til henstilling 2003/361/EF

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

e) alle andre enheder af en type omhandlet i bilag I eller II, som en medlemsstat har identificeret som væsentlige enheder i medfør af artikel 2, stk. 2, litra b)-e)

f) enheder, der er identificeret som kritiske enheder i henhold til direktiv (EU) 2022/2557, jf. artikel 2, stk. 3, i nærværende direktiv

g) hvis medlemsstaten træffer afgørelse herom, enheder, som den pågældende medlemsstat inden den 16. januar 2023 har identificeret som operatører af væsentlige tjenester i overensstemmelse med direktiv (EU) 2016/1148 eller national ret.

2. Med henblik på dette direktiv anses enheder af en type omhandlet i bilag I eller II, der ikke opfylder kriterierne for at være væsentlige enheder i henhold til denne artikels stk. 1, for at være vigtige enheder. Dette indbefatter enheder, som medlemsstaterne har identificeret som vigtige enheder i medfør af artikel 2, stk. 2, litra b)-e).

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

4. Med henblik på udarbejdelsen af den i stk. 3 omhandlede liste pålægger medlemsstaterne de enheder, der er omhandlet i nævnte stykke, at indgive mindst følgende oplysninger til de kompetente myndigheder:

a) enhedens navn

b) adresse og ajourførte kontaktoplysninger, herunder e-mailadresser, IP-intervaller og telefonnumre

c) i givet fald den relevante sektor og delsektor i bilag I eller II, samt

d) i givet fald en liste over de medlemsstater, hvor enheden leverer tjenester, der er omfattet af dette direktivs anvendelsesområde.

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

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

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

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

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

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

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

Artikel 4

Sektorspecifikke EU-retsakter

1. I tilfælde, hvor sektorspecifikke EU-retsakter kræver, at væsentlige eller vigtige enheder træffer foranstaltninger til styring af cybersikkerhedsrisici eller underretter om væsentlige hændelser, og hvor disse krav har en virkning, der mindst svarer til de forpligtelser, der er fastsat i dette direktiv, finder de relevante bestemmelser i dette direktiv, herunder bestemmelserne om tilsyn og håndhævelse, der er fastsat i kapitel VII, ikke finde anvendelse på sådanne enheder. I tilfælde, hvor sektorspecifikke EU-retsakter ikke omfatter alle enheder i en specifik sektor, der er omfattet af dette direktivs anvendelsesområde, finder de relevante bestemmelser i dette direktiv fortsat anvendelse på de enheder, der ikke er omfattet af de nævnte sektorspecifikke EU-retsakter.

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

a) foranstaltningerne til styring af cybersikkerhedsrisici har mindst samme virkning som dem, der er fastsat i artikel 21, stk. 1 og 2, eller

b) den sektorspecifikke EU-retsakt giver CSIRT'erne, de kompetente myndigheder eller de centrale kontaktpunkter i henhold til dette direktiv øjeblikkelig, hvor relevant automatisk og direkte, adgang til underretninger om hændelser, og hvor kravene om at give underretning om væsentlige hændelser mindst har samme virkning som kravene fastsat i dette direktivs artikel 23, stk. 1-6.

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

Artikel 5

Minimumsharmonisering

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

Artikel 6

Definitioner

I dette direktiv forstås ved:

1) »net- og informationssystem«:

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

b) enhver anordning eller gruppe af forbundne eller beslægtede anordninger, hvoraf en eller flere ved hjælp af et program udfører automatisk behandling af digitale data, eller

c) digitale data, som lagres, behandles, fremfindes eller overføres af elementer i litra a) og b) med henblik på deres drift, brug, beskyttelse og vedligeholdelse

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

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

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

5) »nærvedhændelse«: en begivenhed, der kunne have bragt tilgængeligheden, autenticiteten, integriteten eller fortroligheden af lagrede, overførte eller behandlede data eller af de tjenester, der tilbydes af eller er tilgængelige via net- og informationssystemer, i fare, men som det lykkedes at forhindre i at materialisere sig, eller som ikke materialiserede sig

6) »hændelse«: en begivenhed, der bringer tilgængeligheden, autenticiteten, integriteten eller fortroligheden af lagrede, overførte eller behandlede data eller af de tjenester, der tilbydes af eller er tilgængelige via net- og informationssystemer, i fare

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

8) »håndtering af hændelser«: enhver handling og procedure, der tager sigte på at forebygge, opdage, analysere og inddæmme eller at reagere på og reetablere sig efter en hændelse

9) »risiko«: potentialet for tab eller forstyrrelse som følge af en hændelse, udtrykt som en kombination af størrelsen af et sådant tab eller en sådan forstyrrelse og sandsynligheden for, at hændelsen indtræffer

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

11) »væsentlig cybertrussel«: en cybertrussel, som på grundlag af sine tekniske karakteristika kan antages at have potentiale til at få alvorlig indvirkning på en enheds net- og informationssystemer eller på brugerne af enhedens tjenester ved at forårsage betydelig materiel eller immateriel skade

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

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

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

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

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

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

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

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

19) »domænenavnesystem« eller »DNS«: et hierarkisk distribueret navngivningssystem, der gør det muligt at identificere internettjenester og -ressourcer, således at slutbrugerudstyr kan benytte internetrouting- og konnektivitetstjenester til at nå disse tjenester og ressourcer

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

a) offentligt tilgængelige rekursive domænenavnsoversættelsestjenester til internetslutbrugere, eller

b) autoritative domænenavnsoversættelsestjenester til tredjepartsbrug, med undtagelse af rodnavneservere

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

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

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

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

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

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

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

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

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

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

([30]) Europa-Parlamentets og Rådets direktiv (EU) 2015/1535 af 9. september 2015 om en informationsprocedure med hensyn til tekniske forskrifter samt forskrifter for informationssamfundets tjenester (EUT L 241 af 17.9.2015, s. 1).

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

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

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

32) »indholdsleveringsnetværk«: et net af geografisk distribuerede servere med det formål at sikre høj tilgængelighed af, adgang til eller hurtig levering af digitalt indhold og digitale tjenester til internetbrugere på vegne af indholds- og tjenesteudbydere

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

34) »repræsentant«: en fysisk eller juridisk person, der er etableret i Unionen, som udtrykkeligt er udpeget til at handle på vegne af en DNS-tjenesteudbyder, en topdomænenavneadministrator, en enhed, der leverer domænenavnsregistreringstjenester eller en udbyder af cloudcomputingtjenester, af datacentertjenester, af indholdsleveringsnetværk, af administrerede tjenester, af administrerede sikkerhedstjenester, af onlinemarkedspladser, af onlinesøgemaskiner eller af platforme for sociale netværkstjenester, som ikke er etableret i Unionen, og som kan kontaktes af en kompetent myndighed eller en CSIRT på enhedens sted for så vidt angår denne enheds forpligtelser i henhold til dette direktiv

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

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

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

    c) den finansieres overvejende af staten, regionale myndigheder eller af andre offentligretlige organer, er underlagt ledelsesmæssig kontrol af disse myndigheder eller organer, eller har et administrations-, ledelses- eller tilsynsorgan, hvor mere end halvdelen af medlemmerne udpeges af staten, regionale myndigheder eller andre offentligretlige organer

    d) den har beføjelse til at rette administrative eller lovgivningsmæssige afgørelser til fysiske eller juridiske personer, der påvirker deres rettigheder i forbindelse med grænseoverskridende bevægelighed for personer, varer, tjenester eller kapital

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

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

38) »enhed«: en fysisk eller juridisk person, der er oprettet og anerkendt som sådan i henhold til den nationale ret på det sted, hvor den er etableret, og som i eget navn kan udøve rettigheder og være underlagt forpligtelser

39) »udbyder af administrerede tjenester«: en enhed, der leverer tjenester i forbindelse med installation, administration, drift eller vedligeholdelse af IKT-produkter, -net, -infrastruktur, -applikationer eller andre net- og informationssystemer via assistance eller aktiv administration, der udføres enten i kundernes lokaler eller på afstand

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

41) »forskningsorganisation«: en enhed, hvis primære mål er at udføre anvendt forskning eller udvikling med henblik på at udnytte resultaterne af denne forskning til kommercielle formål, men som ikke indbefatter uddannelsesinstitutioner.

KAPITEL II

KOORDINEREDE RAMMER FOR CYBERSIKKERHED

Artikel 7

National cybersikkerhedsstrategi

1. Hver medlemsstat vedtager en national cybersikkerhedsstrategi, der fastlægger de strategiske mål, de nødvendige ressourcer til at nå disse mål, og passende politiske og lovgivningsmæssige foranstaltninger med henblik på at opnå og opretholde et højt cybersikkerhedsniveau. Den nationale cybersikkerhedsstrategi skal omfatte:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

j) fremme af aktiv cyberbeskyttelse.

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

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

Artikel 8

Kompetente myndigheder og centrale kontaktpunkter

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

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

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

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

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

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

Artikel 9

Nationale rammer for cyberkrisestyring

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

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

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

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

a) målene for de nationale beredskabsforanstaltninger og -aktiviteter

b) cyberkrisestyringsmyndighedernes opgaver og ansvarsområder

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

d) nationale beredskabsforanstaltninger, herunder øvelses- og uddannelsesaktiviteter

e) de relevante involverede offentlige og private interessenter og infrastrukturer

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

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

Artikel 10

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

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

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

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

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

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

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

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

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

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

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

Artikel 11

Krav til CSIRT'er og deres tekniske kapaciteter og opgaver

1. CSIRT'erne skal opfylde nedenstående krav:

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

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

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

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

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

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

CSIRT'erne kan deltage i internationale samarbejdsnetværk.

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

3. CSIRT'erne har følgende opgaver:

a) overvågning og analyse af cybertrusler, sårbarheder og hændelser på nationalt plan og, efter anmodning, ydelse af bistand til væsentlige og vigtige enheder vedrørende realtids- eller nærrealtidsovervågning af deres net- og informationssystemer

b) tidlig varsling, alarmer, meddelelser og formidling af oplysninger til berørte væsentlige og vigtige enheder samt til de kompetente myndigheder og andre relevante interessenter om cybertrusler, sårbarheder og hændelser, om muligt i nærrealtid

c) at reagere på hændelser og i givet fald yde bistand til de berørte væsentlige og vigtige enheder

d) at indsamle og analysere kriminaltekniske data og udarbejde dynamiske risiko- og hændelsesanalyser og samt skabe situationsbevidsthed vedrørende cybersikkerhed

e) på anmodning af en væsentlig eller vigtig enhed at foretage en proaktiv scanning af den pågældende enheds net- og informationssystemer for at opdage sårbarheder med en potentielt væsentlig indvirkning

f) at deltage i CSIRT-netværket og yde gensidig bistand i overensstemmelse med deres kapacitet og kompetencer til andre medlemmer af CSIRT-netværket efter anmodning fra disse

g) i givet fald at fungere som koordinator med henblik på den koordinerede offentliggørelse af sårbarheder i henhold til artikel 12, stk. 1

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

CSIRT'erne kan foretage proaktiv ikkeindgribende scanning af væsentlige og vigtige enheders offentligt tilgængelige net- og informationssystemer. En sådan scanning skal foretages for at opdage sårbare eller usikkert konfigurerede net- og informationssystemer og informere de berørte enheder. En sådan scanning må ikke have nogen negativ indvirkning på enhedernes tjenester.

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

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

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

a) procedurer for håndtering af hændelser

b) krisestyring og

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

Artikel 12

Koordineret offentliggørelse af sårbarheder og en europæisk sårbarhedsdatabase

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

a) identifikation af og kontakt til de berørte enheder

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

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

Medlemsstaterne sikrer, at fysiske eller juridiske personer er i stand til at rapportere en sårbarhed, anonymt hvor de anmoder herom, til den CSIRT, der er udpeget som koordinator. Den CSIRT, der er udpeget som koordinator, sørger for omhyggelig opfølgning med hensyn til den rapporterede sårbarhed, og sikrer anonymiteten for den fysiske eller juridiske person, der rapporterer sårbarheden. Hvor en rapporteret sårbarhed vil kunne have en væsentlig indvirkning på enheder i mere end én medlemsstat, samarbejder den CSIRT, der er udpeget som koordinator for hver berørt medlemsstat, om nødvendigt med andre CSIRT'er, der er udpeget som koordinatorer, inden for CSIRT-netværket.

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

a) oplysninger, der beskriver sårbarheden

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

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

Artikel 13

Samarbejde på nationalt plan

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

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

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

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

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

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

KAPITEL III

SAMARBEJDE PÅ EU-PLAN OG INTERNATIONALT PLAN

Artikel 14

Samarbejdsgruppe

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

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

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

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

Sekretariatsopgaverne varetages af Kommissionen.

4. Samarbejdsgruppen har følgende opgaver:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Artikel 15

CSIRT-netværket

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

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

3. CSIRT-netværket har følgende opgaver:

a) at udveksle oplysninger om CSIRT'ernes kapaciteter

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

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

d) at udveksle information vedrørende cybersikkerhedspublikationer og -anbefalinger

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

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

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

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

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

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

   i) kategorier af cybertrusler og hændelser

   ii) tidlig varsling

   iii) gensidig bistand

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

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

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

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

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

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

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

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

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

5. CSIRT-netværket vedtager sin forretningsorden.

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

Artikel 16

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

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

2. EU-CyCLONe består af repræsentanter for medlemsstaternes cyberkrisestyringsmyndigheder samt, i tilfælde hvor en potentiel eller igangværende omfattende cybersikkerhedshændelse har eller sandsynligvis vil have en betydelig indvirkning på tjenester og aktiviteter, der er omfattet af dette direktivs anvendelsesområde, Kommissionen. I andre tilfælde deltager Kommissionen i EU-CyCLONe's aktiviteter som observatør.

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

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

3. EU-CyCLONe har følgende opgaver:

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

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

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

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

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

4. EU-CyCLONe vedtager sin forretningsorden.

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

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

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

Artikel 17

Internationalt samarbejde

Unionen kan, hvor det er hensigtsmæssigt, i overensstemmelse med artikel 218 i TEUF indgå internationale aftaler med tredjelande eller internationale organisationer, der giver mulighed for og tilrettelægger disses deltagelse i bestemte aktiviteter, der foretages af samarbejdsgruppen, CSIRT-netværket og EU-CyCLONe. Sådanne aftaler skal overholde EU-databeskyttelsesretten.

Artikel 18

Rapport om cybersikkerhedssituationen i Unionen

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

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

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

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

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

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

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

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

Artikel 19

Peerevalueringer

1. Samarbejdsgruppen fastlægger senest den 17. januar 2025 med bistand fra Kommissionen og ENISA samt, hvor det er relevant, CSIRT-netværket metodologien og de organisatoriske aspekter af peerevalueringerne med henblik på at lære af fælles erfaringer, styrke gensidig tillid, opnå et højt fælles cybersikkerhedsniveau samt styrke medlemsstaternes cybersikkerhedskapaciteter og -politikker, der er nødvendige for at gennemføre dette direktiv. Deltagelse i peerevalueringer er frivillig. Peerevalueringerne foretages af cybersikkerhedseksperter. Cybersikkerhedseksperterne udpeges af mindst to medlemsstater, som skal være forskellige fra den medlemsstat, der evalueres.

Peerevalueringerne skal mindst omfatte et af følgende aspekter:

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

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

c) CSIRT'ernes operationelle kapacitet

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

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

f) specifikke spørgsmål af grænseoverskridende eller tværsektoriel karakter.

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

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

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

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

6. Peerevalueringer omfatter fysiske eller virtuelle besøg på stedet og ekstern udveksling af oplysninger. I overensstemmelse med princippet om godt samarbejde giver den medlemsstat, der er genstand for peerevalueringen, de udpegede cybersikkerhedseksperter de oplysninger, der er nødvendige for vurderingen, uden at det berører national ret eller EU-retten vedrørende beskyttelse af fortrolige eller klassificerede informationer og varetagelsen af væsentlige statslige funktioner såsom den nationale sikkerhed. Samarbejdsgruppen udarbejder i samarbejde med Kommissionen og ENISA passende adfærdskodekser, der understøtter de udpegede cybersikkerhedseksperters arbejdsmetoder. Alle oplysninger, der indhentes ved peerevalueringen, må kun anvendes til dette formål. De cybersikkerhedseksperter, der deltager i peerevalueringen, må ikke videregive følsomme eller fortrolige oplysninger, som er indhentet som led i denne peerevaluering, til tredjemand.

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

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

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

KAPITEL IV

FORANSTALTNINGER TIL STYRING AF CYBERSIKKERHEDSRISICI OG RAPPORTERINGSFORPLIGTELSER

Artikel 20

Styring

1. Medlemsstaterne sikrer, at de væsentlige og vigtige enheders ledelsesorganer godkender de foranstaltninger til styring af cybersikkerhedsrisici, som disse enheder har truffet med henblik på at overholde artikel 21, fører tilsyn med dens gennemførelse og kan gøres ansvarlige for enhedernes overtrædelser af forpligtelserne i nævnte artikel.

Anvendelsen af dette stykke berører ikke national ret for så vidt angår de ansvarsregler, der gælder for offentlige institutioner, samt ansvaret for embedsmænd og personer valgt eller udnævnt til offentlige hverv.

2. Medlemsstaterne sikrer, at medlemmerne af væsentlige og vigtige enheders ledelsesorganer er forpligtet til at følge kurser, og skal tilskynde væsentlige og vigtige enheder til løbende at tilbyde tilsvarende kurser til deres ansatte, således at de opnår tilstrækkelige kundskaber og færdigheder til at kunne identificere risici og vurdere metoderne til styring af cybersikkerhedsrisici og deres indvirkning på de tjenester, der leveres af enheden.

Artikel 21

Foranstaltninger til styring af cybersikkerhedsrisici

1. Medlemsstaterne sikrer, at væsentlige og vigtige enheder træffer passende og forholdsmæssige tekniske, operationelle og organisatoriske foranstaltninger for at styre risiciene for sikkerheden i net- og informationssystemer, som disse enheder anvender til deres operationer eller til at levere deres tjenester, og for at forhindre hændelser eller minimere deres indvirkning på modtagere af deres tjenester og på andre tjenester.

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

2. De i stk. 1 omhandlede foranstaltninger baseres på en tilgang, der omfatter alle farer og sigter på at beskytte net- og informationssystemer og disse systemers fysiske miljø mod hændelser, og mindst omfatter følgende:

a) politikker for risikoanalyse og informationssystemsikkerhed

b) håndtering af hændelser

c) driftskontinuitet, såsom backup-styring og reetablering efter en katastrofe, og krisestyring

d) forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem den enkelte enhed og dens direkte leverandører eller tjenesteudbydere

e) sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer, herunder håndtering og offentliggørelse af sårbarheder

f) politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici

g) grundlæggende cyberhygiejnepraksisser og cybersikkerhedsuddannelse

h) politikker og procedurer vedrørende brug af kryptografi og, hvor det er relevant, kryptering

i) personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver

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

3. Medlemsstaterne sikrer, at enhederne, når de overvejer, hvilke foranstaltninger omhandlet i denne artikels stk. 2, litra d), der er passende, tager hensyn til de sårbarheder, der er specifikke for hver direkte leverandør og tjenesteudbyder, og den generelle kvalitet af deres leverandørers og tjenesteudbyderes produkter og cybersikkerhedspraksis, herunder deres sikre udviklingsprocedurer. Medlemsstaterne sikrer også, at enhederne, når de overvejer, hvilke foranstaltninger omhandlet i nævnte litra, der er passende, er forpligtet til at tage hensyn til resultaterne af de koordinerede sikkerhedsrisikovurderinger af kritiske forsyningskæder, der foretages i overensstemmelse med artikel 22, stk. 1.

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

5. Senest 17. oktober 2024 vedtager Kommissionen gennemførelsesretsakter, der fastsætter de tekniske og metodologiske krav til de foranstaltninger, der er omhandlet i stk. 2, for så vidt angår DNS-tjenesteudbydere, topdomænenavneadministratorer og udbydere af cloudcomputingtjenester, af datacentertjenester, af indholdsleveringsnetværk, af administrerede tjenester, af administrerede sikkerhedstjenester, af onlinemarkedspladser, af onlinesøgemaskiner og af platforme for sociale netværkstjenester og af tillidstjenester.

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

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

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

Artikel 22

Koordinerede sikkerhedsrisikovurderinger af kritiske forsyningskæder på EU-plan

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

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

Artikel 23

Rapporteringsforpligtelser

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

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

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

2. I givet fald sikrer medlemsstaterne, at væsentlige og vigtige enheder uden unødigt ophold meddeler modtagerne af deres tjenester, som potentielt er berørt af en væsentlig cybertrussel, eventuelle foranstaltninger eller modforholdsregler, som disse modtagere kan træffe som reaktion på den pågældende trussel. Hvor det er relevant, skal enhederne også informere de pågældende modtagere om selve den væsentlige cybertrussel.

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

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

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

4. Medlemsstaterne sikrer, at de berørte enheder med henblik på den i stk. 1 omhandlede underretning fremsender følgende til CSIRT'en eller i givet fald den kompetente myndighed:

a) uden unødigt ophold og under alle omstændigheder inden for 24 timer efter at have fået kendskab til den væsentlige hændelse en tidlig varsling, som i givet fald skal angive, om den væsentlige hændelse mistænkes for at være forårsaget af ulovlige eller ondsindede handlinger eller kunne have en grænseoverskridende virkning

b) uden unødigt ophold og under alle omstændigheder inden for 72 timer efter at have fået kendskab til den væsentlige hændelse, en hændelsesunderretning, som i givet fald skal ajourføre de oplysninger, der er omhandlet under litra a), og give en indledende vurdering af den væsentlige hændelse, herunder dens alvor og indvirkning samt kompromitteringsindikatorerne, hvor sådanne foreligger

c) efter anmodning fra en CSIRT eller i givet fald den kompetente myndighed en foreløbig rapport om relevante statusopdateringer

d) en endelig rapport senest en måned efter forelæggelsen af den i litra b) omhandlede hændelsesunderretning, der skal omfatte følgende:

   i) en detaljeret beskrivelse af hændelsen, herunder dens alvor og indvirkning

   ii) den type trussel eller grundlæggende årsag, der sandsynligvis har udløst hændelsen

   iii) anvendte og igangværende afbødende foranstaltninger

   iv) i givet fald de grænseoverskridende virkninger af hændelsen.

e) i tilfælde af at en hændelse pågår på tidspunktet for indgivelsen af den i litra d), omhandlede endelige rapport, sikrer medlemsstaterne, at berørte enheder forelægger en statusrapport på det pågældende tidspunkt og en endelig rapport senest en måned efter deres håndtering af hændelsen.

Uanset første afsnit, litra b), skal tillidstjenesteudbyderen for så vidt angår væsentlige hændelser, der har en virkning på leveringen af dens tillidstjenester, underrette CSIRT'en eller i givet fald den kompetente myndighed uden unødigt ophold og under alle omstændigheder inden for 24 timer efter at være blevet bekendt med den væsentlige hændelse.

5. CSIRT'en eller den kompetente myndighed giver uden unødigt ophold og, hvor det er muligt, inden for 24 timer efter modtagelsen af den i stk. 4, litra a), omhandlede tidlige varsling den underrettende enhed et svar, herunder indledende tilbagemeldinger om den væsentlige hændelse og, efter anmodning fra enheden, vejledning eller operativ rådgivning om gennemførelsen af mulige afbødende foranstaltninger. Hvor CSIRT'en ikke er den oprindelige modtager af den i stk. 1 omhandlede underretning, gives vejledningen af den kompetente myndighed i samarbejde med CSIRT'en. CSIRT'en yder supplerende teknisk bistand, hvis den berørte enhed anmoder herom. Hvor den væsentlige hændelse mistænkes for at være af strafferetlig karakter, giver CSIRT'en eller den kompetente myndighed også vejledning om underretning om den væsentlige hændelse til retshåndhævende myndigheder.

6. Hvor det er relevant, og navnlig hvor den væsentlige hændelse berører to eller flere medlemsstater, informerer CSIRT'en, den kompetente myndighed eller det centrale kontaktpunkt uden unødigt ophold de øvrige berørte medlemsstater og ENISA om den væsentlige hændelse. Sådan information omfatter den type af oplysninger, der er modtaget i overensstemmelse med stk. 4. CSIRT'en, den kompetente myndighed eller det centrale kontaktpunkt sikrer i den forbindelse i overensstemmelse med EU-retten eller national ret enhedens sikkerhed og kommercielle interesser samt fortrolig behandling af de afgivne oplysninger.

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

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

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

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

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

Senest den 17. oktober 2024 vedtager Kommissionen for så vidt angår DNS-tjenesteudbydere, topdomænenavneadministratorer, enheder, der leverer domænenavnsregistreringstjenester, og udbydere af cloudcomputingtjenester, af datacentertjenester, af indholdsleveringsnetværk, af administrerede tjenester, af administrerede sikkerhedstjenester, af onlinemarkedspladser, af onlinesøgemaskiner og af platforme for sociale netværkstjenester gennemførelsesretsakter, der yderligere præciserer de tilfælde, hvor en hændelse anses for at være væsentlig som omhandlet i stk. 3. Kommissionen kan vedtage sådanne gennemførelsesretsakter for så vidt angår andre væsentlige og vigtige enheder.

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

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

Artikel 24

Brug af europæiske cybersikkerhedscertificeringsordninger

1. For at påvise overensstemmelse med bestemte krav i artikel 21 kan medlemsstaterne kræve, at væsentlige og vigtige enheder bruger særlige IKT-produkter, -tjenester og -processer, der er udviklet af den væsentlige eller vigtige enhed eller indkøbt fra tredjeparter, og som er certificeret i henhold til europæiske cybersikkerhedscertificeringsordning, der er vedtaget i henhold til artikel 49 i forordning (EU) 2019/881. Endvidere skal medlemsstaterne tilskynde væsentlige og vigtige enheder til at anvende kvalificerede tillidstjenester.

2. Kommissionen tillægges beføjelser til at vedtage delegerede retsakter i overensstemmelse med artikel 38 for at supplere dette direktiv ved at præcisere, hvilke kategorier af væsentlige og vigtige enheder der skal anvende visse certificerede IKT-produkter, -tjenester og -processer eller indhente en attest i henhold til en europæisk cybersikkerhedscertificeringsordning, der er vedtaget i henhold til artikel 49 i forordning (EU) 2019/881. Disse delegerede retsakter vedtages, når der er identificeret utilstrækkelige cybersikkerhedsniveauer, og skal indeholde en gennemførelsesperiode.

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

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

Artikel 25

Standardisering

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

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

KAPITEL V

JURISDIKTION OG REGISTRERING

Artikel 26

Jurisdiktion og territorialitet

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

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

b) DNS-tjenesteudbydere, topdomænenavneadministratorer, enheder, der leverer domænenavnsregistreringstjenester, og udbydere af cloudcomputingtjenester, af datacentertjenester, af indholdsleveringsnetværk, af administrerede tjenester, af administrerede sikkerhedstjenester, af onlinemarkedspladser, af onlinesøgemaskiner eller af platforme for sociale netværkstjenester, som anses for at henhøre under jurisdiktionen i den medlemsstat, hvor de har deres hovedforretningssted i Unionen i henhold til stk. 2

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

2. Med henblik på dette direktiv anses en enhed som omhandlet i stk. 1, litra b), for at have sit hovedforretningssted i Unionen i den medlemsstat, hvor beslutningerne vedrørende foranstaltningerne til styring af cybersikkerhedsrisici overvejende træffes. Hvis en sådan medlemsstat ikke kan fastslås, eller hvis sådanne beslutninger ikke træffes i Unionen, anses hovedforretningsstedet for at være i den medlemsstat, hvor der udføres cybersikkerhedsoperationer. Hvis en sådan medlemsstat ikke kan fastslås, anses hovedforretningsstedet for at være i den medlemsstat, hvor den pågældende enheds forretningssted med det største antal ansatte i Unionen er beliggende.

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

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

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

Artikel 27

Register over enheder

1. ENISA opretter og fører et register over DNS-tjenesteudbydere, topdomænenavneadministratorer, enheder, der leverer domænenavnsregistreringstjenester, og udbydere af cloudcomputingtjenester, af datacentertjenester, af indholdsleveringsnetværk, af administrerede tjenester, af administrerede sikkerhedstjenester, af onlinemarkedspladser, af onlinesøgemaskiner og af platforme for sociale netværkstjenester på grundlag af de oplysninger, der modtages fra det centrale kontaktpunkt i overensstemmelse med stk. 4. Efter anmodning giver ENISA de kompetente myndigheder adgang til dette register, idet det i givet fald sikrer de nødvendige garantier til at beskytte fortroligheden af oplysninger.

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

a) enhedens navn

b) den relevante sektor og delsektor og typen af enhed, som i givet fald er omhandlet i bilag I eller II

c) adressen på enhedens hovedforretningssted og dens andre retlige forretningssteder i Unionen eller, hvis den ikke er etableret i Unionen, på den repræsentant, der er udpeget i henhold til artikel 26, stk. 3

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

e) de medlemsstater, hvor enheden leverer tjenester og

f) enhedens IP-intervaller.

3. Medlemsstaterne sikrer, at de i stk. 1 omhandlede enheder straks og under alle omstændigheder senest tre måneder efter den dato, hvor ændringen trådte i kraft, underretter den kompetente myndighed om enhver ændring af de oplysninger, de har indsendt i henhold til stk. 2.

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

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

Artikel 28

Database over domænenavnsregistreringsdata

1. Med henblik på at bidrage til DNS' sikkerhed, stabilitet og modstandsdygtighed pålægger medlemsstaterne topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester, med rettidig omhu at indsamle og vedligeholde nøjagtige og fuldstændige domænenavnsregistreringsdata i en særlig database i overensstemmelse med EU-databeskyttelsesretten for så vidt angår personoplysninger.

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

a) domænenavnet

b) registreringsdatoen

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

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

3. Medlemsstaterne stiller krav om, at topdomænenavneadministratorerne og de enheder, der leverer domænenavnsregistreringstjenester, har indført politikker og procedurer, herunder verifikationsprocedurer, for at sikre, at de i stk. 1 omhandlede databaser indeholder nøjagtige og fuldstændige oplysninger. Medlemsstaterne kræver, at sådanne politikker og procedurer gøres offentligt tilgængelige.

4. Medlemsstaterne pålægger topdomænenavneadministratorerne og de enheder, der leverer domænenavnsregistreringstjenester, uden unødigt ophold efter registreringen af et domænenavn at gøre domænenavnsregistreringsdata, som ikke er personoplysninger, offentligt tilgængelige.

5. Medlemsstaterne pålægger topdomænenavneadministratorerne og de enheder, der udbyder domænenavnsregistreringstjenester, at give adgang til specifikke domænenavnsregistreringsdata efter lovlige og behørigt begrundede anmodninger fra legitime adgangssøgende i overensstemmelse med EU-databeskyttelsesretten. Medlemsstaterne pålægger topdomænenavneadministratorerne og de enheder, der udbyder domænenavnsregistreringstjenester, at besvare anmodninger om adgang uden unødigt ophold og under alle omstændigheder inden for 72 timer efter modtagelse af anmodninger. Medlemsstaterne skal kræve, at sådanne politikker og procedurer gøres offentligt tilgængelige.

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

KAPITEL VI

UDVEKSLING AF OPLYSNINGER

Artikel 29

Ordninger for udveksling af cybersikkerhedsoplysninger

1. Medlemsstaterne sikrer, at enheder, der er omfattet af dette direktivs anvendelsesområde, og, hvor det er relevant, andre enheder, der ikke er omfattet af dette direktivs anvendelsesområde, på frivillig basis er i stand til at udveksle relevante cybersikkerhedsoplysninger indbyrdes, herunder oplysninger om cybertrusler, nærvedhændelser, sårbarheder, teknikker og procedurer, kompromitteringsindikatorer, fjendtlige taktikker, specifikke oplysninger vedrørende trusselsaktører, cybersikkerhedsadvarsler og anbefalinger vedrørende konfiguration af cybersikkerhedsværktøjer til opdagelse af cyberangreb, hvor sådan udveksling af oplysninger:

a) har til formål at forebygge, opdage, reagere på eller reetablere sig efter hændelser eller afbøde deres virkninger

b) øger cybersikkerhedsniveauet, navnlig ved at øge bevidstheden om cybertrusler, begrænse eller hindre sådanne truslers evne til at sprede sig, støtte en række forsvarskapaciteter, afhjælpe og offentliggøre sårbarheder, teknikker til opdagelse, begrænsning og forebyggelse af trusler, afbødningsstrategier eller indsats- og genopretningsfaser eller fremme samarbejde mellem offentlige og private enheder om forskning i trusler.

2. Medlemsstaterne sikrer, at udvekslingen af oplysninger finder sted inden for fællesskaber af væsentlige og vigtige enheder og, hvor det er relevant, deres leverandører eller tjenesteudbydere. En sådan udveksling skal gennemføres ved hjælp af ordninger for udveksling af cybersikkerhedsoplysninger for så vidt angår den potentielt følsomme karakter af de udvekslede oplysninger.

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

4. Medlemsstaterne sikrer, at væsentlige og vigtige enheder underretter de kompetente myndigheder om deres deltagelse i de i stk. 2 omhandlede ordninger for udveksling af cybersikkerhedsoplysninger, når de indtræder i sådanne ordninger, eller, i givet faldt, om deres udtræden af sådanne ordninger, når denne udtræden træder i kraft.

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

Artikel 30

Frivillig meddelelse af relevante oplysninger

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

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

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

2. Medlemsstaterne behandler de i denne artikels stk. 1 omhandlede underretninger i overensstemmelse med proceduren, der er fastsat i artikel 23. Medlemsstaterne kan prioritere behandling af obligatoriske underretninger frem for frivillige underretninger.

Hvor det er nødvendigt, giver CSIRT'erne og i givet fald de kompetente myndigheder det centrale kontaktpunkt de oplysninger om underretninger, de har modtaget i medfør af denne artikel, samtidig med at de sikrer fortroligheden og passende beskyttelse af de oplysninger, der er afgivet af den underrettende enhed. Uden at det berører forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger, må frivillig rapportering ikke medføre, at den underrettende enhed pålægges nogen yderligere forpligtelser, som den ikke ville være omfattet af, hvis den ikke havde foretaget underretningen.

KAPITEL VII

TILSYN OG HÅNDHÆVELSE

Artikel 31

Generelle aspekter vedrørende tilsyn og håndhævelse

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

2. Medlemsstaterne kan tillade deres kompetente myndigheder at prioritere tilsynsopgaver. En sådan prioritering baseres på en risikobaseret tilgang. Med henblik herpå kan de kompetente myndigheder, når de udfører deres tilsynsopgaver i henhold til artikel 32 og 33, fastlægge tilsynsmetoder, der gør det muligt at prioritere sådanne opgaver efter en risikobaseret tilgang.

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

4. Uden at det berører nationale lovgivningsmæssige og institutionelle rammer sikrer medlemsstaterne, at de kompetente myndigheder ved tilsynet med offentlige forvaltningsenheders overholdelse af dette direktiv og indførelsen af håndhævelsesforanstaltninger for så vidt angår overtrædelser af dette direktiv, har passende beføjelser til at udføre sådanne opgaver med operationel uafhængighed i forhold til de offentlige forvaltningsenheder, der føres tilsyn med. Medlemsstaterne kan beslutte at indføre passende, forholdsmæssige og effektive tilsyns- og håndhævelsesforanstaltninger over for disse enheder i overensstemmelse med de nationale lovgivningsmæssige og institutionelle rammer.

Artikel 32

Tilsyns- og håndhævelsesforanstaltninger vedrørende væsentlige enheder

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

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

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

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

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

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

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

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

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

De målrettede sikkerhedsaudits, der er omhandlet i første afsnit, litra b), baseres på risikovurderinger foretaget af den kompetente myndighed eller den reviderede enhed eller på andre tilgængelige risikorelaterede oplysninger.

Resultaterne af enhver målrettet sikkerhedsaudit stilles til rådighed for den kompetente myndighed. Omkostningerne ved en sådan målrettet sikkerhedsaudit, der udføres af et uafhængigt organ, afholdes af den reviderede enhed, undtagen i behørigt begrundede tilfælde når den kompetente myndighed bestemmer andet.

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

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

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

b) udstede bindende instrukser, herunder vedrørende foranstaltninger, der er nødvendige for at forhindre eller afhjælpe en hændelse, samt frister for gennemførelse af sådanne foranstaltninger og for rapportering om deres gennemførelse eller pålægge de pågældende enheder at afhjælpe de konstaterede mangler eller overtrædelserne af dette direktiv

c) pålægge de pågældende enheder at ophøre med at udvise adfærd, der overtræder dette direktiv, og afstå fra at gentage denne adfærd

d) pålægge de pågældende enheder, på en nærmere angivet måde og inden for en nærmere angivet frist, at sikre, at deres foranstaltninger til styring af cybersikkerhedsrisici overholder artikel 21, eller at efterleve underretningsforpligtelserne i artikel 23

e) pålægge de pågældende enheder at underrette de fysiske eller juridiske personer med hensyn til hvilke de leverer tjenester eller udfører aktiviteter, som potentielt er berørt af en væsentlig cybertrussel, om denne trussels karakter samt om eventuelle beskyttelsesforanstaltninger eller afhjælpende foranstaltninger, som disse fysiske eller juridiske personer kan træffe som reaktion på denne trussel

f) pålægge de pågældende enheder at gennemføre de anbefalinger, der er fremsat som følge af en sikkerhedsaudit, inden for en rimelig frist

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

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

i) pålægge, eller anmode de relevante organer eller domstole om i overensstemmelse med national ret at pålægge, en administrativ bøde i henhold til artikel 34 ud over enhver af de foranstaltninger, der er omhandlet i dette stykkes litra a)-h).

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

a) midlertidigt at suspendere, eller anmode et certificerings- eller godkendelsesorgan eller en domstol om i overensstemmelse med national ret midlertidigt at suspendere en certificering eller godkendelse vedrørende dele af eller alle de relevante tjenester, der leveres, eller aktiviteter, der udføres, af en væsentlig enhed

b) at anmode de relevante organer eller domstole om i overensstemmelse med national ret midlertidigt at forbyde enhver fysisk person med ledelsesansvar på direktionsniveau eller som juridisk repræsentant i den pågældende væsentlige enhed at udøve ledelsesfunktioner i den pågældende enhed.

Midlertidige suspensioner eller forbud, som er pålagt i henhold til dette stykke, anvendes kun, indtil den pågældende enhed træffer de nødvendige foranstaltninger til at afhjælpe manglerne eller opfylde den kompetente myndighed krav, som gav anledning til, at disse håndhævelsesforanstaltninger blev anvendt. Pålæggelse af sådanne midlertidige suspensioner eller forbud skal være underlagt passende proceduremæssige garantier i overensstemmelse med de generelle principper i EU-retten og chartret, herunder retten til effektive retsmidler og til en retfærdig rettergang, uskyldsformodningen og retten til et forsvar.

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

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

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

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

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

   i) gentagne overtrædelser

   ii) manglende underretning om eller afhjælpning af væsentlige hændelser

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

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

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

b) overtrædelsens varighed

c) den pågældende enheds relevante tidligere overtrædelser

d) enhver materiel eller immateriel skade, der er forårsaget, herunder ethvert finansielt eller økonomisk tab, virkninger for andre tjenester og antallet af brugere, der er berørt

e) hvorvidt gerningsmanden har begået overtrædelsen forsætligt eller uagtsomt

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

g) hvorvidt godkendte adfærdskodekser eller godkendte certificeringsmekanismer er overholdt

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

8. De kompetente myndigheder giver en detaljeret begrundelse for deres håndhævelsesforanstaltninger. Inden de kompetente myndigheder træffer sådanne foranstaltninger, underretter de berørte enheder om deres foreløbige resultater. De giver også disse enheder en rimelig frist til at fremsætte bemærkninger, undtagen i behørigt begrundede tilfælde, hvor øjeblikkelige foranstaltninger til at forebygge eller reagere på hændelser ellers ville blive hindret.

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

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

Artikel 33

Tilsyns- og håndhævelsesforanstaltninger vedrørende vigtige enheder

1. Når medlemsstaterne kommer i besiddelse af dokumentation for eller tegn på eller oplysninger om, at en vigtig enhed angiveligt ikke overholder dette direktiv, navnlig artikel 21 og 23 deri, sikrer de, at de kompetente myndigheder træffer foranstaltninger, hvor det er nødvendigt, gennem efterfølgende tilsynsforanstaltninger. Medlemsstaterne sikrer, at disse foranstaltninger er effektive, står i rimeligt forhold til overtrædelsen og har afskrækkende virkning under hensyntagen til omstændighederne i hver enkelt sag.

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

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

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

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

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

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

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

De målrettede sikkerhedsaudits, der er omhandlet i første afsnit, litra b), baseres risikovurderinger foretaget af den kompetente myndighed eller den reviderede enhed eller på andre tilgængelige risikorelaterede oplysninger.

Resultaterne af enhver målrettet sikkerhedsaudit stilles til rådighed for den kompetente myndighed. Omkostningerne ved en sådan målrettet sikkerhedsaudit, der udføres af et uafhængigt organ, afholdes af den reviderede enhed, undtagen i behørigt begrundede tilfælde når den kompetente myndighed bestemmer andet.

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

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

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

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

c) pålægge de pågældende enheder at ophøre med at udvise adfærd, der overtræder dette direktiv, og afstå fra at gentage denne adfærd

d) pålægge de pågældende enheder, på en nærmere angivet måde og inden for en nærmere angivet frist, at sikre, at deres foranstaltninger til styring af cybersikkerhedsrisici overholder artikel 21, eller at efterleve underretningsforpligtelserne i artikel 23

e) pålægge de pågældende enheder at underrette de fysiske eller juridiske personer med hensyn til hvilke de leverer tjenester eller udfører aktiviteter, som potentielt er berørt af en væsentlig cybertrussel, om denne trussels karakter samt om eventuelle beskyttelsesforanstaltninger eller afhjælpende foranstaltninger, som disse fysiske eller juridiske personer kan træffe som reaktion på denne trussel

f) pålægge de pågældende enheder at gennemføre de anbefalinger, der er fremsat som følge af en sikkerhedsaudit, inden for en rimelig frist

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

h) pålægge eller anmode de relevante organer eller domstole om i overensstemmelse med national ret at pålægge en administrativ bøde i henhold til artikel 34 ud over enhver af de foranstaltninger, der er omhandlet i dette stykkes litra a)-g).

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

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

Artikel 34

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

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

2. Administrative bøder pålægges i tillæg til en hvilken som helst af foranstaltningerne omhandlet i artikel 32, stk. 4, litra a)-h), artikel 32, stk. 5, og artikel 33, stk. 4, litra a)-g).

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

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

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

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

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

8. Hvis en medlemsstats retssystem ikke giver mulighed for at pålægge administrative bøder, sørger den pågældende medlemsstat for, at denne artikel anvendes på en sådan måde, at den kompetente myndighed tager skridt til bøder, og de kompetente nationale domstole pålægger dem, idet det sikres, at disse retsmidler er effektive, og at deres virkning svarer til virkningen af administrative bøder, som pålægges af de kompetente myndigheder. De bøder, der pålægges, skal under alle omstændigheder være effektive, stå i rimeligt forhold til overtrædelsen og have afskrækkende virkning. Medlemsstaten giver Kommissionen meddelelse om bestemmelserne i de love, som den vedtager i henhold til dette stykke, senest den 17. oktober 2024 og underretter den straks om eventuelle senere ændringslove eller ændringer, der berører dem.

Artikel 35

Overtrædelser, der medfører brud på persondatasikkerheden

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

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

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

Artikel 36

Sanktioner

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

Artikel 37

Gensidig bistand

1. Hvor en enhed leverer tjenester i mere end én medlemsstat, eller hvor den leverer tjenester i en eller flere medlemsstater og dens net- og informationssystemer er beliggende i en eller flere andre medlemsstater, samarbejder de kompetente myndigheder i de pågældende medlemsstater med og bistå hinanden efter behov. Dette samarbejde indebærer mindst, at:

a) de kompetente myndigheder, der anvender tilsyns- eller håndhævelsesforanstaltninger i en medlemsstat, via det fælles kontaktpunkt underretter og hører de kompetente myndigheder i de øvrige berørte medlemsstater om de tilsyns- og håndhævelsesforanstaltninger, der er truffet

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

c) en kompetent myndighed efter modtagelse af en begrundet anmodning fra en anden kompetent myndighed yder bistand til den anden kompetente myndighed, der står i et rimeligt forhold til dens egne ressourcer, således at tilsyns- eller håndhævelsesforanstaltningerne kan gennemføres på en effektiv, virkningsfuld og konsekvent måde.

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

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

KAPITEL VIII

DELEGEREDE RETSAKTER OG GENNEMFØRELSESRETSAKTER

Artikel 38

Udøvelse af de delegerede beføjelser

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

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

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

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

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

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

Artikel 39

Udvalgsprocedure

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

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

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

KAPITEL IX

AFSLUTTENDE BESTEMMELSER

Artikel 40

Evaluering

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

Artikel 41

Gennemførelse

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

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

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

Artikel 42

Ændringer af forordning (EU) nr. 910/2014

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

Artikel 43

Ændring af direktiv (EU) 2018/1972

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

Artikel 44

Ophævelse

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

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

Artikel 45

Ikrafttræden

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

Artikel 46

Adressater

Dette direktiv er rettet til medlemsstaterne.

Udfærdiget i Strasbourg, den 14. december 2022.

På Europa-Parlamentets vegne	*På Rådets vegne*
R. METSOLA	M. BEK
Formand	*Formand*

BILAG I

SEKTORER AF SÆRLIGT KRITISK BETYDNING

Sektor	Delsektor	Type enhed
1. Energi	a) Elektricitet	— Elektricitetsvirksomheder som defineret i artikel 2, nr. 57), i Europa-Parlamentets og Rådets direktiv (EU) 2019/944 ([1]), der varetager »levering« som defineret i nævnte direktivs artikel 2, nr. 12)
		— Distributionssystemoperatører som defineret i artikel 2, nr. 29), i direktiv (EU) 2019/944
		— Transmissionssystemoperatører som defineret i artikel 2, nr. 35), i direktiv (EU) 2019/944
		— Producenter som defineret i artikel 2, nr. 38), i direktiv (EU) 2019/944
		— Udpegede elektricitetsmarkedsoperatører som defineret i artikel 2, nr. 8), i Europa-Parlamentets og Rådets forordning (EU) 2019/943 ([2]) — Markedsdeltagere som defineret i artikel 2, nr. 25), i forordning (EU) 2019/943, der leverer tjenester, der vedrører aggregering, fleksibelt elforbrug eller energilagring som defineret i artikel 2, nr. 18), 20) og 59), i direktiv (EU) 2019/944 — Operatører af ladestationer, der er ansvarlige for forvaltningen og driften af en ladestation, som leverer en ladetjeneste til slutbrugere, herunder i en mobilitetstjenesteudbyders navn og på dennes vegne
	b) Fjernvarme og fjernkøling	— Operatører af fjernvarme eller fjernkøling som defineret i artikel 2, nr. 19), i Europa-Parlamentets og Rådets direktiv (EU) 2018/2001 ([3])
	c) Olie	— Olierørledningsoperatører
		— Operatører af olieproduktionsanlæg, -raffinaderier og -behandlingsanlæg, olielagre og olietransmission
		— Centrale lagerenheder som defineret i artikel 2, litra f), i Rådets direktiv 2009/119/EF ([4])
	d) Gas	— Forsyningsvirksomheder som defineret i artikel 2, nr. 8), i Europa-Parlamentets og Rådets direktiv 2009/73/EF ([5])
		— Distributionssystemoperatører som defineret i artikel 2, nr. 6), i direktiv 2009/73/EF
		— Transmissionssystemoperatører som defineret i artikel 2, nr. 4), i direktiv 2009/73/EF
		— Lagersystemoperatører som defineret i artikel 2, nr. 10), i direktiv 2009/73/EF
		— LNG-systemoperatører som defineret i artikel 2, nr. 12), i direktiv 2009/73/EF
		— Naturgasvirksomheder som defineret i artikel 2, nr. 1), i direktiv 2009/73/EF
		— Operatører af naturgasraffinaderier og -behandlingsanlæg
	e) Brint	— Operatører inden for brintproduktion, -lagring og -transmission

Sektor	Delsektor	Type enhed
2. Transport	a) Luft	— Luftfartsselskaber som defineret i artikel 3, nr. 4), i forordning (EF) nr. 300/2008, der anvendes til kommercielle formål
		— Lufthavnsdriftsorganer som defineret i artikel 2, nr. 2), i Europa-Parlamentets og Rådets direktiv 2009/12/EF ([6]), lufthavne som defineret i nævnte direktivs artikel 2, nr. 1), herunder de hovedlufthavne, der er anført i afsnit 2 i bilag II til Europa-Parlamentets og Rådets forordning (EU) nr. 1315/2013 ([7]); og enheder med tilknyttede anlæg i lufthavne
		— Trafikledelses- og kontroloperatører, der udøver flyvekontroltjenester som defineret i artikel 2, nr. 1), i Europa-Parlamentets og Rådets forordning (EF) nr. 549/2004 ([8])
	b) Jernbane	— Infrastrukturforvaltere som defineret i artikel 3, nr. 2), i Europa-Parlamentets og Rådets direktiv 2012/34/EU ([9])
		— Jernbanevirksomheder som defineret i artikel 3, nr. 1), i direktiv 2012/34/EU, herunder operatører af servicefaciliteter som defineret i nævnte direktivs artikel 3, nr. 12)
	c) Vand	— Rederier, som udfører passager- og godstransport ad indre vandveje, i højsøfarvand eller kystnært farvand som defineret for søtransport i bilag I til Europa-Parlamentets og Rådets forordning (EF) nr. 725/2004 ([10]), bortset fra de enkelte fartøjer, som drives af disse rederier
		— Driftsorganer i havne som defineret i artikel 3, nr. 1), i Europa-Parlamentets og Rådets direktiv 2005/65/EF ([11]), herunder deres havnefaciliteter som defineret i artikel 2, nr. 11), i forordning (EF) nr. 725/2004; og enheder, der opererer anlæg og udstyr i havne
		— Operatører af skibstrafiktjenester som defineret i artikel 3, litra o), i Europa-Parlamentets og Rådets direktiv 2002/59/EF ([12])
	d) Vejtransport	— Vejmyndigheder som defineret i artikel 2, nr. 12), i Kommissionens delegerede forordning (EU) 2015/962 ([13]), der er ansvarlige for trafikledelse, med undtagelse af offentlige enheder, for hvilke trafikledelse eller drift af intelligente transportsystemer er en ikkevæsentlig del af deres generelle aktivitet
		— Operatører af intelligente transportsystemer som defineret i artikel 4, nr. 1), i Europa-Parlamentets og Rådets direktiv 2010/40/EU ([14])
3. Bankvirksomhed		Kreditinstitutter som defineret i artikel 4, nr. 1), i Europa-Parlamentets og Rådets forordning (EU) nr. 575/2013 ([15])
4. Finansielle markedsinfrastrukturer		— Operatører af markedspladser som defineret i artikel 4, nr. 24), i Europa-Parlamentets og Rådets direktiv 2014/65/EU ([16])
		— Centrale modparter (CCP'er) som defineret i artikel 2, nr. 1), i Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012 ([17])

Sektor	Delsektor	Type enhed
5. Sundhed		— Sundhedstjenesteydere som defineret i artikel 3, litra g), i Europa-Parlamentets og Rådets direktiv 2011/24/EU ([18])
		— EU-referencelaboratorier, der er omhandlet i artikel 15, i Europa-Parlamentets og Rådets forordning (EU) 2022/2371 ([19])
		— Enheder, der udfører forsknings- og udviklingsaktiviteter vedrørende lægemidler som defineret i artikel 1, nr. 2), i Europa-Parlamentets og Rådets direktiv 2001/83/EF ([20]) — Enheder, der fremstiller farmaceutiske råvarer og farmaceutiske præparater som omhandlet i hovedafdeling C, hovedgruppe 21, i NACE rev. 2 — Enheder, som fremstiller medicinsk udstyr, som den anser for at være kritisk i en folkesundhedsmæssig krisesituation (»liste over kritisk medicinsk udstyr til folkesundhedsmæssige krisesituationer«) i den i artikel 22 i Europa-Parlamentets og Rådets forordning (EU) 2022/123 ([21]) anvendte betydning
6. Drikkevand		Leverandører og distributører af drikkevand som defineret i artikel 2, nr. 1), litra a), i Europa-Parlamentets og Rådets direktiv (EU) 2020/2184 ([22]) bortset fra distributører, for hvilke distribution af drikkevand er en ikkevæsentlig del af deres generelle aktivitet med distribution af andre råvarer og varer
7. Spildevand		Virksomheder, der indsamler, bortskaffer eller behandler byspildevand, husspildevand eller industrispildevand som defineret i artikel 2, nr. 1), 2) og 3), i Rådets direktiv 91/271/EØF ([23]), bortset fra virksomheder, for hvilke indsamling, bortskaffelse eller behandling af byspildevand, husspildevand eller industrispildevand er en ikkevæsentlig del af deres generelle aktivitet
8. Digital infrastruktur		— Udbydere af internetudvekslingspunkter
		— DNS-tjenesteudbydere, bortset fra operatører af rodnavneservere
		— Topdomænenavneadministratorer
		— Udbydere af cloudcomputingtjenester
		— Udbydere af datacentertjenester
		— Udbydere af indholdsleveringsnetværk
		— Tillidstjenesteudbydere
		— Udbydere af offentlige elektroniske kommunikationsnet
		— Udbydere af offentligt tilgængelige elektroniske kommunikationstjenester
9. Forvaltning af IKT-tjenester (business-to-business)		— Udbydere af administrerede tjenester — Udbydere af administrerede sikkerhedstjenester

Sektor	Delsektor	Type enhed
10. Offentlig forvaltning		— Offentlige forvaltningsenheder under den centrale forvaltning som defineret af en medlemsstat i overensstemmelse med national ret
		— Offentlige forvaltningsenheder på regionalt plan som defineret af en medlemsstat i overensstemmelse med national ret
11. Rummet		Operatører af jordbaseret infrastruktur, der ejes, forvaltes og drives af medlemsstater eller private parter, og som understøtter levering af rumbaserede tjenester, undtagen udbydere af offentlige elektroniske kommunikationsnet

([1]) Europa-Parlamentets og Rådets direktiv (EU) 2019/944 af 5. juni 2019 om fælles regler for det indre marked for elektricitet og om ændring af direktiv 2012/27/EU (EUT L 158 af 14.6.2019, s. 125).
([2]) Europa-Parlamentets og Rådets forordning (EU) 2019/943 af 5. juni 2019 om det indre marked for elektricitet (EUT L 158 af 14.6.2019, s. 54).
([3]) Europa-Parlamentets og Rådets direktiv (EU) 2018/2001 af 11. december 2018 om fremme af anvendelsen af energi fra vedvarende energikilder (EUT L 328 af 21.12.2018, s. 82).
([4]) Rådets direktiv 2009/119/EF af 14. september 2009 om forpligtelse for medlemsstaterne til at holde minimumslagre af råolie og/eller olieprodukter (EUT L 265 af 9.10.2009, s. 9).
([5]) Europa-Parlamentets og Rådets direktiv 2009/73/EF af 13. juli 2009 om fælles regler for det indre marked for naturgas og om ophævelse af direktiv 2003/55/EF (EUT L 211 af 14.8.2009, s. 94).
([6]) Europa-Parlamentets og Rådets direktiv 2009/12/EF af 11. marts 2009 om lufthavnsafgifter (EUT L 70 af 14.3.2009, s. 11).
([7]) Europa-Parlamentets og Rådets forordning (EU) nr. 1315/2013 af 11. december 2013 om Unionens retningslinjer for udvikling af det transeuropæiske transportnet og om ophævelse af afgørelse nr. 661/2010/EU (EUT L 348 af 20.12.2013, s. 1).
([8]) Europa-Parlamentets og Rådets forordning (EF) nr. 549/2004 af 10. marts 2004 om rammerne for oprettelse af et fælles europæisk luftrum (»rammeforordningen«) (EUT L 96 af 31.3.2004, s. 1).
([9]) Europa-Parlamentets og Rådets direktiv 2012/34/EU af 21. november 2012 om oprettelse af et fælles europæisk jernbaneområde (EUT L 343 af 14.12.2012, s. 32).
([10]) Europa-Parlamentets og Rådets forordning (EF) nr. 725/2004 af 31. marts 2004 om bedre sikring af skibe og havnefaciliteter (EUT L 129 af 29.4.2004, s. 6).
([11]) Europa-Parlamentets og Rådets direktiv 2005/65/EF af 26. oktober 2005 om bedre havnesikring (EUT L 310 af 25.11.2005, s. 28).
([12]) Europa-Parlamentets og Rådets direktiv 2002/59/EF af 27. juni 2002 om oprettelse af et trafikovervågnings- og trafikinformationssystem for skibsfarten i Fællesskabet og om ophævelse af Rådets direktiv 93/75/EØF (EFT L 208 af 5.8.2002, s. 10).
([13]) Kommissionens delegerede forordning (EU) 2015/962 af 18. december 2014 om supplerende regler til Europa-Parlamentets og Rådets direktiv 2010/40/EU for så vidt angår tilrådighedsstillelse af EU-dækkende tidstro trafikinformationstjenester (EUT L 157 af 23.6.2015, s. 21).
([14]) Europa-Parlamentets og Rådets direktiv 2010/40/EU af 7. juli 2010 om rammerne for indførelse af intelligente transportsystemer på vejtransportområdet og for grænsefladerne til andre transportformer (EUT L 207 af 6.8.2010, s. 1).
([15]) Europa-Parlamentets og Rådets forordning (EU) nr. 575/2013 af 26. juni 2013 om tilsynsmæssige krav til kreditinstitutter og om ændring af forordning (EU) nr. 648/2012 (EUT L 176 af 27.6.2013, s. 1).
([16]) Europa-Parlamentets og Rådets direktiv 2014/65/EU af 15. maj 2014 om markeder for finansielle instrumenter og om ændring af direktiv 2002/92/EF og direktiv 2011/61/EU (EUT L 173 af 12.6.2014, s. 349).
([17]) Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012 af 4. juli 2012 om OTC-derivater, centrale modparter og transaktionsregistre (EUT L 201 af 27.7.2012, s. 1).
([18]) Europa-Parlamentets og Rådets direktiv 2011/24/EU af 9. marts 2011 om patientrettigheder i forbindelse med grænseoverskridende sundhedsydelser (EUT L 88 af 4.4.2011, s. 45).

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

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

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

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

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

BILAG II

ANDRE KRITISKE SEKTORER

Sektor	Delsektor	Type enhed
1. Post- og kurertjenester		Postbefordrende virksomheder som defineret i artikel 2, nr. 1a), i direktiv 97/67/EF, herunder udbydere af kurertjenester
2. Affaldshåndtering		Virksomheder, der varetager affaldshåndtering som defineret i artikel 3, nr. 9), i Europa-Parlamentets og Rådets direktiv 2008/98/EF ([1]), bortset fra virksomheder, for hvilke affaldshåndtering ikke er deres vigtigste økonomiske aktivitet
3. Fremstilling, produktion og distribution af kemikalier		Virksomheder, der beskæftiger sig med fremstilling af stoffer og distribution af stoffer eller blandinger som omhandlet i artikel 3, nr. 9) og 14), i Europa-Parlamentets og Rådets forordning (EF) nr. 1907/2006 ([2]) og virksomheder, der beskæftiger sig med produktion af artikler som defineret i artikel 3, nr. 3), i nævnte forordning ud af stoffer eller blandinger
4. Produktion, tilvirkning og distribution af fødevarer		Fødevarevirksomheder som defineret i artikel 3, nr. 2), i Europa-Parlamentets og Rådets forordning (EF) nr. 178/2002 ([3]), der beskæftiger sig med engrosdistribution og industriel produktion og tilvirkning
5. Fremstilling	a) Fremstilling af medicinsk udstyr og medicinsk udstyr til in vitro-diagnostik	Enheder, der fremstiller medicinsk udstyr som defineret i artikel 2, nr. 1), i Europa-Parlamentets og Rådets forordning (EU) 2017/745 ([4]), og enheder, der fremstiller medicinsk udstyr til in vitro-diagnostik som defineret i artikel 2, nr. 2), i Europa-Parlamentets og Rådets forordning (EU) 2017/746 ([5]), med undtagelse af enheder, der fremstiller medicinsk udstyr omhandlet i dette direktivs bilag I, punkt 5, femte led
	b) Fremstilling af computere og elektroniske og optiske produkter	Virksomheder, der udøver en af de økonomiske aktiviteter, der er omhandlet i hovedafdeling C, hovedgruppe 26, i NACE rev. 2
	c) Fremstilling af elektrisk udstyr	Virksomheder, der udøver en af de økonomiske aktiviteter, der er omhandlet i hovedafdeling C, hovedgruppe 27, i NACE rev. 2
	d) Fremstilling af maskiner og udstyr i.a.n.	Virksomheder, der udøver en af de økonomiske aktiviteter, der er omhandlet i hovedafdeling C, hovedgruppe 28, i NACE rev. 2
	e) Fremstilling af motorkøretøjer, påhængsvogne og sættevogne	Virksomheder, der udøver en af de økonomiske aktiviteter, der er omhandlet i hovedafdeling C, hovedgruppe 29, i NACE rev. 2
	f) Fremstilling af andre transportmidler	Virksomheder, der udøver en af de økonomiske aktiviteter, der er omhandlet i hovedafdeling C, hovedgruppe 30, i NACE rev. 2

Sektor	Delsektor	Type enhed
6. Digitale udbydere		— Udbydere af onlinemarkedspladser
		— Udbydere af onlinesøgemaskiner
		— Udbydere af platforme for sociale netværkstjenester
7. Forskning		Forskningsorganisationer

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

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

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

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

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

BILAG III

SAMMENLIGNINGSTABEL

Direktiv (EU) 2016/1148	Nærværende direktiv
Artikel 1, stk. 1	Artikel 1, stk. 1
Artikel 1, stk. 2	Artikel 1, stk. 2
Artikel 1, stk. 3	—
Artikel 1, stk. 4	Artikel 2, stk. 12
Artikel 1, stk. 5	Artikel 2, stk. 13
Artikel 1, stk. 6	Artikel 2, stk. 6 og 11
Artikel 1, stk. 7	Artikel 4
Artikel 2	Artikel 2, stk. 14
Artikel 3	Artikel 5
Artikel 4	Artikel 6
Artikel 5	—
Artikel 6	—
Artikel 7, stk. 1	Artikel 7, stk. 1 og 2
Artikel 7, stk. 2	Artikel 7, stk. 4
Artikel 7, stk. 3	Artikel 7, stk. 3
Artikel 8, stk. 1-5	Artikel 8, stk. 1-5
Artikel 8, stk. 6	Artikel 13, stk. 4
Artikel 8, stk. 7	Artikel 8, stk. 6
Artikel 9, stk. 1, 2 og 3	Artikel 10, stk. 1, 2 og 3
Artikel 9, stk. 4	Artikel 10, stk. 9
Artikel 9, stk. 5	Artikel 10, stk. 10
Artikel 10, stk. 1, stk. 2 og stk. 3, første afsnit	Artikel 13, stk. 1, 2 og 3
Artikel 10, stk. 3, andet afsnit	Artikel 23, stk. 9
Artikel 11, stk. 1	Artikel 14, stk. 1 og 2
Artikel 11, stk. 2	Artikel 14, stk. 3
Artikel 11, stk. 3	Artikel 14, stk. 4, første afsnit, litra a)-q) og litra s), og stk. 7
Artikel 11, stk. 4	Artikel 14, stk. 4, første afsnit, litra r), og andet afsnit
Artikel 11, stk. 5	Artikel 14, stk. 8
Artikel 12, stk. 1-5	Artikel 15, stk. 1-5
Artikel 13	Artikel 17
Artikel 14, stk. 1 og 2	Artikel 21, stk. 1-4
Artikel 14, stk. 3	Artikel 23, stk. 1
Artikel 14, stk. 4	Artikel 23, stk. 3
Artikel 14, stk. 5	Artikel 23, stk. 5, 6 og 8

Direktiv (EU) 2016/1148	Nærværende direktiv
Artikel 14, stk. 6	Artikel 23, stk. 7
Artikel 14, stk. 7	Artikel 23, stk. 11
Artikel 15, stk. 1	Artikel 31, stk. 1
Artikel 15, stk. 2, første afsnit, litra a)	Artikel 32, stk. 2, litra e)
Artikel 15, stk. 2, første afsnit, litra b)	Artikel 32, stk. 2, litra g)
Artikel 15, stk. 2, andet afsnit	Artikel 32, stk. 3
Artikel 15, stk. 3	Artikel 32, stk. 4, litra b)
Artikel 15, stk. 4	Artikel 31, stk. 3
Artikel 16, stk. 1 og 2	Artikel 21, stk. 1-4
Artikel 16, stk. 3	Artikel 23, stk. 1
Artikel 16, stk. 4	Artikel 23, stk. 3
Artikel 16, stk. 5	—
Artikel 16, stk. 6	Artikel 23, stk. 6
Artikel 16, stk. 7	Artikel 23, stk. 7
Artikel 16, stk. 8 og 9	Artikel 21, stk. 5, og artikel 23, stk. 11
Artikel 16, stk. 10	—
Artikel 16, stk. 11	Artikel 2, stk. 1, 2 og 3
Artikel 17, stk. 1	Artikel 33, stk. 1
Artikel 17, stk. 2, litra a)	Artikel 32, stk. 2, litra e)
Artikel 17, stk. 2, litra b)	Artikel 32, stk. 4, litra b)
Artikel 17, stk. 3	Artikel 37, stk. 1, litra a) og b)
Artikel 18, stk. 1	Artikel 26, stk. 1, litra b), og stk. 2
Artikel 18, stk. 2	Artikel 26, stk. 3
Artikel 18, stk. 3	Artikel 26, stk. 4
Artikel 19	Artikel 25
Artikel 20	Artikel 30
Artikel 21	Artikel 36
Artikel 22	Artikel 39
Artikel 23	Artikel 40
Artikel 24	—
Artikel 25	Artikel 41
Artikel 26	Artikel 45
Artikel 27	Artikel 46
Bilag I, punkt 1	Artikel 11, stk. 1
Bilag I, punkt 2, litra a), nr. i)-iv)	Artikel 11, stk. 2, litra a)-d)

Direktiv (EU) 2016/1148	Nærværende direktiv
Bilag I, punkt 2, litra a), nr. v)	Artikel 11, stk. 2, litra f)
Bilag I, punkt 2, litra b)	Artikel 11, stk. 4
Bilag I, punkt 2, litra c), nr. i) og ii)	Artikel 11, stk. 5, litra a)
Bilag II	Bilag I
Bilag III, punkt 1 og 2	Bilag II, punkt 6
Bilag III, punkt 3	Bilag I, punkt 8

EUROPA-PARLAMENTETS OG RÅDETS DIREKTIV (EU) 2022/2556

af 14. december 2022

om ændring af direktiv 2009/65/EF, 2009/138/EF, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 og (EU) 2016/2341 for så vidt angår digital operationel modstandsdygtighed i den finansielle sektor

(EØS-relevant tekst)

EUROPA-PARLAMENTET OG RÅDET FOR DEN EUROPÆISKE UNION HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel 53, stk. 1, og artikel 114,

under henvisning til forslag fra Europa-Kommissionen,

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

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

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

efter den almindelige lovgivningsprocedure ([3]), og

ud fra følgende betragtninger:

(1) Unionen skal på fyldestgørende og fuldstændig vis imødegå digitale risici for alle finansielle enheder som følge af en øget anvendelse af informations- og kommunikationsteknologi (IKT) i forbindelse med levering og forbrug af finansielle tjenesteydelser og dermed bidrage til realisering af det potentiale, der ligger i digital finansiering med hensyn til at styrke innovation og fremmekonkurrence i et sikkert digitalt miljø.

(2) Finansielle enheder er stærkt afhængige af brugen af digitale teknologier i deres daglige aktiviteter. Det er derfor yderst vigtigt at sikre deres digitale aktiviteters operationelle modstandsdygtighed over for IKT-risiko. Dette behov er blevet endnu mere presserende på grund af væksten i banebrydende teknologier på markedet, og navnlig de teknologier, der skaber mulighed for, at digitale repræsentationer af værdier eller rettigheder, der skal overføres og lagres elektronisk ved hjælp af distributed ledger-teknologi eller lignende teknologi (kryptoaktiver), og i tjenesteydelser forbundet med disse aktiver.

([1]) EUT C 343 af 26.8.2021, s. 1.
([2]) EUT C 155 af 30.4.2021, s. 38.
([3]) Europa-Parlamentets holdning af 10.11.2022 (endnu ikke offentliggjort i EUT) og Rådets afgørelse af 28.11.2022.

(3) På EU-plan er kravene vedrørende styring af IKT-risikoen i den finansielle sektor fastsat i Europa-Parlamentets og Rådets direktiv 2009/65/EF ([4]), 2009/138/EF ([5]), 2011/61/EU ([6]), 2013/36/EU ([7]), 2014/59/EU ([8]), 2014/65/EU ([9]), (EU) 2015/2366 ([10]) og (EU) 2016/2341 ([11]).

Disse krav er forskellige og i nogle tilfælde ufuldstændige. I visse tilfælde er IKT-risikoen kun implicit omhandlet som en del af den operationelle risiko, og den er i andre overhovedet ikke omhandlet. Disse problemer udbedres ved vedtagelsen af Europa-Parlamentets og Rådets forordning (EU) 2022/2554 ([12]). Nævnte direktiver bør derfor ændres for at sikre overensstemmelse med nævnte forordning. Nærværende direktiv introducerer en række ændringer, som forekommer nødvendige for at skabe juridisk klarhed og sammenhæng, når finansielle enheder, som er meddelt tilladelse og underlagt tilsyn i overensstemmelse med nævnte direktiver, anvender forskellige krav vedrørende digital operationel modstandsdygtighed, som er nødvendige for udøvelsen af deres aktiviteter og leveringen af ydelser og dermed garanterer et velfungerende indre marked. Det er nødvendigt at sikre, at disse krav er tilstrækkelige i forhold til markedsudviklingen, samtidig med at der tilskyndes til proportionalitet, navnlig med hensyn til de finansielle enheders størrelse og de specifikke ordninger som de er omfattet af, med henblik på at reducere overholdelsesomkostningerne.

(4) På området for bankydelser fastsætter direktiv 2013/36/EU i øjeblikket kun generelle regler vedrørende intern ledelse og bestemmelser om operationel risiko, der omfatter krav vedrørende beredskabs- og kontinuitetsplaner, som implicit udgør grundlaget for håndtering af IKT-risiko. For at håndtere IKT-risiko eksplicit og tydeligt bør kravene vedrørende beredskabs- og kontinuitetsplaner imidlertid ændres, således at de også omfatter forretningskontinuitetsplaner samt planer for indsats- og genopretning vedrørende IKT-risiko i overensstemmelse med kravene i forordning (EU) 2022/2554. Desuden er IKT-risiko kun implicit medtaget, i forbindelse med operationelle risici, i den tilsynskontrol- og vurderingsproces (SREP), der udføres af de kompetente myndigheder, og kriterierne for vurderingen heraf er i øjeblikket fastlagt i Retningslinjer om IKT-risikovurdering under tilsynskontrol- og vurderingsprocessen (SREP), der er udsted af Den Europæiske Tilsynsmyndighed (Den Europæiske Banktilsynsmyndighed) (EBA), som blev oprettet ved Europa-Parlamentets og Rådets forordning (EU) nr. 1093/2010 ([13]). Med henblik på at skabe juridisk klarhed og sikre, at banktilsynsmyndighederne rent faktisk afdækker IKT-risiko og

([4]) Europa-Parlamentets og Rådets direktiv 2009/65/EF af 13. juli 2009 om samordning af love og administrative bestemmelser om visse institutter for kollektiv investering i værdipapirer (investeringsinstitutter) (EUT L 302 af 17.11.2009, s. 32).

([5]) Europa-Parlamentets og Rådets direktiv 2009/138/EF af 25. november 2009 om adgang til og udøvelse af forsikrings- og genforsikringsvirksomhed (Solvens II) (EUT L 335 af 17.12.2009, s. 1).

([6]) Europa-Parlamentets og Rådets direktiv 2011/61/EU af 8. juni 2011 om forvaltere af alternative investeringsfonde og om ændring af direktiv 2003/41/EF og 2009/65/EF samt forordning (EF) nr. 1060/2009 og (EU) nr. 1095/2010 (EUT L 174 af 1.7.2011, s. 1).

([7]) Europa-Parlamentets og Rådets direktiv 2013/36/EU af 26. juni 2013 om adgang til at udøve virksomhed som kreditinstitut og om tilsyn med kreditinstitutter og investeringsselskaber, om ændring af direktiv 2002/87/EF og om ophævelse af direktiv 2006/48/EF og 2006/49/EF (EUT L 176 af 27.6.2013, s. 338).

([8]) Europa-Parlamentets og Rådets direktiv 2014/59/EU af 15. maj 2014 om et regelsæt for genopretning og afvikling af kreditinstitutter og investeringsselskaber og om ændring af Rådets direktiv 82/891/EØF og Europa-Parlamentets og Rådets direktiv 2001/24/EF, 2002/47/EF, 2004/25/EF, 2005/56/EF, 2007/36/EF, 2011/35/EU, 2012/30/EU og 2013/36/EU samt forordning (EU) nr. 1093/2010 og (EU) nr. 648/2012 (EUT L 173 af 12.6.2014, s. 190).

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

([10]) Europa-Parlamentets og Rådets direktiv (EU) 2015/2366 af 25. november 2015 om betalingstjenester i det indre marked, og om ændring af direktiv 2002/65/EF, 2009/110/EF og 2013/36/EU og forordning (EU) nr. 1093/2010 og om ophævelse af direktiv 2007/64/EF (EUT L 337 af 23.12.2015, s. 35).

([11]) Europa-Parlamentets og Rådets direktiv (EU) 2016/2341 af 14. december 2016 om arbejdsmarkedsrelaterede pensionskassers (IORP'ers) aktiviteter og tilsynet hermed (EUT L 354 af 23.12.2016, s. 37).

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

([13]) Europa-Parlamentets og Rådets forordning (EU) nr. 1093/2010 af 24. november 2010 om oprettelse af en europæisk tilsynsmyndighed (Den Europæiske Banktilsynsmyndighed), om ændring af afgørelse nr. 716/2009/EF og om ophævelse af Kommissionens afgørelse 2009/78/EF (EUT L 331 af 15.12.2010, s. 12).

overvåger finansielle enheders styring heraf i overensstemmelse med den nye ramme for digital operationel modstandsdygtighed, bør anvendelsesområdet for SREP også ændres, så det eksplicit henviser til kravene i forordning (EU) 2022/2554 og navnlig dækker de risici, der afdækkes i indberetninger om større IKT-relaterede hændelser og af resultaterne af de test af den digitale operationelle modstandsdygtighed, som de finansielle enheder udfører i overensstemmelse med nævnte forordning.

(5) Digital operationel modstandsdygtighed er en væsentlig forudsætning for at opretholde en finansiel enheds kritiske funktioner og centrale forretningsområder i tilfælde af dens afvikling og derved undgå forstyrrelser af realøkonomien og i det finansielle system. Større operationelle hændelser kan hæmme en finansiel enheds evne til at fortsætte driften og kan true afviklingsmålene. Visse kontraktlige ordninger for brugen af IKT-tjenester er vigtige for at sikre operationel kontinuitet og at levere de nødvendige data i tilfælde af afvikling. Med henblik på tilpasning til målene i EU's ramme for operationel modstandsdygtighed bør direktiv 2014/59/EU ændres i overensstemmelse hermed for at sikre, at oplysninger vedrørende operationel modstandsdygtighed tages i betragtning i forbindelse med afviklingsplanlægning og vurdering af finansieringsenheders afviklingsmuligheder.

(6) Direktiv 2014/65/EU fastsætter kun strengere regler med hensyn til IKT-risiko for investeringsselskaber og markedspladser, der er involveret i algoritmisk handel. Der gælder mindre detaljerede krav for dataindberetningstjenester og transaktionsregistre. Direktiv 2014/65/EU omhandler også kun i begrænset omfang kontrol- og sikkerhedsforanstaltninger på edb-området og anvendelsen af passende systemer, ressourcer og procedurer til sikring af kontinuiteten og regelmæssigheden i forbindelse med erhvervstjenester. Desuden bør nævnte direktiv bringes i overensstemmelse med forordning (EU) 2022/2554 for så vidt angår kontinuitet og regelmæssighed i ydelsen af investeringsservice og udførelsen af investeringsaktiviteter, operationel modstandsdygtighed, handelssystemers kapacitet og effektivitet i forbindelse med ordninger til sikring af driftsstabilitet og risikostyring.

(7) Direktiv (EU) 2015/2366 fastsætter særlige regler for IKT-sikkerhedskontroller og begrænsende elementer med henblik på tilladelse til at udbyde betalingstjenester. Disse regler om tilladelse bør ændres, så de bliver bragt i overensstemmelse med forordning (EU) 2022/2554. For at mindske den administrative byrde og undgå kompleksitet og overlappende indberetningskrav bør reglerne om indberetning af hændelser i nævnte direktiv desuden ophøre med at finde anvendelse på betalingstjenesteudbydere, der reguleres i henhold til nævnte direktiv og også er omfattet af forordning (EU) 2022/2554, således at disse betalingstjenesteudbydere kan benytte sig af en fælles og fuldt ud harmoniseret mekanisme til indberetning af hændelser med hensyn til alle operationelle hændelser eller sikkerhedsmæssig betalingsrelaterede hændelser, uanset om sådanne hændelser er IKT-relaterede.

(8) Direktiv 2009/138/EF og (EU) 2016/2341 omfatter delvis IKT-risiko i de almindelige bestemmelser om ledelse og risikostyring, idet visse krav skal præciseres i delegerede retsakter med eller uden specifik henvisning til IKT-risiko. På tilsvarende vis er de regler, der finder anvendelse på forvaltere af alternative investeringsfonde som omhandlet i direktiv 2011/61/EU og administrationsselskaber som omhandlet i direktiv 2009/65/EF, udelukkende meget generelle. Nævnte direktiver bør derfor bringes i overensstemmelse med de krav, der er fastsat i forordning (EU) 2022/2554 for så vidt angår styringen af IKT-systemer og -værktøjer.

(9) I mange tilfælde er der allerede fastlagt krav til IKT-risiko i delegerede retsakter og gennemførelsesretsakter, som er vedtaget på grundlag af udkast til reguleringsmæssige tekniske standarder og udkast til gennemførelsesmæssige tekniske standarder, som er udviklet af den kompetente europæiske tilsynsmyndighed. Eftersom bestemmelserne i forordning (EU) 2022/2554 fremover udgør den retlige ramme for IKT-risiko i den finansielle sektor, bør visse beføjelser til at vedtage delegerede retsakter og gennemførelsesretsakter i direktiv 2009/65/EF, 2009/138/EF, 2011/61/EU og 2014/65/EU ændres, således at bestemmelserne om IKT-risiko fjernes fra anvendelsesområdet for de pågældende beføjelser.

(10) For at sikre en sammenhængende gennemførelse af den nye ramme for digital operationel modstandsdygtighed i den finansielle sektor, bør medlemsstaterne anvende bestemmelserne i national ret om gennemførelse af dette direktiv fra datoen for anvendelse af forordning (EU) 2022/2554.

(11) Direktiv 2009/65/EF, 2009/138/EF, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 og (EU) 2016/2341 er vedtaget på grundlag af artikel 53, stk. 1, eller artikel 114 i traktaten om Den Europæiske Unions funktionsmåde (TEUF), eller begge. Ændringerne i nærværende direktiv er blevet indarbejdet i én enkelt lovgivningsmæssig retsakt, da genstanden for og målene med ændringerne er indbyrdes forbundet. Nærværende direktiv bør derfor vedtages på grundlag af både artikel 53, stk. 1, og artikel 114 i TEUF.

(12) Målene for dette direktiv kan ikke i tilstrækkelig grad opfyldes af medlemsstaterne, da de indebærer harmonisering af krav, der allerede er indeholdt i direktiver, men kan på grund af foranstaltningens omfang og virkninger bedre nås på EU-plan; Unionen kan derfor vedtage foranstaltninger i overensstemmelse med nærhedsprincippet, jf. artikel 5 i traktaten om Den Europæiske Union. I overensstemmelse med proportionalitetsprincippet, jf. nævnte artikel, går dette direktiv ikke videre, end hvad der er nødvendigt for at nå disse mål.

(13) I henhold til den fælles politiske erklæring af 28. september 2011 fra medlemsstaterne og Kommissionen om forklarende dokumenter ([14]) har medlemsstaterne forpligtet sig til i tilfælde, hvor det er berettiget, at lade meddelelsen af gennemførelsesforanstaltninger ledsage af et eller flere dokumenter, der forklarer forholdet mellem et direktivs bestanddele og de tilsvarende dele i de nationale gennemførelsesinstrumenter. I forbindelse med dette direktiv finder lovgiver, at fremsendelse af sådanne dokumenter er berettiget —

VEDTAGET DETTE DIREKTIV:

Artikel 1

Ændringer af direktiv 2009/65/EF

I artikel 12 i direktiv 2009/65/EF foretages følgende ændringer:

1) Stk. 1, andet afsnit, litra a), affattes således:

»a) har en sund administrativ og regnskabsmæssig praksis, kontrol- og sikringsforanstaltninger på edb-området, herunder hvad angår net- og informationssystemer, som oprettes og styres i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) 2022/2554 (*), samt fyldestgørende interne kontrolprocedurer, herunder navnlig regler for de ansattes personlige transaktioner eller for besiddelse eller administration af investeringer i finansielle instrumenter med henblik på investering for egen regning, som mindst sikrer, at enhver transaktion, der implicerer investeringsinstituttet, kan rekonstrueres med hensyn til oprindelse, implicerede parter, art samt tid og sted for gennemførelsen, og at aktiver i investeringsinstitutter, der administreres af administrationsselskaber, investeres i overensstemmelse med fondsbestemmelserne eller vedtægterne og gældende ret

(*) 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).«

2) Stk. 3 affattes således:

»3. Uden at det berører artikel 116, vedtager Kommissionen ved hjælp af delegerede retsakter i overensstemmelse med artikel 112a, foranstaltninger, der fastlægger

a) de procedurer og de foranstaltninger, der er omhandlet i stk. 1, andet afsnit, litra a), bortset fra de procedurer og foranstaltninger, der vedrører net- og informationssystemer

b) de strukturer og organisatoriske krav med henblik på minimering af interessekonflikter, som er omhandlet i stk. 1, andet afsnit, litra b).«

([14]) EUT C 369 af 17.12.2011, s. 14.

Artikel 2

Ændringer af direktiv 2009/138/EF

I direktiv 2009/138/EF foretages følgende ændringer:

1) Artikel 41, stk. 4, affattes således:

»4. Forsikrings- og genforsikringsselskaber træffer passende foranstaltninger til at sikre kontinuitet og regelmæssighed i udøvelsen af deres virksomhed, inklusive udarbejdelse af beredskabsplaner. Selskabet anvender med henblik herpå hensigtsmæssige og rimeligt afpassede systemer, ressourcer og procedurer og opretter og styrer navnlig net- og informationssystemer i overensstemmelse med i Europa-Parlamentets og Rådets forordning (EU) 2022/2554 (*).

(*) 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).«

2) Artikel 50, stk. 1, litra a) og b), affattes således:

»a) elementerne i de systemer, der er omhandlet i artikel 41, artikel 44, navnlig de områder, der er omhandlet i artikel 44, stk. 2, og artikel 46 og 47, bortset fra de elementer, der vedrører risikostyring i forbindelse med informations- og kommunikationsteknologi

b) de funktioner, der er omhandlet i artikel 44, 46, 47 og 48, bortset fra de funktioner, der vedrører risikostyring i forbindelse med informations- og kommunikationsteknologi.«

Artikel 3

Ændring af direktiv 2011/61/EU

Artikel 18 i direktiv 2011/61/EU affattes således:

»*Artikel 18*

Generelle principper

1. Medlemsstaterne kræver, at FAIF'er til enhver tid anvender tilstrækkelige og egnede menneskelige og tekniske ressourcer for at sikre korrekt forvaltning af AIF'er.

Især skal de kompetente myndigheder i FAIF'ens hjemland under hensyntagen til karakteren af de AIF'er, der forvaltes af FAIF'en, kræve, at FAIF'en har sunde administrative og regnskabsmæssige praksis, kontrol- og sikringsforanstaltninger på edb-området, herunder hvad angår net- og informationssystemer, som oprettes og styres i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) 2022/2554 (*), samt fyldestgørende interne kontrolmekanismer, herunder navnlig regler for sine arbejdstageres personlige transaktioner eller for besiddelse eller forvaltning af investeringer med henblik på investering for egen regning, som mindst sikrer, at enhver transaktion, der implicerer AIF'er, kan rekonstrueres med hensyn til oprindelse, involverede parter, art samt tid og sted for gennemførelsen, og at aktiver i de AIF'er, som forvaltes af FAIF'en, investeres i overensstemmelse med AIF'ens regler eller vedtægter og gældende ret.

2. Kommissionen vedtager ved hjælp af delegerede retsakter i overensstemmelse med artikel 56 og på de i artikel 57 og 58 anførte betingelser foranstaltninger til præcisering af de procedurer og foranstaltninger, der er omhandlet i nærværende artikels stk. 1, bortset fra de procedurer og foranstaltninger, der vedrører net- og informationssystemer.

(*) 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).«

Artikel 4

Ændringer af direktiv 2013/36/EU

I direktiv 2013/36/EU foretages følgende ændringer:

1) Artikel 65, stk. 3, litra a), nr. vi), affattes således:

»vi) tredjeparter, som de enheder, der er omhandlet i nr. i)-iv), har outsourcet funktioner eller aktiviteter til, herunder tredjepartsudbydere af IKT-tjenester som omhandlet i kapitel V i Europa-Parlamentets og Rådets forordning (EU) 2022/2554 (*)

(*) 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).«

2) Artikel 74, stk. 1, første afsnit, affattes således:

»Institutter skal have robuste ledelsesordninger, hvilket omfatter en klar organisatorisk struktur med en veldefineret, gennemsigtig og konsekvent ansvarsfordeling og effektive procedurer til at identificere, styre, overvåge og indberette de risici, som institutterne er eller kan blive eksponeret for, fyldestgørende interne kontrolmekanismer, herunder en sund administrativ og regnskabsmæssig praksis samt net- og informationssystemer, der etableres og styres i overensstemmelse med forordning (EU) 2022/2554, og en aflønningspolitik og -praksis, som er i overensstemmelse med og fremmer en forsvarlig og effektiv risikostyring.«

3) Artikel 85, stk. 2, affattes således:

»2. De kompetente myndigheder sikrer, at institutterne råder over fyldestgørende beredskabs- og kontinuitetspolitikker og planer, herunder politikker og planer for IKT-driftsstabilitet og planer for IKT-indsats- og genopretning i forbindelse med den teknologi, som de anvender til formidling af oplysninger, og at disse planer udarbejdes, forvaltes og testes i overensstemmelse med artikel 11 i forordning (EU) 2022/2554, med henblik på at gøre det muligt for institutterne at videreføre driften i tilfælde af alvorlige driftsforstyrrelser og begrænse tab som følge af sådanne forstyrrelser.«

4) I artikel 97, stk. 1, tilføjes følgende litra:

»d) de risici, som afsløres ved test af digital operationel modstandsdygtighed i overensstemmelse med kapitel IV i forordning (EU) 2022/2554.«

Artikel 5

Ændringer af direktiv 2014/59/EU

I direktiv 2014/59/EU foretages følgende ændringer:

1) I artikel 10 foretages følgende ændringer:

a) Stk. 7, litra c), affattes således:

»c) en beskrivelse af, hvordan kritiske funktioner og centrale forretningsområder i nødvendigt omfang vil kunne adskilles juridisk og økonomisk fra andre funktioner for at sikre deres videreførelse og digitale operationelle modstandsdygtighed i tilfælde af, at instituttet bliver nødlidende«.

b) Stk. 7, litra q), affattes således:

»q) en beskrivelse af de aktiviteter og systemer, der har afgørende betydning for opretholdelsen af den fortsatte gennemførelse af instituttets operationelle procedurer, herunder net- og informationssystemer som omhandlet i Europa-Parlamentets og Rådets forordning (EU) 2022/2554 (*)

(*) 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).«

c) I stk. 9 tilføjes følgende afsnit:

»EBA gennemgår og ajourfører om nødvendigt de reguleringsmæssige tekniske standarder i overensstemmelse med artikel 10 i forordning (EU) nr. 1093/2010 for bl.a. at tage højde for bestemmelserne i kapitel II i forordning (EU) 2022/2554.«

2) I bilaget foretages følgende ændringer:

a) Afsnit A, punkt 16), affattes således:

»16) ordninger og foranstaltninger, som er nødvendige for at bevare den fortsatte drift af instituttets operationelle procedurer, herunder net- og informationssystemer, som oprettes og styres i overensstemmelse med forordning (EU) 2022/2554«.

b) I afsnit B foretages følgende ændringer:

i) Punkt 14) affattes således:

»14) identifikation af ejerne af de i punkt 13) anførte systemer, tilknyttede serviceleveranceaftaler og software og systemer eller licenser, herunder en oversigt pr. deres juridiske enheder, kritiske funktioner og centrale forretningsområder samt identifikation af kritiske tredjepartsudbydere af IKT-tjenester som defineret i artikel 3, nr. 23), i forordning (EU) 2022/2554«.

ii) Følgende punkt indsættes:

»14a) resultaterne af institutternes test af digital operationel modstandsdygtighed i henhold til forordning (EU) 2022/2554«.

c) I afsnit C foretages følgende ændringer:

i) Punkt 4) affattes således:

»4) hvorvidt de serviceaftaler, som instituttet har indgået, herunder kontraktlige ordninger for brugen af IKT-tjenester, er robuste og kan håndhæves fuldt ud i tilfælde af afvikling af instituttet«.

ii) Følgende punkt indsættes:

»4a) den digitale operationelle modstandsdygtighed for de net- og informationssystemer, der understøtter instituttets kritiske funktioner og centrale forretningsområder, under hensyntagen til indberetninger om større IKT-relaterede hændelser og resultaterne af test af digital operationel modstandsdygtighed i henhold til forordning (EU) 2022/2554«.

Artikel 6

Ændringer af direktiv 2014/65/EU

I direktiv 2014/65/EU foretages følgende ændringer:

1) I artikel 16 foretages følgende ændringer:

a) Stk. 4 affattes således:

»4. Et investeringsselskab skal, inden for rimelighedens grænser, træffe sådanne foranstaltninger, som måtte være nødvendige for at sikre kontinuitet og regelmæssighed i ydelsen af investeringsservice og udførelsen af investeringsaktiviteter. Investeringsselskabet anvender med henblik herpå hensigtsmæssige og forholdsmæssigt afpassede systemer, herunder informations- og kommunikationsteknologisystemer (»IKT-systemer«), som oprettes og styres i overensstemmelse med artikel 7 i Europa-Parlamentets og Rådets forordning (EU) 2022/2554 (*), samt hensigtsmæssige og forholdsmæssigt afpassede ressourcer og procedurer.

(*) 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).«

b) Stk. 5, andet og tredje afsnit, affattes således:

»Et investeringsselskab skal have en sund administrativ og regnskabsmæssig praksis, interne kontrolmekanismer og effektive procedurer til risikovurdering.

Uden at det berører kompetente myndigheders mulighed for at kræve adgang til kommunikation i overensstemmelse med dette direktiv og forordning (EU) nr. 600/2014 skal et investeringsselskab have etableret forsvarlige sikkerhedsmekanismer med henblik på i overensstemmelse med kravene i forordning (EU) 2022/2554 at garantere sikring og autentificering af midlerne til overførsel af information, at minimere risikoen for dataforvanskning og uautoriseret adgang og forhindre lækage af oplysninger, således at datasikkerheden garanteres til enhver tid.«

2) I artikel 17 foretages følgende ændringer:

a) Stk. 1 affattes således:

»1. Et investeringsselskab, der benytter sig af algoritmisk handel, skal have effektive systemer og risikokontrolforanstaltninger, som svarer til den virksomhed, som selskabet driver, med henblik på at sikre, at dets handelssystemer er modstandsdygtige og har tilstrækkelig kapacitet i overensstemmelse med kravene i kapitel II i forordning (EU) 2022/2554, er underlagt passende handelstærskler og -begrænsninger og forhindrer, at der afgives fejlagtige ordrer, eller at systemerne på anden måde fungerer dårligt, så det skaber eller bidrager til forstyrrelser på markedet.

Et sådant selskab skal også have effektive systemer og risikokontrolforanstaltninger med henblik på at sikre, at handelssystemerne ikke kan anvendes til formål, som strider mod forordning (EU) nr. 596/2014 eller mod de regler, der gælder for en markedsplads, som det er knyttet til.

Investeringsselskabet skal have effektive ordninger for forretningskontinuitet med henblik på at kunne håndtere en brist i dets handelssystemer, herunder politikker og planer for IKT-driftsstabilitet og planer for IKT-indsats- og genopretning, som er udarbejdet i overensstemmelse med artikel 11 i forordning (EU) 2022/2554, og skal desuden sørge for, at dets systemer er grundigt afprøvet og underlagt behørig overvågning med henblik på at sikre, at de opfylder kravene fastsat i dette stykke og eventuelle specifikke krav fastsat i kapitel II og IV i forordning (EU) 2022/2554.«

b) Stk. 7, litra a), affattes således:

»a) enkelthederne i de i stk. 1-6 fastsatte organisatoriske krav, bortset fra de organisatorisk krav, der vedrører IKT-risikostyring, som skal opfyldes af investeringsselskaber, som udfører forskellige former for investeringsservice, investeringsaktiviteter, accessoriske tjenesteydelser eller kombinationer heraf, hvorved præciseringerne vedrørende de organisatoriske krav i stk. 5 skal fastlægge de specifikke krav for direkte markedsadgang og sponsoreret adgang, således at det sikres, at kontrolforanstaltningerne i forbindelse med sponsoreret adgang mindst svarer til dem, der anvendes i forbindelse med direkte markedsadgang«.

3) I artikel 47, stk. 1, foretages følgende ændringer:

a) Litra b) affattes således:

»b) er tilstrækkelig rustet til at styre de risici, markedet udsættes for, herunder til at styre IKT-risiko i overensstemmelse med kapitel II i forordning (EU) 2022/2554, anvender fyldestgørende ordninger og systemer med henblik på at påvise væsentlige risici for markedets drift og har indført effektive foranstaltninger til at mindske disse risici«.

b) Litra c) udgår.

4) I artikel 48 foretages følgende ændringer:

a) Stk. 1 affattes således:

»1. Medlemsstaterne stiller krav om, at et reguleret marked skal etablere og opretholde sin operationelle modstandsdygtighed i overensstemmelse med kravene i kapitel II i forordning (EU) 2022/2554 for at sikre, at dets handelssystemer er modstandsdygtige, har tilstrækkelig kapacitet til at klare spidsbelastninger med hensyn til ordrer og meddelelser, kan sikre korrekt handel i tilfælde af alvorlig markedsstress, er fuldt gennemprøvede for at sikre, at sådanne betingelser er opfyldt, og er omfattet af effektive ordninger til sikring af driftsstabilitet, herunder politikker og planer for IKT-driftsstabilitet og planer for IKT-indsats- og genopretning udarbejdet i overensstemmelse med artikel 11 i forordning (EU) 2022/2554, til at sikre opretholdelsen af markedets tjenester i tilfælde af et svigt af dets handelssystemer.«

b) Stk. 6 affattes således:

»6. Medlemsstaterne stiller krav om, at et reguleret marked skal have etableret effektive systemer, procedurer og ordninger, som bl.a. kræver, at medlemmer eller deltagere gennemfører passende test af algoritmer, og skaber rammer, der letter en sådan test i overensstemmelse med kravene i kapital II og IV i forordning (EU) 2022/2554 til at sikre, at algoritmiske handelssystemer ikke kan skabe eller bidrage til ureglementerede handelsvilkår på markedet og til at håndtere eventuelle ureglementerede handelsvilkår, der opstår på grund af sådanne algoritmiske handelssystemer, herunder systemer, der begrænser forholdet mellem ikkeudførte ordrer og transaktioner, der kan indføres i systemet af et medlem eller en deltager, således at det bliver muligt at bremse ordrestrømmen, hvis der er risiko for, at man når op på systemets maksimale kapacitet, og at den minimumskursændring (tick size), der kan anvendes på markedet, begrænses og håndhæves.«

c) I stk. 12 foretages følgende ændringer:

i) Litra a) affattes således:

»a) forpligtelserne til at sikre, at regulerede markeders handelssystemer er fleksible og har en tilstrækkelig kapacitet, med undtagelse af de forpligtelser, som vedrører digital operationel modstandsdygtighed«.

ii) Litra g) affattes således:

»g) forpligtelserne til at sikre passende test af algoritmer, bortset fra test af digital operationel modstandsdygtighed, med henblik på at sikre, at algoritmiske handelssystemer, herunder algoritmiske højfrekvenshandelssystemer, ikke kan skabe eller bidrage til ureglementerede handelsvilkår på markedet.«

Artikel 7

Ændring af direktiv (EU) 2015/2366

I direktiv (EU) 2015/2366 foretages følgende ændringer:

1) Artikel 3, litra j), affattes således:

»j) tjenester leveret af udbydere af tekniske tjenester, der understøtter udbuddet af betalingstjenester, uden at udbyderne på noget tidspunkt kommer i besiddelse af de midler, som skal overføres, herunder behandling og lagring af data, tillidsskabende tjenester og tjenester til beskyttelse af privatlivets fred, autentifikation af data og enheder, levering af informations- og kommunikationsteknologi (IKT) og kommunikationsnetværk, levering og vedligeholdelse af terminaler og anordninger til brug for betalingstjenester, med undtagelse af betalingsinitieringstjenester og kontooplysningstjenester«.

2) I artikel 5, stk. 1, foretages følgende ændringer:

a) I første afsnit foretages følgende ændringer:

i) Litra e) affattes således:

»e) en beskrivelse af ansøgerens forvaltningsordninger og interne kontrolmekanismer, herunder administrative, risikostyringsmæssige og regnskabsmæssige procedurer samt ordninger for brug af IKT-tjenester i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) 2022/2554 (*), der dokumenterer, at disse forvaltningsordninger og interne kontrolmekanismer er proportionale, passende, forsvarlige og tilstrækkelige

(*) 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).«

ii) Litra f) affattes således:

»f) en beskrivelse af den procedure, der er indført for at håndtere og følge op på sikkerhedshændelser og sikkerhedsrelaterede kundeklager, herunder en ordning for indberetning af hændelser, hvori der er taget højde for betalingsinstituttets indberetningsforpligtelser, jf. kapitel III i forordning (EU) 2022/2554«.

iii) Litra h) affattes således:

»h) en beskrivelse af ordningerne for forretningskontinuitet, herunder en klar fastlæggelse af de kritiske funktioner, effektive politikker og planer for IKT-driftsstabilitet og planer for IKT-indsats- og genopretning og en procedure til regelmæssigt at teste og evaluere, om sådanne planer er tilstrækkelige og effektive, i overensstemmelse med forordning (EU) 2022/2554«.

b) Tredje afsnit affattes således:

»Det skal i tilknytning til de i første afsnits litra j) omhandlede sikkerhedskontrolforanstaltninger og begrænsende foranstaltninger angives, hvordan de sikrer et højt niveau af digital operationel modstandsdygtighed i overensstemmelse med kapitel II i forordning (EU) 2022/2554, navnlig med hensyn til teknisk sikkerhed og databeskyttelse, herunder vedrørende de software- og IKT-systemer, der anvendes af ansøgeren eller de virksomheder, som ansøgeren outsourcer hele eller dele af sine aktiviteter til. Disse foranstaltninger skal også omfatte de sikkerhedsforanstaltninger, der er fastsat i dette direktivs artikel 95, stk. 1. Foranstaltningerne skal tage højde for EBA's retningslinjer om sikkerhedsforanstaltninger som omhandlet i dette direktivs artikel 95, stk. 3, når de foreligger.«

3) Artikel 19, stk. 6, andet afsnit, affattes således:

»Vigtige driftsmæssige funktioner, herunder IKT-systemer, må ikke outsources på en måde, der i væsentlig grad forringer kvaliteten af betalingsinstituttets interne kontrol og de kompetente myndigheders mulighed for at kunne overvåge og spore, om betalingsinstituttet overholder alle forpligtelserne i dette direktiv.«

4) I artikel 95, stk. 1, tilføjes følgende afsnit:

»Første afsnit berører ikke anvendelsen af kapitel II i forordning (EU) 2022/2554 på:

a) betalingstjenesteudbydere som omhandlet i dette direktivs artikel 1, stk. 1, litra a), b) og d)

b) kontooplysningstjenesteudbydere, jf. dette direktivs artikel 33, stk. 1

c) betalingsinstitutter, der er undtaget i henhold til dette direktivs artikel 32, stk. 1, og

d) e-pengeinstitutter, der er omfattet af en undtagelse, som omhandlet i artikel 9, stk. 1, i direktiv 2009/110/EF.«

5) I artikel 96 tilføjes følgende stykke:

»7. Medlemsstaterne sikrer, at nærværende artikels stk. 1-5 ikke finder anvendelse på:

a) betalingstjenesteudbydere som omhandlet i dette direktivs artikel 1, stk. 1, litra a), b) og d)

b) kontooplysningstjenesteudbydere, jf. dette direktivs artikel 33, stk. 1

c) betalingsinstitutter, der er undtaget i henhold til dette direktivs artikel 32, stk. 1, og

d) e-pengeinstitutter, der er omfattet af en undtagelse som omhandlet i artikel 9, stk. 1, i direktiv 2009/110/EF.«

6) Artikel 98, stk. 5, affattes således:

»5. EBA gennemgår og ajourfører om nødvendigt regelmæssigt de reguleringsmæssige tekniske standarder i overensstemmelse med artikel 10 i forordning (EU) nr. 1093/2010 for bl.a. at tage højde for innovation og den teknologiske udvikling og for bestemmelserne i kapitel II i forordning (EU) 2022/2554.«

Artikel 8

Ændring af direktiv (EU) 2016/2341

Artikel 21, stk. 5, i direktiv (EU) 2016/2341 affattes således:

»5. Medlemsstaterne sikrer, at IORP'er træffer passende foranstaltninger til at sikre kontinuitet og regelmæssighed i udøvelsen af deres virksomhed, herunder udarbejdelse af beredskabsplaner. IORP'er anvender med henblik herpå

hensigtsmæssige og rimeligt afpassede systemer, ressourcer og procedurer og opretter og styrer navnlig net- og informationssystemer i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) 2022/2554 (*), hvis det er relevant.

(*) 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).«

Artikel 9

Gennemførelse

1. Medlemsstaterne vedtager og offentliggør senest den 17. januar 2025 de bestemmelser, der er nødvendige for at efterkomme dette direktiv. De underretter straks Kommissionen herom.

De anvender disse bestemmelser fra den 17. januar 2025.

Disse bestemmelser skal ved vedtagelsen indeholde en henvisning til dette direktiv eller skal ved offentliggørelsen ledsages af en sådan henvisning. De nærmere regler for henvisningen fastsættes af medlemsstaterne.

2. Medlemsstaterne meddeler Kommissionen teksten til de vigtigste nationale love og bestemmelser, som de udsteder på det område, der er omfattet af dette direktiv.

Artikel 10

Ikrafttræden

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

Artikel 11

Adressater

Dette direktiv er rettet til medlemsstaterne.

Udfærdiget i Strasbourg, den 14. december 2022.

På Europa-Parlamentets vegne	*På Rådets vegne*
R. METSOLA	M. BEK
Formand	*Formand*

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

(EØS-relevant tekst)

EUROPA-PARLAMENTET OG RÅDET FOR DEN EUROPÆISKE UNION HAR —

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

under henvisning til forslag fra Europa-Kommissionen,

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

under henvisning til udtalelse fra Det Europæiske Økonomiske og Sociale Udvalg ([1]),

under henvisning til udtalelse fra Regionsudvalget ([2]),

efter den almindelige lovgivningsprocedure ([3]), og

ud fra følgende betragtninger:

(1) Kritiske enheder spiller som leverandører af væsentlige tjenester en uundværlig rolle med hensyn til opretholdelse af vitale samfundsmæssige funktioner eller økonomiske aktiviteter på det indre marked i en stadig mere indbyrdes afhængig EU-økonomi. Det er derfor vigtigt at fastlægge en EU-ramme med det formål at både styrke kritiske enheders modstandsdygtighed på det indre marked ved at fastsætte harmoniserede minimumsregler og bistå dem gennem sammenhængende og målrettede støtte- og tilsynsforanstaltninger.

(2) Rådets direktiv 2008/114/EF ([4]) indeholder bestemmelser om en procedure for udpegning af europæisk kritisk infrastruktur i energi- og transportsektoren, hvis forstyrrelse eller ødelæggelse vil få betydelig grænseoverskridende indvirkning på mindst to medlemsstater. Nævnte direktiv fokuserer udelukkende på beskyttelse af sådan infrastruktur. Den evaluering af direktiv 2008/114/EF, der blev foretaget i 2019, viste imidlertid, at på grund af den stadig mere indbyrdes forbundne og grænseoverskridende karakter af operationer, der anvender kritisk infrastruktur, er beskyttelsesforanstaltninger vedrørende individuelle aktiver i sig selv utilstrækkelige til at forhindre alle forstyrrelser. Det er derfor nødvendigt at ændre tilgangen til sikring af, at der tages bedre hensyn til risici, at kritiske enheders rolle og opgaver som leverandører af tjenester, der er væsentlige for det indre markeds funktion, defineres bedre og er sammenhængende, og at der vedtages EU-regler for at styrke kritiske enheders modstandsdygtighed.

([1]) EUT C 286 af 16.7.2021, s. 170.
([2]) EUT C 440 af 29.10.2021, s. 99.
([3]) Europa-Parlamentets holdning af 22.11.2022 (endnu ikke offentliggjort i EUT) og Rådets afgørelse af 8.12.2022.
([4]) Rådets direktiv 2008/114/EF af 8. december 2008 om indkredsning og udpegning af europæisk kritisk infrastruktur og vurdering af behovet for at beskytte den bedre (EUT L 345 af 23.12.2008, s. 75).

Kritiske enheder bør være i stand til at styrke deres evne til at forebygge, beskytte mod, reagere på, modstå, afbøde, absorbere, tilpasse sig til og komme på fode igen efter hændelser, der har potentiale til at forstyrre leveringen af væsentlige tjenester.

(3) Selv om en række foranstaltninger på EU-plan, såsom det europæiske program for beskyttelse af kritisk infrastruktur, og på nationalt plan har til formål at støtte beskyttelsen af kritisk infrastruktur i Unionen, bør der gøres mere for bedre at udstyre de enheder, der driver sådan infrastruktur, til at håndtere risiciene for deres drift, som kunne føre til forstyrrelse i leveringen af væsentlige tjenester. Der bør også gøres mere for bedre at udstyre sådanne enheder, da der foreligger et dynamisk trusselsbillede, der omfatter voksende hybride trusler og terrortrusler, og voksende indbyrdes afhængighed mellem infrastruktur og sektorer. Desuden er der en øget fysisk risiko som følge af naturkatastrofer og klimaændringer, hvilket intensiverer hyppigheden og omfanget af ekstreme vejrforhold og medfører langsigtede ændringer i de gennemsnitlige klimaforhold, der kan reducere visse infrastrukturtypers kapacitet, effektivitet og levetid, hvis foranstaltninger til klimatilpasning ikke er på plads. Endvidere er det indre marked kendetegnet ved fragmentering med hensyn til identifikation af kritiske enheder, fordi relevante sektorer og kategorier af enheder ikke anerkendes konsekvent som kritiske i alle medlemsstaterne. Dette direktiv bør derfor opnå et solidt harmoniseringsniveau med hensyn til de sektorer og kategorier af enheder, der er omfattet af dets anvendelsesområde.

(4) Visse sektorer af økonomien, såsom energi- og transportsektorerne, er allerede reguleret gennem sektorspecifikke EU-retsakter, men disse retsakter indeholder bestemmelser, der kun vedrører visse aspekter af modstandsdygtigheden af enheder, som opererer inden for disse sektorer. For at håndtere modstandsdygtigheden af de enheder, der er kritiske for et velfungerende indre marked, på en omfattende måde skaber dette direktiv en overordnet ramme, der tager højde for kritiske enheders modstandsdygtighed over for alle farer, hvad enten de er naturlige eller menneskeskabte, hændelige eller tilsigtede.

(5) Den voksende indbyrdes afhængighed mellem infrastruktur og sektorer er resultatet af et stadig mere grænseoverskridende og indbyrdes afhængigt net af tjenester, der anvender nøgleinfrastruktur i hele Unionen, i sektorerne energi, transport, bankvæsen, drikkevand, spildevand, produktion, tilvirkning og distribution af fødevarer, sundhed, rummet, finansiel markedsinfrastruktur og digital infrastruktur samt i visse aspekter af sektoren for offentlig forvaltning. Rumsektoren er omfattet af dette direktivs anvendelsesområde med hensyn til levering af visse tjenester, der er afhængige af jordbaseret infrastruktur, som ejes, forvaltes og drives af enten medlemsstaterne eller private parter; derfor er infrastruktur, der ejes, forvaltes eller drives af eller på vegne af Unionen som led i dens rumprogram, ikke omfattet af dette direktivs anvendelsesområde.

Hvad angår energisektoren og navnlig metoderne til produktion og transmission af elektricitet (med hensyn til elforsyning), er det underforstået, at elproduktion, for så vidt det skønnes hensigtsmæssigt, kan inkludere eltransmissionsdele af kernekraftværker uden at inkludere de specifikt nukleare elementer, der er omfattet af traktater og EU-retten, herunder relevante EU-retsakter vedrørende kernekraft. Processen for identifikation af kritiske enheder i fødevaresektoren bør på passende vis afspejle det indre markeds karakter i denne sektor og de omfattende EU-regler vedrørende de generelle principper og krav for fødevareret og fødevaresikkerhed. For at sikre, at der er en forholdsmæssig tilgang og for på passende vis at afspejle disse enheders rolle og betydning på nationalt plan bør kritiske enheder derfor kun identificeres blandt fødevarevirksomheder, hvad enten de er med eller uden gevinst for øje, og uanset om de er offentlige eller private, som udelukkende beskæftiger sig med logistik, engrosdistribution og industriel produktion og tilvirkning i stor skala med en betydelig markedsandel som observeret på nationalt plan. Disse indbyrdes afhængighedsforhold betyder, at enhver forstyrrelse af væsentlige tjenester, selv en, der oprindeligt var begrænset til én enhed eller én sektor, kan have kaskadevirkninger mere generelt, hvilket potentielt kan føre til en vidtrækkende og langsigtet negativ indvirkning på leveringen af tjenester på hele det indre marked. Store kriser, såsom covid-19-pandemien, har vist, at vores stadig mere indbyrdes afhængige samfund er sårbare over for risici med stor indvirkning og lav sandsynlighed.

(6) De enheder, der er involveret i levering af væsentlige tjenester, er i stigende grad underlagt forskellige krav i henhold til national ret. Det forhold, at nogle medlemsstater stiller mindre strenge sikkerhedskrav til disse enheder, fører ikke kun til forskellige grader af modstandsdygtighed, men risikerer også at have negativ indvirkning på opretholdelsen af vitale samfundsmæssige funktioner eller økonomiske aktiviteter i hele Unionen og fører til hindringer for et velfungerende indre marked. Investorer og virksomheder kan støtte sig til og stole på kritiske enheder, der er modstandsdygtige, og pålidelighed og tillid er hjørnestenene i et velfungerende indre marked. Enheder af samme type betragtes som kritiske i nogle medlemsstater, men ikke i andre, og de enheder, der er identificeret som kritiske, er underlagt forskellige krav i forskellige medlemsstater. Dette medfører en yderligere og unødvendig administrativ byrde for virksomheder, der opererer på tværs af grænserne, navnlig for virksomheder, der er aktive i medlemsstater med strengere krav. En EU-ramme vil derfor også skabe lige konkurrencevilkår for kritiske enheder i hele Unionen.

(7) Det er nødvendigt at fastsætte harmoniserede minimumsregler for at sikre leveringen af væsentlige tjenester på det indre marked, styrke kritiske enheders modstandsdygtighed og forbedre det grænseoverskridende samarbejde mellem kompetente myndigheder. Det er vigtigt, at disse regler er fremtidssikrede med hensyn til udformning og gennemførelse, samtidig med at der gives mulighed for den nødvendige fleksibilitet. Det er også afgørende at forbedre kritiske enheders kapacitet til at levere væsentlige tjenester i lyset af en række forskellige risici.

(8) For at opnå en høj grad af modstandsdygtighed bør medlemsstaterne identificere kritiske enheder, som vil være underlagt specifikke krav og specifikt tilsyn og som vil ydes særlig støtte og vejledning over for alle relevante risici.

(9) I betragtning af betydning af cybersikkerhed for kritiske enheders modstandsdygtighed og af hensyn til konsistens bør der i videst muligt omfang sikres en sammenhængende tilgang mellem dette direktiv og Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 ([5]). I lyset af cyberrisicis øgede hyppighed og særlige karakteristika pålægger direktiv (EU) 2022/2555 en lang række enheder omfattende krav for at sikre deres cybersikkerhed. Da cybersikkerhed behandles tilstrækkeligt i direktiv (EU) 2022/2555, bør de spørgsmål, der er omfattet af nævnte direktiv, udelukkes fra nærværende direktivs anvendelsesområde, uden at det berører den særlige ordning for enheder i sektoren for digital infrastruktur.

(10) Hvor bestemmelser i sektorspecifikke EU-retsakter kræver, at kritiske enheder træffer foranstaltninger for at styrke deres modstandsdygtighed, og hvor disse krav er anerkendt af medlemsstaterne som svarende mindst til de tilsvarende forpligtelser i dette direktiv, bør de relevante bestemmelser i dette direktiv ikke finde anvendelse for at undgå dobbeltarbejde og unødvendige byrder. I så fald bør de relevante bestemmelser i sådanne EU-retsakter finde anvendelse. Hvis de relevante bestemmelser i dette direktiv ikke finder anvendelse, bør bestemmelserne om tilsyn og håndhævelse i dette direktiv heller ikke finde anvendelse.

(11) Dette direktiv berører ikke medlemsstaternes og deres myndigheders kompetencer med hensyn til administrativ autonomi eller deres ansvar for at varetage national sikkerhed og forsvar eller deres beføjelse til at varetage andre væsentlige statslige funktioner, navnlig vedrørende offentlig sikkerhed, territorial integritet og opretholdelse af lov og orden. Udelukkelsen af offentlige forvaltningsenheder fra dette direktivs anvendelsesområde bør gælde for enheder, hvis aktiviteter hovedsageligt udføres på områderne national sikkerhed, offentlig sikkerhed, forsvar eller retshåndhævelse, herunder efterforskning, afsløring og retsforfølgning af strafbare handlinger. Offentlige forvaltningsenheder, hvis aktiviteter kun er marginalt relateret til disse områder, bør dog være omfattet af dette direktivs anvendelsesområde. Med henblik på dette direktiv anses enheder med reguleringsbeføjelser ikke for at udføre aktiviteter inden for retshåndhævelse, og de er derfor ikke på dette grundlag udelukket fra dette direktivs anvendelsesområde. Offentlige forvaltningsenheder, der er etableret i fællesskab med et tredjeland i overensstemmelse med en international aftale, er udelukket fra dette direktivs anvendelsesområde. Dette direktiv finder ikke anvendelse på medlemsstaternes diplomatiske og konsulære missioner i tredjelande.

([5]) 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-direktiv) (se side 80 i denne EUT).

Visse kritiske enheder udfører aktiviteter på områderne national sikkerhed, offentlig sikkerhed, forsvar eller retshåndhævelse, herunder efterforskning, afsløring og retsforfølgning af strafbare handlinger, eller leverer udelukkende tjenester til offentlige forvaltningsenheder, der hovedsageligt udfører aktiviteter på disse områder. I betragtning af medlemsstaternes ansvar for at varetage national sikkerhed og forsvar bør medlemsstater kunne beslutte, at kritiske enheders forpligtelser fastsat i dette direktiv helt eller delvist ikke finder anvendelse på disse kritiske enheder, hvis de tjenester, som de leverer, eller de aktiviteter, som de udfører, hovedsageligt vedrører områderne national sikkerhed, offentlig sikkerhed, forsvar eller retshåndhævelse, herunder efterforskning, afsløring og retsforfølgning af strafbare handlinger. Kritiske enheder, hvis tjenester eller aktiviteter kun er marginalt relaterede til disse områder, bør stadig være omfattet af dette direktivs anvendelsesområde. Ingen medlemsstat bør være forpligtet til at meddele oplysninger, hvis videregivelse vil stride mod væsentlige interesser med hensyn til dens nationale sikkerhed. EU-regler eller nationale regler om beskyttelse af klassificerede informationer og hemmeligholdelsesaftaler er relevante.

(12) For ikke at bringe national sikkerhed eller kritiske enheders sikkerhed og kommercielle interesser i fare bør adgang til samt udveksling og håndtering af følsomme oplysninger foregå med omtanke og med særlig vægt på de transmissionskanaler og lagringskapaciteter, der anvendes.

(13) Med henblik på at sikre en samlet tilgang til kritiske enheders modstandsdygtighed bør hver medlemsstat have en strategi for styrkelse af kritiske enheders modstandsdygtighed på plads (»strategien«). Strategien bør fastsætte de strategiske mål og politikforanstaltninger, der skal gennemføres. Af hensyn til sammenhæng og effektivitet bør strategien udformes således, at de uden problemer kan integrere eksisterende politikker, og så vidt muligt bygge på eksisterende nationale og sektorspecifikke strategier, planer eller lignende dokumenter. For at opnå en samlet tilgang bør medlemsstaterne sikre, at deres strategier skaber en politikramme for øget koordinering mellem de kompetente myndigheder i henhold til dette direktiv og de kompetente myndigheder i henhold til direktiv (EU) 2022/2555 i forbindelse med udveksling af oplysninger om cybersikkerhedsrisici, cybertrusler og cyberhændelser og ikkecyberrisici, -trusler og -hændelser samt i forbindelse med udførelse af tilsynsopgaver. Når medlemsstaterne indfører deres strategier, bør medlemsstaterne tage behørigt hensyn til den hybride karakter af trusler mod kritiske enheder.

(14) Medlemsstaterne bør meddele Kommissionen deres strategier og væsentlige ajourføringer heraf, navnlig for at sætte Kommissionen i stand til at vurdere, om dette direktiv anvendes korrekt for så vidt angår politiktilgange til kritiske enheders modstandsdygtighed på nationalt plan. Strategierne vil, hvor det er nødvendigt, kunne meddeles som klassificerede informationer. Kommissionen bør udarbejde en sammenfattende rapport om de strategier, som medlemsstaterne har meddelt, der skal tjene som grundlag for udvekslinger med henblik på at identificere bedste praksis og spørgsmål af fælles interesse inden for rammerne af en Gruppe for Kritiske Enheders Modstandsdygtighed. På grund af den følsomme karakter af de samlede oplysninger, der vil være indeholdt i den sammenfattende rapport, uanset om de er klassificerede eller ej, bør Kommissionen forvalte den sammenfattende rapport med et passende niveau af opmærksomhed med hensyn til kritiske enheders, medlemsstaters og Unionens sikkerhed. Den sammenfattende rapport og strategierne bør beskyttes mod ulovlige eller ondsindede handlinger og bør kun være tilgængelige for bemyndigede personer med henblik på at opfylde målene i dette direktiv. Meddelelsen af strategierne og væsentlige ajourføringer heraf bør også hjælpe Kommissionen med at forstå udviklingen i tilgangene til kritiske enheders modstandsdygtighed og bidrage til overvågningen af dette direktivs indvirkning og merværdi, som Kommissionen regelmæssigt skal gennemgå.

(15) Medlemsstaternes tiltag til at identificere og bidrage til at sikre kritiske enheders modstandsdygtighed bør følge en risikobaseret tilgang, hvor der fokuseres på de enheder, der er mest relevante for udførelsen af vitale samfundsmæssige funktioner eller økonomiske aktiviteter. For at sikre en sådan målrettet tilgang bør hver medlemsstat inden for en harmoniseret ramme foretage en vurdering af de relevante naturlige og menneskeskabte risici, herunder tværsektorielle eller grænseoverskridende risici, der vil kunne påvirke leveringen af væsentlige tjenester, herunder ulykker, naturkatastrofer, folkesundhedskriser såsom pandemier og hybride trusler eller andre antagonistiske trusler, herunder terrorhandlinger, kriminel infiltration og sabotage (»medlemsstatsrisikovurdering«). Når medlemsstaterne foretager medlemsstatsrisikovurderinger, bør de tage hensyn til andre generelle eller sektorspecifikke risikovurderinger, der er foretaget i henhold til andre EU-retsakter, og til omfanget af afhængighed mellem sektorer, herunder af sektorer i andre medlemsstater og tredjelande. Resultaterne af medlemsstatsrisikovurderinger bør anvendes til at identificere kritiske enheder og bistå disse enheder med at opfylde deres modstandsdyg-

tighedskrav. Dette direktiv finder kun anvendelse på medlemsstater og kritiske enheder, der opererer i Unionen. Ikke desto mindre vil den ekspertise og viden, der genereres af kompetente myndigheder, navnlig gennem risikovurderinger, og af Kommissionen, navnlig gennem forskellige former for støtte og samarbejde, kunne anvendes, hvor det er relevant og i overensstemmelse med de gældende retlige instrumenter, til fordel for tredjelande, navnlig dem i Unionens umiddelbare nærområde, ved at bidrage til eksisterende samarbejde om modstandsdygtighed.

(16) For at sikre, at alle relevante enheder er omfattet af dette direktivs modstandsdygtighedskrav, og for at mindske forskellene i denne henseende er det vigtigt at fastsætte harmoniserede regler, der muliggør en konsekvent identifikation af kritiske enheder i hele Unionen, samtidig med at medlemsstaterne også får mulighed for i tilstrækkelig grad at afspejle disse enheders rolle og betydning på nationalt plan. Ved anvendelse af de kriterier, der er fastlagt i dette direktiv, bør hver medlemsstat identificere enheder, der leverer en eller flere væsentlige tjenester, og som opererer og har kritisk infrastruktur, der er beliggende på dens område. En enhed bør anses for at operere på en medlemsstats område, hvor den udfører de aktiviteter, der er nødvendige for den eller de pågældende væsentlige tjenester, og hvor enhedens kritiske infrastruktur, som anvendes til at levere den eller de pågældende tjenester, er beliggende. Hvis der ikke er nogen enhed, der opfylder disse kriterier i en medlemsstat, bør den pågældende medlemsstat ikke være forpligtet til at identificere en kritisk enhed i den tilsvarende sektor eller delsektor. Af hensyn til effektivitet, virkningsfuldhed, konsistens og retssikkerhed bør der fastsættes passende regler med hensyn til underretning af enheder om, at de er identificeret som kritiske enheder.

(17) Medlemsstaterne bør på en måde, der opfylder målene i dette direktiv, forelægge Kommissionen en liste over væsentlige tjenester, antallet af kritiske enheder, som er identificeret for hver sektor og delsektor anført i bilaget og for den eller de væsentlige tjenester, som hver enhed leverer, og såfremt sådanne anvendes, tærskler. Det bør være muligt at fremlægge tærskler som sådan eller i sammenfattet form, hvorved forstås, at oplysningerne kan gøres til genstand for en gennemsnitsberegning efter geografisk område, år, sektor, delsektor eller andre metoder og kan omfatte oplysninger om omfanget af de forelagte indikatorer.

(18) Der bør fastlægges kriterier for bestemmelse af betydningen af en forstyrrende virkning som følge af en hændelse. Disse kriterier bør være baseret på kriterierne i Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 ([6]) for at udnytte medlemsstaternes indsats for at identificere operatører af væsentlige tjenester som defineret i nævnte direktiv og de erfaringer, der er gjort i denne forbindelse. Større kriser, såsom covid-19-pandemien, har vist, hvor vigtigt det er at sørge for forsyningskædesikkerhed, og har påvist, hvordan forstyrrelse heraf kan have negativ økonomisk og samfundsmæssig indvirkning inden for en lang række sektorer og på tværs af grænserne. Medlemsstaterne bør derfor også i det omfang, det er muligt, overveje virkningerne på forsyningskæden, når de fastslår i hvilket omfang andre sektorer og delsektorer afhænger af de væsentlige tjenester, der udbydes af en kritisk enhed.

(19) I overensstemmelse med gældende EU-ret og national ret, herunder Europa-Parlamentets og Rådets forordning (EU) 2019/452 ([7]), som fastlægger et regelsæt for screening af udenlandske direkte investeringer i Unionen, skal den potentielle trussel, som udenlandsk ejerskab af kritisk infrastruktur i Unionen udgør, anerkendes, idet tjenester, økonomien og EU-borgernes frie bevægelighed og sikkerhed er afhængige af velfungerende kritisk infrastruktur.

(20) I henhold til direktiv (EU) 2022/2555 skal enheder, der tilhører sektoren for digital infrastruktur, og som kunne betragtes som kritiske enheder i henhold til nærværende direktiv, træffe passende og forholdsmæssige tekniske, operationelle og organisatoriske foranstaltninger for at styre risiciene for sikkerheden i net- og informationssystemer samt underrette om væsentlige hændelser og cybertrusler. Da trusler mod sikkerheden i net- og informationssystemer kan have forskellig oprindelse, anvender direktiv (EU) 2022/2555 en tilgang, der omfatter alle farer, og som omfatter net- og informationssystemers modstandsdygtighed samt disse systemers fysiske komponenter og fysiske miljø.

([6]) Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (EUT L 194 af 19.7.2016, s. 1).

([7]) Europa-Parlamentets og Rådets forordning (EU) 2019/452 af 19. marts 2019 om et regelsæt for screening af udenlandske direkte investeringer i Unionen (EUT L 79 I af 21.3.2019, s. 1).

Eftersom kravene i forbindelse hermed i direktiv (EU) 2022/2555 mindst svarer til de tilsvarende forpligtelser i nærværende direktiv, bør forpligtelserne i artikel 11 og kapitel III, IV og VI i nærværende direktiv ikke finde anvendelse på enheder, der tilhører sektoren for digital infrastruktur, for at undgå dobbeltarbejde og unødvendige administrative byrder. I betragtning af den betydning, som tjenester, der leveres af enheder, der tilhører den digitale infrastruktursektor, har for kritiske enheder, der tilhører alle andre sektorer, bør medlemsstaterne imidlertid på grundlag af kriterierne og ved anvendelse af proceduren i dette direktiv identificere enheder, der tilhører sektoren for digital infrastruktur, som kritiske enheder. Derfor bør strategierne, medlemsstatsrisikovurderingerne og støtteforanstaltningerne fastsat i dette direktivs kapitel II finde anvendelse. Medlemsstaterne bør kunne vedtage eller opretholde bestemmelser i national ret for at opnå en højere grad af modstandsdygtighed for disse kritiske enheder, forudsat at disse bestemmelser er i overensstemmelse med gældende EU-ret.

(21) I EU-retten om finansielle tjenesteydelser fastsættes omfattende krav til finansielle enheder om at håndtere alle risici, som de står over for, herunder operationelle risici, og sikre forretningskontinuitet. Denne ret omfatter Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012 ([8]), (EU) nr. 575/2013 ([9]) og (EU) nr. 600/2014 ([10]) og Europa-Parlamentets og Rådets direktiv 2013/36/EU ([11]) og 2014/65/EU ([12]). Denne retlige ramme suppleres med Europa-Parlamentets og Rådets forordning (EU) 2022/2554 ([13]), som fastsætter krav til finansielle enheder om at styre risici i forbindelse med informations- og kommunikationsteknologi (IKT), herunder vedrørende beskyttelse af fysisk IKT-infrastruktur. Eftersom disse enheders modstandsdygtighed derfor er fuldt ud dækket, bør artikel 11 og kapitel III, IV og VI i dette direktiv ikke finde anvendelse på disse enheder for at undgå dobbeltarbejde og unødvendige administrative byrder.

I betragtning af den betydning, som tjenester, der leveres af enheder i den finansielle sektor, har for kritiske enheder, der tilhører alle andre sektorer, bør medlemsstaterne imidlertid på grundlag af kriterierne og ved anvendelse af proceduren i dette direktiv identificere enheder i den finansielle sektor som kritiske enheder. Derfor bør strategierne, medlemsstatsrisikovurderingerne og støtteforanstaltningerne fastsat i dette direktivs kapitel II finde anvendelse. Medlemsstaterne bør kunne vedtage eller opretholde bestemmelser i national ret for at opnå en højere grad af modstandsdygtighed for disse kritiske enheder, forudsat at disse bestemmelser er i overensstemmelse med gældende EU-ret.

(22) Medlemsstaterne bør udpege eller oprette myndigheder, der har kompetence til at føre tilsyn med anvendelsen af og om nødvendigt håndhæve reglerne i dette direktiv, og sikre, at disse myndigheder har tilstrækkelige beføjelser og ressourcer. I lyset af forskellene i nationale forvaltningsstrukturer, for at sikre allerede eksisterende sektorspecifikke ordninger eller EU-tilsyns- og reguleringsorganer og for at undgå dobbeltarbejde bør medlemsstaterne kunne udpege eller oprette mere end én kompetent myndighed. Hvis medlemsstaterne udpeger eller opretter mere end én kompetent myndighed, bør de klart afgrænse de berørte myndigheders respektive opgaver og sikre, at de samarbejder gnidningsløst og effektivt. Alle kompetente myndigheder bør også samarbejde mere generelt med andre relevante myndigheder, både på EU-plan og nationalt plan.

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

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

([10]) Europa-Parlamentets og Rådets forordning (EU) nr. 600/2014 af 15. maj 2014 om markeder for finansielle instrumenter og om ændring af forordning (EU) nr. 648/2012 (EUT L 173 af 12.6.2014, s. 84).

([11]) Europa-Parlamentets og Rådets direktiv 2013/36/EU af 26. juni 2013 om adgang til at udøve virksomhed som kreditinstitut og om tilsyn med kreditinstitutter og investeringsselskaber, om ændring af direktiv 2002/87/EF og om ophævelse af direktiv 2006/48/EF og 2006/49/EF (EUT L 176 af 27.6.2013, s. 338).

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

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

(23) For at lette grænseoverskridende samarbejde og kommunikation og muliggøre en effektiv gennemførelse af dette direktiv bør hver medlemsstat, uden at dette berører kravene i sektorspecifikke EU-retsakter, udpege et centralt kontaktpunkt med ansvar for at koordinere spørgsmål vedrørende kritiske enheders modstandsdygtighed og grænseoverskridende samarbejde på EU-plan i denne henseende, hvis relevant inden for en kompetent myndighed. Hvert centralt kontaktpunkt bør holde kontakt med og koordinere kommunikationen, hvor det er relevant, med sin medlemsstats kompetente myndigheder, med andre medlemsstaters centrale kontaktpunkter og med Gruppen for Kritiske Enheders Modstandsdygtighed.

(24) De kompetente myndigheder i henhold til dette direktiv, og de kompetente myndigheder i henhold til direktiv (EU) 2022/2555, bør samarbejde og udveksle oplysninger om cybersikkerhedsrisici, cybertrusler og cyberhændelser og ikkecyberrisici, -trusler og -hændelser, som berører kritiske enheder, samt i forhold til relevante foranstaltninger, der er truffet af de kompetente myndigheder i henhold til nærværende direktiv og de kompetente myndigheder i henhold til direktiv (EU) 2022/2555 Det er vigtigt, at medlemsstaterne sikrer, at kravene i nærværende direktiv og i direktiv (EU) 2022/2555 gennemføres på en komplementær måde, og at kritiske enheder ikke pålægges en administrativ byrde, der går ud over, hvad der er nødvendigt for at nå målene i nærværende direktiv og nævnte direktiv.

(25) Medlemsstaterne bør støtte kritiske enheder, herunder dem, der kan betegnes som små eller mellemstore virksomheder, med at styrke deres modstandsdygtighed i overensstemmelse med medlemsstaternes forpligtelser i dette direktiv, uden at dette berører de kritiske enheders eget retlige ansvar for at sikre en sådan opfyldelse, og i denne forbindelse hindre uforholdsmæssigt store administrative byrder. Medlemsstaterne vil navnlig kunne udvikle vejledningsmaterialer og -metoder, støtte tilrettelæggelse af øvelser for at afprøve kritiske enheders modstandsdygtighed og yde rådgivning og tilbyde uddannelse til personale i kritiske enheder. Hvor det er nødvendigt og begrundet i almene hensyn, kan medlemsstaterne stille finansielle ressourcer til rådighed og bør lette frivillig udveksling af oplysninger og udveksling af god praksis mellem kritiske enheder, uden at det berører anvendelsen af konkurrencereglerne i traktaten om Den Europæiske Unions funktionsmåde (TEUF).

(26) For at styrke modstandsdygtigheden af kritiske enheder, som er identificeret af medlemsstaterne, og for at mindske den administrative byrde for disse kritiske enheder bør de kompetente myndigheder konsultere hinanden, når det er hensigtsmæssigt, med henblik på at sikre en konsistent anvendelse af dette direktiv. Disse konsultationer bør indledes efter anmodning fra enhver interesseret kompetent myndighed og bør fokusere på at sikre en konvergerende tilgang til indbyrdes forbundne kritiske enheder, der anvender kritisk infrastruktur, som er fysisk sammenkoblet mellem to eller flere medlemsstater, og som tilhører de samme koncerner eller selskabsstrukturer, eller som er blevet identificeret i én medlemsstat og leverer væsentlige tjenester til eller i andre medlemsstater.

(27) Hvis bestemmelser i EU-retten eller national ret kræver, at kritiske enheder vurderer risici, der er relevante i forbindelse med dette direktiv, og træffer foranstaltninger for at sikre deres egen modstandsdygtighed, bør der tages tilstrækkeligt hensyn til disse krav med henblik på at føre tilsyn med kritiske enheders overholdelse af dette direktiv.

(28) Kritiske enheder bør have en omfattende forståelse af de relevante risici, som de er eksponeret for, og en pligt til at analysere disse risici. Med henblik herpå bør de foretage risikovurderinger, når det er nødvendigt i lyset af deres særlige omstændigheder og udviklingen af disse risici og under alle omstændigheder hvert fjerde år, for at vurdere alle relevante risici, der vil kunne forstyrre leveringen af deres væsentlige tjenester (»kritiske enheders risikovurdering«). Hvor kritiske enheder har foretaget andre risikovurderinger eller udarbejdet dokumenter i henhold til forpligtelser i andre retsakter, der er relevante for deres risikovurdering, bør de kunne anvende disse vurderinger og dokumenter til at opfylde kravene i dette direktiv vedrørende kritiske enheders risikovurdering. En kompetent myndighed bør kunne erklære, at en eksisterende risikovurdering foretaget af en kritisk enhed, der behandler de relevante risici og det relevante omfang af afhængighed, helt eller delvist opfylder forpligtelserne i dette direktiv.

(29) Kritiske enheder bør træffe passende tekniske, sikkerhedsmæssige og organisatoriske foranstaltninger, der står i et rimeligt forhold til de risici, som de står over for, for at forebygge, beskytte mod, reagere på, modstå, afbøde, absorbere, tilpasse sig til og komme på fode igen efter en hændelse. Mens kritiske enheder bør træffe disse foranstaltninger i overensstemmelse med dette direktiv, bør sådanne foranstaltningers nærmere enkeltheder og omfang afspejle de forskellige risici, som hver kritiske enhed har identificeret som led i sin risikovurdering, og de særlige forhold, der gør sig gældende for en sådan enhed, på en passende og forholdsmæssig måde. For at fremme en sammenhængende EU-tilgang bør Kommissionen efter høring af Gruppen for Kritiske Enheders Modstandsdygtighed vedtage ikkebindende retningslinjer for nærmere at præcisere disse tekniske, sikkerhedsmæssige og organisatoriske foranstaltninger. Medlemsstaterne bør sikre, at hver kritisk enhed udpeger en forbindelsesofficer eller tilsvarende som kontaktpunkt for de kompetente myndigheder.

(30) Af hensyn til effektivitet og ansvarlighed bør kritiske enheder under hensyntagen til de identificerede risici beskrive de foranstaltninger, som de træffer, med en detaljeringsgrad, som i tilstrækkelig grad når målene om effektivitet og ansvarlighed, i en plan for modstandsdygtighed eller i et eller flere dokumenter, der svarer til en plan for modstandsdygtighed, og anvende denne plan i praksis. Hvis en kritisk enhed allerede har truffet tekniske, sikkerhedsmæssige og organisatoriske foranstaltninger og udarbejdet dokumenter i henhold til andre retsakter, der er relevante for modstandsdygtighedsstyrkende foranstaltninger i henhold til dette direktiv, bør den for at undgå dobbeltarbejde kunne anvende disse foranstaltninger og dokumenter til at opfylde kravene med hensyn til modstandsdygtighedsforanstaltninger i henhold til dette direktiv. For at undgå dobbeltarbejde bør en kompetent myndighed kunne erklære, at en kritisk enheds eksisterende modstandsdygtighedsforanstaltninger, der tager hånd om dens forpligtelse til at træffe tekniske, sikkerhedsmæssige og organisatoriske foranstaltninger i henhold til dette direktiv, helt eller delvist opfylder kravene i dette direktiv.

(31) I Europa-Parlamentets og Rådets forordning (EF) nr. 725/2004 ([14]) og (EF) nr. 300/2008 ([15]) og Europa-Parlamentets og Rådets direktiv 2005/65/EF ([16]) fastsættes krav til enheder i luftfarts- og søtransportsektoren med henblik på at forebygge hændelser forårsaget af ulovlige handlinger og modstå og afbøde følgerne af sådanne hændelser. Selv om de foranstaltninger, der kræves i henhold til nærværende direktiv, er bredere med hensyn til de risici, der håndteres, og de typer af foranstaltninger, der skal træffes, bør kritiske enheder i disse sektorer i deres plan for modstandsdygtighed eller tilsvarende dokumenter afspejle de foranstaltninger, der er truffet i henhold til disse andre EU-retsakter. Kritiske enheder skal også tage hensyn til Europa-Parlamentets og Rådets direktiv 2008/96/EF ([17]), som indfører en vejnetvurdering med henblik på at kortlægge risiciene for ulykker og en målrettet trafiksikkerhedsinspektion med henblik på at afdække farlige forhold, mangler og problemer, som øger risikoen for ulykker og tilskadekomst, baseret på besigtigelse af eksisterende veje eller vejstrækninger. Sikring af kritiske enheders beskyttelse og modstandsdygtighed er af allerstørste betydning for jernbanesektoren, og kritiske enheder tilskyndes til at henvise til ikkebindende retningslinjer og dokumenter om god praksis, der er udarbejdet under sektorspecifikke arbejdsgange, såsom EU-sikkerhedsplatformen for jernbanepassagerer, der er oprettet ved Kommissionens afgørelse 2018/C 232/03 ([18]), når de gennemfører modstandsdygtighedsforanstaltninger i henhold til dette direktiv.

(32) Risikoen for, at ansatte i kritiske enheder eller deres kontrahenter misbruger for eksempel deres adgangsret inden for den kritiske enheds organisation til at skade og forvolde skade, giver anledning til stigende bekymring. Medlemsstaterne bør derfor angive de betingelser, på hvilke kritiske enheder i behørigt begrundede tilfælde og under hensyntagen til medlemsstatsrisikovurderinger har tilladelse til at indgive anmodninger om baggrundskontrol af personer, der tilhører specifikke kategorier af deres personale. Det bør sikres, at de relevante myndigheder vurderer sådanne anmodninger inden for en rimelig frist og behandler dem i overensstemmelse med national ret og nationale procedurer samt relevant og gældende EU-ret, herunder om beskyttelse af personoplysninger. For at bekræfte identiteten af en person, der er genstand for en baggrundskontrol, er det hensigtsmæssigt, at medlemsstaterne kræver et identitetsbevis, såsom et pas, et nationalt identitetskort eller en digital form for identifikation, i overensstemmelse med gældende ret.

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

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

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

([17]) Europa-Parlamentets og Rådets direktiv 2008/96/EF af 19. november 2008 om forvaltning af vejinfrastrukturens sikkerhed (EUT L 319 af 29.11.2008, s. 59).

([18]) Kommissionens afgørelse af 29. juni 2018 om oprettelse af EU-sikkerhedsplatformen for togpassagerer 2018/C 232/03 (EUT C 232 af 3.7.2018, s. 10).

Baggrundskontrol bør omfatte kontrol af strafferegistre for den pågældende person. Medlemsstaterne bør anvende det europæiske informationssystem vedrørende strafferegistre i overensstemmelse med procedurerne i Rådets rammeafgørelse 2009/315/RIA ([19]) og, hvor det er relevant og finder anvendelse, Europa-Parlamentets og Rådets forordning (EU) 2019/816 ([20]) med henblik på indhentning af oplysninger fra andre medlemsstaters strafferegistre. Medlemsstaterne kan også, hvor det er relevant og finder anvendelse, trække på anden generation af Schengeninformationssystemet (SIS II), der blev oprettet ved Europa-Parlamentets og Rådets forordning (EU) 2018/1862 ([21]), efterretninger og alle andre tilgængelige objektive oplysninger, som måtte være nødvendige for at fastslå, om den berørte person er egnet til at beklæde den stilling, for hvilken den kritiske enhed har anmodet om en baggrundskontrol.

(33) Der bør oprettes en mekanisme til underretning om visse hændelser for at gøre det muligt for de kompetente myndigheder at reagere hurtigt og hensigtsmæssigt på hændelser og danne sig et samlet overblik over indvirkningen, arten, årsagen og de mulige konsekvenser af hændelser, som kritiske enheder håndterer. Kritiske enheder bør uden unødigt ophold underrette de kompetente myndigheder om hændelser, der i betydelig grad forstyrrer eller har potentiale til i betydelig grad at forstyrre leveringen af væsentlige tjenester. Medmindre det operationelt ikke er muligt, bør kritiske enheder indgive en første underretning senest 24 timer efter, at de er blevet opmærksomme på en hændelse. Den første underretning bør kun indeholde de oplysninger, der er strengt nødvendige for at gøre den kompetente myndighed opmærksom på hændelsen og give den kritiske enhed mulighed for at søge bistand, hvis det er nødvendigt. En sådan underretning bør, hvor det er muligt, angive den formodede årsag til hændelsen. Medlemsstaterne bør sikre, at kravet om at foretage denne første underretning ikke afleder den kritiske enheds ressourcer fra aktiviteter vedrørende håndtering af hændelser, der bør prioriteres. Den første underretning bør, hvor det er relevant, efterfølges af en detaljeret rapport senest en måned efter hændelsen. Den detaljerede rapport bør supplere den første underretning og give et mere fuldstændigt overblik over hændelsen.

(34) Standardisering bør fortsat primært være en markedsstyret proces. Der kan imidlertid stadig være situationer, hvor det er hensigtsmæssigt at kræve overholdelse af specifikke standarder. Medlemsstaterne bør, hvor det er nyttigt, tilskynde til anvendelse af europæiske og internationale standarder og tekniske specifikationer af relevans for de sikkerheds- og modstandsdygtighedsforanstaltninger, som finder anvendelse på kritiske enheder.

(35) Selv om kritiske enheder generelt opererer som en del af et stadig mere sammenkoblet net af tjenester og infrastruktur og ofte leverer væsentlige tjenester i mere end én medlemsstat, er nogle af disse kritiske enheder af særlig betydning for Unionen og dens indre marked, fordi de leverer væsentlige tjenester til eller i seks eller flere medlemsstater og derfor vil kunne drage fordel af specifik støtte på EU-plan. Der bør derfor fastsættes regler om rådgivende missioner for sådanne kritiske enheder af særlig europæisk betydning. Disse regler berører ikke reglerne om tilsyn og håndhævelse i dette direktiv.

(36) Efter en begrundet anmodning fra Kommissionen eller en eller flere medlemsstater, hvortil eller hvori en væsentlig tjeneste leveres, bør en medlemsstat, der har identificeret en kritisk enhed af særlig europæisk betydning som kritisk enhed, give Kommissionen visse oplysninger som fastsat dette direktiv, hvis der er behov for yderligere oplysninger for at kunne rådgive den kritiske enhed om opfyldelse af dens forpligtelser i henhold til dette direktiv eller vurdere, om den kritiske enhed af særlig europæisk betydning opfylder disse forpligtelser. Efter aftale med den medlemsstat, der har identificeret den kritiske enhed af særlig europæisk betydning som kritisk enhed, bør Kommissionen kunne tilrettelægge en rådgivende mission for at vurdere de foranstaltninger, som den pågældende enhed har truffet. For at sikre, at sådanne rådgivende missioner gennemføres korrekt, bør der fastsættes supplerende regler, navnlig for de rådgivende missioners tilrettelæggelse og gennemførelse, de opfølgende tiltag, der skal tages, og forpligtelserne for berørte kritiske enheder af særlig europæisk betydning. Rådgivende missioner bør, uden at det berører behovet for,

([19]) Rådets rammeafgørelse 2009/315/RIA af 26. februar 2009 om tilrettelæggelsen og indholdet af udvekslinger af oplysninger fra strafferegistre mellem medlemsstaterne (EUT L 93 af 7.4.2009, s. 23).

([20]) Europa-Parlamentets og Rådets forordning (EU) 2019/816 af 17. april 2019 om oprettelse af et centralt system til bestemmelse af, hvilke medlemsstater der ligger inde med oplysninger om straffedomme afsagt over tredjelandsstatsborgere og statsløse personer (ECRIS-TCN) for at supplere det europæiske informationssystem vedrørende strafferegistre, og om ændring af forordning (EU) 2018/1726 (EUT L 135 af 22.5.2019, s. 1).

([21]) Europa-Parlamentets og Rådets forordning (EU) 2018/1862 af 28. november 2018 om oprettelse, drift og brug af Schengeninformationssystemet (SIS) på området politisamarbejde og strafferetligt samarbejde, om ændring og ophævelse af Rådets afgørelse 2007/533/RIA og om ophævelse af Europa-Parlamentets og Rådets forordning (EF) nr. 1986/2006 og Kommissionens afgørelse 2010/261/EU (EUT L 312 af 7.12.2018, s. 56).

at den medlemsstat, hvor en rådgivende mission gennemføres, og den berørte enhed overholder reglerne i dette direktiv, gennemføres i henhold til de detaljerede regler i den pågældende medlemsstats nationale ret, f.eks. om de præcise betingelser, der skal opfyldes for at få adgang til relevante lokaler eller dokumenter, og om domstolsprøvelse. Der vil, hvor det er relevant, kunne anmodes om specifik ekspertbistand til sådanne rådgivende missioner via Katastrofeberedskabskoordinationscentret, som er oprettet ved Europa-Parlamentets og Rådets afgørelse nr. 1313/2013/EU ([22]).

(37) For at støtte Kommissionen og lette samarbejde mellem medlemsstaterne og udveksling af oplysninger, herunder bedste praksis, om spørgsmål vedrørende dette direktiv bør der nedsættes en Gruppe for Kritiske Enheders Modstandsdygtighed som en ekspertgruppe i Kommissionen. Medlemsstaterne bør bestræbe sig på at sikre et effektivt samarbejde mellem de udpegede repræsentanter for deres kompetente myndigheder i Gruppen for Kritiske Enheders Modstandsdygtighed, herunder ved at udpege repræsentanter, der er sikkerhedsgodkendt, hvis det er relevant. Gruppen for Kritiske Enheders Modstandsdygtighed bør begynde at udføre sine opgaver så snart som muligt for at tilvejebringe yderligere midler til passende samarbejde i løbet af gennemførelsesperioden for dette direktiv. Gruppen for Kritiske Enheders Modstandsdygtighed bør indgå i et samspil med andre relevante sektorspecifikke ekspertgrupper.

(38) Gruppen for Kritiske Enheders Modstandsdygtighed bør samarbejde med den samarbejdsgruppe, der er nedsat i henhold til direktiv (EU) 2022/2555, med henblik på at støtte en omfattende ramme for kritiske enheders cyber- og ikkecybermodstandsdygtighed. Gruppen for Kritiske Enheders Modstandsdygtighed og den samarbejdsgruppe, der er nedsat i henhold til direktiv (EU) 2022/2555, bør indgå i en regelmæssig dialog for at fremme samarbejde mellem de kompetente myndigheder i henhold til nærværende direktiv og de kompetente myndigheder i henhold til direktiv (EU) 2022/2555, og for at lette udveksling af oplysninger, navnlig om emner af relevans for begge grupper.

(39) For at nå målene i dette direktiv, og uden at dette berører medlemsstaternes og kritiske enheders retlige ansvar for at sikre, at de respektive forpligtelser, der er fastsat heri, opfyldes, bør Kommissionen, hvor den finder det hensigtsmæssigt, støtte kompetente myndigheder og kritiske enheder med henblik på at lette opfyldelsen af deres respektive forpligtelser. Når Kommissionen yder støtte til medlemsstaterne og kritiske enheder ved opfyldelsen af forpligtelserne i henhold til dette direktiv, bør den tage udgangspunkt i eksisterende strukturer og værktøjer såsom dem inden for rammerne af EU-civilbeskyttelsesmekanismen, der blev oprettet ved afgørelse nr. 1313/2013/EU, og det europæiske referencenetværk for beskyttelse af kritisk infrastruktur. Den bør desuden orientere medlemsstaterne om midler, der er til rådighed på EU-plan, f.eks. inden for Fonden for Intern Sikkerhed, der blev oprettet ved Europa-Parlamentets og Rådets forordning (EU) 2021/1149 ([23]), Horisont Europa, der blev oprettet ved Europa-Parlamentets og Rådets forordning (EU) 2021/695 ([24]), eller andre instrumenter, der er relevante for kritiske enheders modstandsdygtighed.

(40) Medlemsstaterne bør sikre, at deres kompetente myndigheder har visse specifikke beføjelser til at sikre en korrekt anvendelse og håndhævelse af dette direktiv i forbindelse med kritiske enheder, når disse enheder hører under deres jurisdiktion som fastsat i dette direktiv. Disse beføjelser bør navnlig omfatte beføjelse til at foretage inspektioner og revision, til at føre tilsyn, til at kræve, at kritiske enheder fremlægger oplysninger og dokumentation vedrørende de foranstaltninger, som de har truffet for at opfylde deres forpligtelser, og, hvor det er nødvendigt, til at udstede påbud for at afhjælpe konstaterede overtrædelser. Når medlemsstaterne udsteder sådanne påbud, bør de ikke kræve foranstaltninger, der går ud over, hvad der er nødvendigt og rimeligt for at sikre, at den pågældende kritiske enhed opfylder forpligtelserne, navnlig under hensyntagen til overtrædelsens alvor og den pågældende kritiske enheds økonomiske formåen. Mere generelt bør disse beføjelser ledsages af passende og effektive garantier, der fastsættes i national ret i overensstemmelse med Den Europæiske Unions charter om grundlæggende rettigheder. Ved

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

([23]) Europa-Parlamentets og Rådets forordning (EU) 2021/1149 af 7. juli 2021 om oprettelse af Fonden for Intern Sikkerhed (EUT L 251 af 15.7.2021, s. 94).

([24]) Europa-Parlamentets og Rådets forordning (EU) 2021/695 af 28. april 2021 om oprettelse af Horisont Europa — rammeprogrammet for forskning og innovation — og om reglerne for deltagelse og formidling og om ophævelse af forordning (EU) nr. 1290/2013 og (EU) nr. 1291/2013 (EUT L 170 af 12.5.2021, s. 1).

vurderingen af, om en kritisk enhed opfylder sine forpligtelser som fastsat i dette direktiv, bør de kompetente myndigheder i henhold til dette direktiv kunne anmode de kompetente myndigheder i henhold til direktiv (EU) 2022/2555 om at udøve deres tilsyns- og håndhævelsesbeføjelser over for en enhed i henhold til nævnte direktiv, som er identificeret som kritisk enhed i henhold til nærværende direktiv. De kompetente myndigheder i henhold til nærværende direktiv og de kompetente myndigheder i henhold til direktiv (EU) 2022/2555 bør samarbejde og udveksle oplysninger med henblik herpå.

(41) For at dette direktiv kan anvendes på en effektiv og konsekvent måde, bør beføjelsen til at vedtage retsakter delegeres til Kommissionen i overensstemmelse med artikel 290 i TEUF med henblik på at supplere dette direktiv ved at udarbejde en liste over væsentlige tjenester. Denne liste bør anvendes af kompetente myndigheder med henblik på at foretage medlemsstatsrisikovurderinger og identificere kritiske enheder i henhold til dette direktiv. I lyset af dette direktivs tilgang med minimumsharmonisering er denne liste ikkeudtømmende, og medlemsstaterne kan supplere den med yderligere væsentlige tjenester på nationalt plan for at tage hensyn til særlige nationale forhold i forbindelse med levering af væsentlige tjenester. Det er navnlig vigtigt, at Kommissionen gennemfører relevante høringer under sit forberedende arbejde, herunder på ekspertniveau, og at disse høringer gennemføres i overensstemmelse med principperne i den interinstitutionelle aftale af 13. april 2016 om bedre lovgivning ([25]). For at sikre lige deltagelse i forberedelsen af delegerede retsakter modtager Europa-Parlamentet og Rådet navnlig alle dokumenter på samme tid som medlemsstaternes eksperter, og deres eksperter har systematisk adgang til møder i Kommissionens ekspertgrupper, der beskæftiger sig med forberedelse af delegerede retsakter.

(42) For at sikre ensartede betingelser for gennemførelsen af dette direktiv bør Kommissionen tillægges gennemførelsesbeføjelser. Disse beføjelser bør udøves i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) nr. 182/2011 ([26]).

(43) Målene for dette direktiv, nemlig at sikre at tjenester, der er væsentlige for opretholdelsen af vitale samfundsmæssige funktioner eller økonomiske aktiviteter, leveres uhindret på det indre marked, og at styrke modstandsdygtigheden af kritiske enheder, som leverer sådanne tjenester, kan ikke i tilstrækkelig grad opfyldes af medlemsstaterne, men kan på grund af foranstaltningens virkninger bedre nås på EU-plan; Unionen kan derfor vedtage foranstaltninger i overensstemmelse med nærhedsprincippet, jf. artikel 5 i traktaten om Den Europæiske Union. I overensstemmelse med proportionalitetsprincippet, jf. nævnte artikel 5, går dette direktiv ikke videre, end hvad der er nødvendigt for at nå disse mål.

(44) Den Europæiske Tilsynsførende for Databeskyttelse er blevet hørt i overensstemmelse med artikel 42, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) 2018/1725 ([27]) og afgav udtalelse den 11. august 2021.

(45) Direktiv 2008/114/EF bør derfor ophæves —

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

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

([27]) 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).

VEDTAGET DETTE DIREKTIV:

KAPITEL I

ALMINDELIGE BESTEMMELSER

Artikel 1

Genstand og anvendelsesområde

1. Ved dette direktiv:

a) fastsættes forpligtelser for medlemsstaterne til at træffe specifikke foranstaltninger med henblik på at sikre, at tjenester, der er væsentlige for opretholdelsen af vitale samfundsmæssige funktioner eller økonomiske aktiviteter inden for anvendelsesområdet for artikel 114 i TEUF, leveres uhindret på det indre marked, navnlig forpligtelser til at identificere kritiske enheder og til at støtte kritiske enheder i at opfylde de forpligtelser, som de er pålagt

b) fastsættes forpligtelser for kritiske enheder med henblik på at styrke deres modstandsdygtighed og evne til at levere de i litra a) omhandlede tjenester på det indre marked

c) fastsættes regler for:

   i) tilsyn med kritiske enheder

   ii) håndhævelse

   iii) identifikation af kritiske enheder af særlig europæisk betydning og for rådgivende missioner for at vurdere de foranstaltninger, som sådanne enheder har truffet for at opfylde deres forpligtelser i henhold til kapitel III

d) fastsættes fælles procedurer for samarbejde og rapportering med henblik på anvendelse af dette direktiv

e) indføres foranstaltninger med henblik på at opnå en høj grad af modstandsdygtighed i kritiske enheder for at sikre levering af væsentlige tjenester i Unionen og forbedre det indre markeds funktion.

2. Dette direktiv finder ikke anvendelse på spørgsmål, der er omfattet af direktiv (EU) 2022/2555, jf. dog nærværende direktivs artikel 8. I lyset af forbindelsen mellem kritiske enheders fysiske sikkerhed og cybersikkerhed sikrer medlemsstaterne en koordineret gennemførelse af nærværende direktiv og direktiv (EU) 2022/2555.

3. Hvor bestemmelser i sektorspecifikke EU-retsakter kræver, at kritiske enheder træffer foranstaltninger for at styrke deres modstandsdygtighed, og hvor disse krav er anerkendt af medlemsstaterne som svarende mindst til de tilsvarende forpligtelser, der er fastsat i dette direktiv, finder de relevante bestemmelser i dette direktiv, herunder bestemmelsen om tilsyn og håndhævelse i kapitel VI, ikke anvendelse.

4. Uden at det berører artikel 346 i TEUF, udveksles oplysninger, der er fortrolige i henhold til EU-regler eller nationale regler, såsom regler om forretningshemmeligheder, kun med Kommissionen og andre relevante myndigheder i overensstemmelse med dette direktiv, hvor denne udveksling er nødvendig for anvendelsen af dette direktiv. De udvekslede oplysninger begrænses til, hvad der er relevant og forholdsmæssigt under hensyntagen til formålet med udvekslingen. Udvekslingen af oplysninger skal bevare de pågældende oplysningers fortrolighed og beskytte de kritiske enheders sikkerhed og kommercielle interesser, samtidig med at medlemsstaternes sikkerhed respekteres.

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

6. Dette direktiv finder ikke anvendelse på offentlige forvaltningsenheder, som udfører deres aktiviteter indenfor national sikkerhed, offentlig sikkerhed, forsvar eller retshåndhævelse, herunder efterforskning, afsløring og retsforfølgning af strafbare handlinger.

7. Medlemsstaterne kan beslutte, at artikel 11 og kapitel III, IV og VI helt eller delvist ikke finder anvendelse på specifikke kritiske enheder, der udfører aktiviteter inden for national sikkerhed, offentlig sikkerhed, forsvar eller retshåndhævelse, herunder efterforskning, afsløring og retsforfølgning af strafbare handlinger, eller som udelukkende leverer tjenester til de offentlige forvaltningsenheder, der er omhandlet i nærværende artikels stk. 6.

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

9. Dette direktiv berører ikke EU-retten om beskyttelse af personoplysninger, navnlig Europa-Parlamentets og Rådets forordning (EU) 2016/679 ([28]) og Europa-Parlamentets og Rådets direktiv 2002/58/EF ([29]).

Artikel 2

Definitioner

I dette direktiv forstås ved:

1) »kritisk enhed«: en offentlig eller privat enhed, som er blevet identificeret af en medlemsstat i overensstemmelse med artikel 6 som tilhørende en af kategorierne anført i tredje kolonne i tabellen i bilaget

2) »modstandsdygtighed«: en kritisk enheds evne til at forebygge, beskytte mod, reagere på, modstå, afbøde, absorbere, tilpasse sig og komme på fode igen efter en hændelse

3) »hændelse«: en begivenhed, der har potentiale til i betydelig grad at forstyrre, eller som forstyrrer, leveringen af en væsentlig tjeneste, herunder når den påvirker de nationale systemer, der sikrer retsstatsprincippet

4) »kritisk infrastruktur«: et aktiv, en facilitet, udstyr, et netværk eller et system, eller en del af et aktiv, en facilitet, udstyr, et netværk eller et system, som er nødvendig(t) for leveringen af en væsentlig tjeneste

5) »væsentlig tjeneste«: en tjeneste, der er afgørende for opretholdelsen af vitale samfundsmæssige funktioner, økonomiske aktiviteter, folkesundhed og offentlig sikkerhed eller miljøet

6) »risiko«: potentialet for tab eller forstyrrelse som følge af en hændelse, der skal udtrykkes som en kombination af størrelsen af et sådant tab eller en sådan forstyrrelse og sandsynligheden for, at hændelsen indtræffer

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

8) »standard«: en standard som defineret i artikel 2, nr. 1), i Europa-Parlamentets og Rådets forordning (EU) nr. 1025/2012 ([30])

([28]) 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).

([29]) 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).

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

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

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

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

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

c) den finansieres overvejende af statslige myndigheder eller af andre offentligretlige organer på centralt niveau, er underlagt ledelsestilsyn af disse myndigheder eller organer, eller har et administrations-, ledelses- eller tilsynsorgan, hvor mere end halvdelen af medlemmerne udpeges af statslige myndigheder eller andre offentligretlige organer på centralt niveau

d) den har beføjelse til at rette administrative eller lovgivningsmæssige afgørelser til fysiske eller juridiske personer, der påvirker deres rettigheder i forbindelse med grænseoverskridende bevægelighed for personer, varer, tjenester eller kapital.

Artikel 3

Minimumsharmonisering

Dette direktiv er ikke til hinder for, at medlemsstaterne vedtager eller opretholder bestemmelser i national ret med henblik på at opnå et højere niveau for kritiske enheders modstandsdygtighed, forudsat at sådanne bestemmelser er i overensstemmelse med medlemsstaternes forpligtelser, der er fastsat i EU-retten.

KAPITEL II

NATIONALE RAMMER FOR KRITISKE ENHEDERS MODSTANDSDYGTIGHED

Artikel 4

Strategi for kritiske enheders modstandsdygtighed

1. Efter en høring, der i det omfang, det er praktisk muligt, er åben for relevante interessenter, vedtager hver medlemsstat senest den 17. januar 2026 en strategi for styrkelse af kritiske enheders modstandsdygtighed (»strategien«). Byggende på relevante eksisterende nationale og sektorspecifikke strategier, planer eller lignende dokumenter skal strategien indeholde strategiske mål og politikforanstaltninger med henblik på at opnå og opretholde en høj grad af modstandsdygtighed i kritiske enheder og mindst omfatte de sektorer, der er anført i bilaget.

2. Hver strategi skal mindst indeholde følgende elementer:

a) strategiske mål og prioriteter med henblik på at styrke kritiske enheders overordnede modstandsdygtighed under hensyntagen til grænseoverskridende og tværsektoriel afhængighed og indbyrdes afhængighed

b) en forvaltningsramme for at nå de strategiske mål og prioriteter, herunder en beskrivelse af roller og ansvarsområder for de forskellige myndigheder, kritiske enheder og andre parter, der er involveret i gennemførelsen af strategien

c) en beskrivelse af de foranstaltninger, der er nødvendige for at styrke kritiske enheders overordnede modstandsdygtighed, herunder en beskrivelse af risikovurderingen omhandlet i artikel 5

d) en beskrivelse af den proces, hvorved kritiske enheder identificeres

e) en beskrivelse af processen for støtte til kritiske enheder i overensstemmelse med dette kapitel, herunder foranstaltninger til styrkelse af samarbejdet mellem den offentlige sektor på den ene side og den private sektor og offentlige og private enheder på den anden side

f) en liste over de vigtigste myndigheder og relevante interessenter, ud over kritiske enheder, der er involveret i gennemførelsen af strategien

g) en politikramme for koordinering mellem de kompetente myndigheder i henhold til dette direktiv (»de kompetente myndigheder«) og de kompetente myndigheder i henhold til direktiv (EU) 2022/2555 med henblik på udveksling af oplysninger om cybersikkerhedsrisici, cybertrusler og cyberhændelser og ikkecyberrisici, -trusler og -hændelser samt udøvelse af tilsynsopgaver

h) en beskrivelse af allerede indførte foranstaltninger, der har til formål at lette opfyldelsen af forpligtelser i henhold til dette direktivs kapitel III for små og mellemstore virksomheder i den i bilaget til Kommissionens henstilling 2003/361/EF ([31]) anvendte betydning, som den pågældende medlemsstat har identificeret som kritiske enheder.

Efter en høring, der i det omfang, det er praktisk muligt, er åben for relevante interessenter, ajourfører medlemsstaterne deres strategier mindst hvert fjerde år.

3. Medlemsstaterne meddeler Kommissionen deres strategier og væsentlige ajourføringer heraf inden for tre måneder efter deres vedtagelse.

Artikel 5

Medlemsstaternes risikovurdering

1. Kommissionen tillægges beføjelse til at vedtage en delegeret retsakt i overensstemmelse med artikel 23 senest den 17. november 2023 for at supplere dette direktiv ved at udarbejde en ikkeudtømmende liste over væsentlige tjenester i sektorerne og delsektorerne anført i bilaget. De kompetente myndigheder bruger denne liste over væsentlige tjenester til at foretage en risikovurdering (»medlemsstatsrisikovurdering«) senest den 17. januar 2026, når det er nødvendigt efterfølgende, og mindst hvert fjerde år. De kompetente myndigheder bruger medlemsstatsrisikovurderinger med henblik på at identificere kritiske enheder i overensstemmelse med artikel 6 og til at bistå disse kritiske enheder med at træffe foranstaltninger i henhold til artikel 13.

Medlemsstatsrisikovurderinger skal tage højde for de relevante naturlige og menneskeskabte risici, herunder af tværsektoriel eller grænseoverskridende karakter, ulykker, naturkatastrofer, folkesundhedskriser og hybride trusler eller andre antagonistiske trusler, herunder terrorhandlinger som fastsat i Europa-Parlamentets og Rådets direktiv (EU) 2017/541 ([32]).

2. Ved foretagelse af medlemsstatsrisikovurderinger tager medlemsstaterne mindst hensyn til følgende:

a) den generelle risikovurdering, som foretages i henhold til artikel 6, stk. 1, i afgørelse nr. 1313/2013/EU

b) andre relevante risikovurderinger, der foretages i overensstemmelse med kravene i de relevante sektorspecifikke EU-retsakter, herunder Europa-Parlamentets og Rådets forordning (EU) 2017/1938 ([33]) og (EU) 2019/941 ([34]) og Europa-Parlamentets og Rådets direktiv 2007/60/EF ([35]) og 2012/18/EU ([36])

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

([32]) Europa-Parlamentets og Rådets direktiv (EU) 2017/541 af 15. marts 2017 om bekæmpelse af terrorisme og om erstatning af Rådets rammeafgørelse 2002/475/RIA og ændring af Rådets afgørelse 2005/671/RIA (EUT L 88 af 31.3.2017, s. 6).

([33]) Europa-Parlamentets og Rådets forordning (EU) 2017/1938 af 25. oktober 2017 om foranstaltninger til opretholdelse af gasforsyningssikkerheden og ophævelse af forordning (EU) nr. 994/2010 (EUT L 280 af 28.10.2017, s. 1).

([34]) 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).

([35]) Europa-Parlamentets og Rådets direktiv 2007/60/EF af 23. oktober 2007 om vurdering og styring af risikoen for oversvømmelser (EUT L 288 af 6.11.2007, s. 27).

([36]) Europa-Parlamentets og Rådets direktiv 2012/18/EU af 4. juli 2012 om kontrol med risikoen for større uheld med farlige stoffer og om ændring og efterfølgende ophævelse af Rådets direktiv 96/82/EF (EUT L 197 af 24.7.2012, s. 1).

c) de relevante risici som følge af omfanget af afhængighed mellem de sektorer, der er anført i bilaget, herunder som følge af omfanget af afhængighed af enheder beliggende i andre medlemsstater og tredjelande, og den indvirkning, som en betydelig forstyrrelse i en sektor kan have på andre sektorer, herunder eventuelle betydelige risici for borgerne og det indre marked

d) eventuelle oplysninger om hændelser, der er underrettet om i overensstemmelse med artikel 15.

Med henblik på første afsnit, litra c), samarbejder medlemsstaterne med andre medlemsstaters og tredjelandes kompetente myndigheder, alt efter hvad der er relevant.

3. Medlemsstaterne stiller, hvor det er relevant gennem deres centrale kontaktpunkter, de relevante elementer i medlemsstatsrisikovurderinger til rådighed for de kritiske enheder, som de har identificeret i overensstemmelse med artikel 6. Medlemsstaterne sikrer, at de oplysninger, der gives til de kritiske enheder, bistår dem med at foretage deres risikovurdering i henhold til artikel 12 og træffe foranstaltninger for at sikre deres modstandsdygtighed i henhold til artikel 13.

4. Inden for tre måneder efter at have foretaget en medlemsstatsrisikovurdering meddeler en medlemsstat Kommissionen relevante oplysninger om risikotyperne identificeret som følge af, og resultaterne af, denne medlemsstatsrisikovurdering pr. sektor og delsektor anført i bilaget.

5. Kommissionen udarbejder i samarbejde med medlemsstaterne en frivillig fælles rapporteringsmodel med henblik på overholdelse af stk. 4.

Artikel 6

Identifikation af kritiske enheder

1. Senest den 17. juli 2026 identificerer medlemsstaterne de kritiske enheder for sektorerne og delsektorerne anført i bilaget.

2. Når en medlemsstat identificerer kritiske enheder i henhold til stk. 1, tager den hensyn til resultaterne af dens medlemsstatsrisikovurdering og dens strategi og anvender alle følgende kriterier:

a) enheden leverer en eller flere væsentlige tjenester

b) enheden opererer og dens kritiske infrastruktur er beliggende på denne medlemsstats område og

c) en hændelse vil have betydelige forstyrrende virkninger som fastslået i overensstemmelse med artikel 7, stk. 1, på enhedens levering af en eller flere væsentlige tjenester eller på leveringen af andre væsentlige tjenester i sektorerne anført i bilaget, som er afhængige af denne eller disse væsentlige tjenester.

3. Hver medlemsstat opstiller en liste over de kritiske enheder, der er identificeret i henhold til stk. 2, og sikrer, at disse kritiske enheder inden for en måned efter denne identifikation underrettes om, at de er blevet identificeret som kritiske enheder. Medlemsstaterne orienterer disse kritiske enheder om deres forpligtelser i henhold til kapitel III og IV og om, fra hvilken dato disse forpligtelser finder anvendelse på dem, uden at det berører artikel 8. Medlemsstaterne orienterer kritiske enheder i sektorerne i punkt 3, 4 og 8 i tabellen i bilaget, om, at de ikke har nogen forpligtelser i henhold til kapitel III og IV, medmindre andet er fastsat i nationale foranstaltninger.

For de berørte kritiske enheder finder kapitel III anvendelse fra ti måneder efter datoen for underretningen omhandlet i dette stykkes første afsnit.

4. Medlemsstaterne sikrer, at deres kompetente myndigheder i henhold til dette direktiv underretter de kompetente myndigheder i henhold til direktiv (EU) 2022/2555, om identiteten af de kritiske enheder, som de har identificeret i henhold til denne artikel, inden for en måned efter denne identifikation. Af underretningen skal det, hvor det er relevant, fremgå, at de pågældende kritiske enheder er enheder i sektorerne i punkt 3, 4 og 8 i tabellen i bilaget til nærværende direktiv, og ikke har nogen forpligtelser i henhold til nærværende direktivs kapitel III og IV.

5. Medlemsstaterne gennemgår, hvor det er nødvendigt og under alle omstændigheder mindst hvert fjerde år, listen over identificerede kritiske enheder omhandlet i stk. 3 og ajourfører, hvor det er relevant, denne. Hvis disse ajourføringer fører til identifikation af yderligere kritiske enheder, finder stk. 3 og 4 anvendelse for de yderligere kritiske enheder. Medlemsstaterne sikrer desuden, at enheder, der ikke længere identificeres som kritiske enheder som følge af en sådan ajourføring, rettidigt underrettes herom og om, at de ikke længere er omfattet af forpligtelserne i henhold til kapitel III fra datoen for modtagelsen af denne orientering.

6. Kommissionen udarbejder i samarbejde med medlemsstaterne henstillinger og ikkebindende retningslinjer for at bistå medlemsstaterne med at identificere kritiske enheder.

Artikel 7

Betydelig forstyrrende virkning

1. Ved fastlæggelsen af betydningen af en forstyrrende virkning som omhandlet i artikel 6, stk. 2, litra c), skal medlemsstaterne tage hensyn til følgende kriterier:

a) antal brugere, der er afhængige af den væsentlige tjeneste, som udbydes af den berørte enhed

b) omfanget af andre i bilaget anførte sektorers og delsektorers afhængighed af den pågældende væsentlige tjeneste

c) den indvirkning, som hændelser kunne have med hensyn til omfang og varighed på økonomiske og samfundsmæssige aktiviteter, miljøet, den offentlige sikkerhed eller befolkningens sundhed

d) enhedens markedsandel på markedet for den berørte væsentlige tjeneste eller de berørte væsentlige tjenester

e) det geografiske område, der kunne blive berørt af en hændelse, herunder eventuel grænseoverskridende indvirkning, under hensyntagen til den sårbarhed, som er forbundet med den grad af afsondrethed, der kendetegner visse typer af geografiske områder, såsom øregioner, afsidesliggende regioner eller bjergområder

f) enhedens betydning med hensyn til at opretholde et tilstrækkeligt niveau for den væsentlige tjeneste under hensyntagen til tilgængelighed af alternative måder at levere denne væsentlige tjeneste på.

2. Efter identifikationen af de kritiske enheder i henhold til artikel 6, stk. 1, sender hver medlemsstat uden unødigt ophold Kommissionen følgende oplysninger:

a) en liste over væsentlige tjenester i pågældende medlemsstat, hvis der er yderligere væsentlige tjenester sammenlignet med den i artikel 5, stk. 1, omhandlede liste over væsentlige tjenester

b) antallet af identificerede kritiske enheder for hver sektor og delsektor anført i bilaget og for hver væsentlig tjeneste

c) eventuelle tærskler, der anvendes til at specificere et eller flere af kriterierne i stk. 1.

Tærskler som omhandlet i første afsnits litra c) kan forelægges som de er eller i aggregeret form.

Medlemsstaterne sender efterfølgende de i første afsnit omhandlede oplysninger, når det er nødvendigt, og mindst hvert fjerde år.

3. Kommissionen vedtager efter høring af Gruppen for Kritiske Enheders Modstandsdygtighed omhandlet i artikel 19 ikkebindende retningslinjer for at lette anvendelsen af kriterierne omhandlet i denne artikels stk. 1 under hensyntagen til de i denne artikels stk. 2 omhandlede oplysninger.

Artikel 8

Kritiske enheder i sektorerne bankvæsen, finansiel markedsinfrastruktur og digital infrastruktur

Medlemsstaterne sikrer, at artikel 11 og kapitel III, IV og VI ikke finder anvendelse på kritiske enheder, som de har identificeret i sektorerne i punkt 3, 4 og 8 i tabellen i bilaget. Medlemsstaterne kan vedtage eller opretholde bestemmelser i national ret for at opnå et højere niveau for disse kritiske enheders modstandsdygtighed, forudsat at disse bestemmelser er i overensstemmelse med gældende EU-ret.

Artikel 9

Kompetente myndigheder og centralt kontaktpunkt

1. Hver medlemsstat udpeger eller opretter en eller flere kompetente myndigheder, der er ansvarlige for korrekt anvendelse og, hvor det er nødvendigt, håndhævelse af reglerne fastsat i dette direktiv på nationalt plan.

For så vidt angår kritiske enheder i sektorerne i punkt 3 og 4 i tabellen i dette direktivs bilag, skal de kompetente myndigheder i princippet være de kompetente myndigheder, som er omhandlet i artikel 46 i forordning (EU) 2022/2554. For så vidt angår de kritiske enheder i den sektor, der er anført i punkt 8 i tabellen i bilaget til nærværende direktiv, skal de kompetente myndigheder i princippet være de kompetente myndigheder i henhold direktiv (EU) 2022/2555. Medlemsstaterne kan udpege en anden kompetent myndighed for sektorerne i punkt 3, 4 og 8 i tabellen i bilaget til nærværende direktiv i overensstemmelse med eksisterende nationale rammer.

Hvor medlemsstaterne udpeger eller opretter mere end én kompetent myndighed, skal de klart angive hver berørt myndigheds opgaver og sikre, at de samarbejder effektivt om at udføre deres opgaver i henhold til dette direktiv, herunder med hensyn til udpegelsen af et centralt kontaktpunkt og dets aktiviteter, der er omhandlet i stk. 2.

2. Hver medlemsstat udpeger eller opretter et centralt kontaktpunkt til at varetage en forbindelsesfunktion med henblik på at sikre grænseoverskridende samarbejde med de andre medlemsstaters centrale kontaktpunkter og Gruppen for Kritiske Enheders Modstandsdygtighed omhandlet i artikel 19 (»centralt kontaktpunkt«). Hvis det er relevant, udpeger en medlemsstat sit centrale kontaktpunkt inden for en kompetent myndighed. Hvis det er relevant, kan en medlemsstat bestemme, at dens centrale kontaktpunkt også udøver en forbindelsesfunktion med Kommissionen og sikrer samarbejde med tredjelande.

3. Senest den 17. juli 2028 og derefter hvert andet år forelægger de centrale kontaktpunkter en sammenfattende rapport for Kommissionen og for Gruppen for Kritiske Enheders Modstandsdygtighed omhandlet i artikel 19 om de underretninger, de har modtaget, herunder antallet af underretninger, arten af de hændelser, der er underrettet om, og de tiltag, der er taget i overensstemmelse med artikel 15, stk. 3.

Kommissionen udarbejder i samarbejde med Gruppen for Kritiske Enheders Modstandsdygtighed en fælles rapporteringsmodel. De kompetente myndigheder kan anvende denne fælles rapporteringsmodel på frivillig basis med henblik på at forelægge sammenfattende rapporter som omhandlet i første afsnit.

4. Hver medlemsstat sikrer, at dens kompetente myndighed og dets centrale kontaktpunkt har beføjelser og tilstrækkelige finansielle, menneskelige og tekniske ressourcer til på en virkningsfuld og effektiv måde at kunne udføre de opgaver, som de har fået pålagt.

5. Hver medlemsstat sikrer, at dens kompetente myndighed, når det er hensigtsmæssigt og i overensstemmelse med EU-retten og national ret, hører og samarbejder med andre relevante nationale myndigheder, herunder myndigheder med ansvar for civilbeskyttelse, retshåndhævelse og beskyttelse af personoplysninger, samt med kritiske enheder og med relevante interesserede parter.

6. Hver medlemsstat sikrer, at dens kompetente myndighed i henhold til dette direktiv samarbejder og udveksler oplysninger med kompetente myndigheder i henhold til direktiv (EU) 2022/2555 om cybersikkerhedsrisici, cybertrusler og cyberhændelser og ikkecyberrisici, -trusler og -hændelser, som påvirker kritiske enheder, herunder med hensyn til relevante foranstaltninger, der træffes af dens kompetente myndighed og kompetente myndigheder i henhold til direktiv (EU) 2022/2555.

7. Hver medlemsstat underretter Kommissionen om identiteten af den kompetente myndighed og det centrale kontaktpunkt inden for tre måneder efter udpegelsen eller oprettelsen af disse, samt om deres opgaver og ansvarsområder i henhold til dette direktiv, deres kontaktoplysninger og eventuelle efterfølgende ændringer heraf. Medlemsstaterne underretter Kommissionen, hvis de beslutter at udpege andre myndigheder end dem, der er omhandlet i stk. 1, andet afsnit, som de kompetente myndigheder for så vidt angår de kritiske enheder i sektorerne i punkt 3, 4 og 8 i tabellen i bilaget. Hver medlemsstat offentliggør identiteten af den kompetente myndighed og det centrale kontaktpunkt.

8. Kommissionen gør en liste over de centrale kontaktpunkter offentligt tilgængelig.

Artikel 10

Medlemsstaternes støtte til kritiske enheder

1. Medlemsstaterne støtter kritiske enheder med at styrke deres modstandsdygtighed. Denne støtte kan omfatte udvikling af vejledningsmaterialer og -metoder, støtte til tilrettelæggelse af øvelser for at afprøve deres modstandsdygtighed, og rådgivning og uddannelse af personale i kritiske enheder. Uden at dette berører gældende statsstøtteregler kan medlemsstaterne stille finansielle ressourcer til rådighed for kritiske enheder, hvor det er nødvendigt og begrundet i mål af samfundsmæssig interesse.

2. Hver medlemsstat sikrer, at dens kompetente myndighed samarbejder og udveksler oplysninger og god praksis med kritiske enheder i de sektorer, der er anført i bilaget.

3. Medlemsstaterne letter frivillig udveksling af oplysninger mellem kritiske enheder vedrørende spørgsmål, der er omfattet af dette direktiv, i overensstemmelse med EU-retten og national ret om navnlig klassificerede og følsomme informationer, konkurrence og beskyttelse af personoplysninger.

Artikel 11

Samarbejde mellem medlemsstaterne

1. Når det er relevant, konsulterer medlemsstaterne hinanden vedrørende kritiske enheder med henblik på at sikre en konsekvent anvendelse af dette direktiv. Sådanne konsultationer skal navnlig finde sted vedrørende kritiske enheder, der:

a) anvender kritisk infrastruktur, som er fysisk sammenkoblet mellem to eller flere medlemsstater

b) er en del af selskabsstrukturer, som er sammenkoblet eller forbundet med kritiske enheder i en anden medlemsstat

c) er blevet identificeret som kritiske enheder i en medlemsstat, og som leverer væsentlige tjenester til eller i andre medlemsstater.

2. De i stk. 1 omhandlede konsultationer tager sigte på at styrke kritiske enheders modstandsdygtighed og, hvor det er muligt, mindske disses administrative byrde.

KAPITEL III

KRITISKE ENHEDERS MODSTANDSDYGTIGHED

Artikel 12

Kritiske enheders risikovurdering

1. Uanset fristen i artikel 6, stk. 3, andet afsnit, sikrer medlemsstaterne, at kritiske enheder inden for ni måneder efter modtagelsen af den i artikel 6, stk. 3, omhandlede underretning, når det er nødvendigt efterfølgende, og mindst hvert fjerde år, på grundlag af medlemsstatsrisikovurderinger og andre relevante informationskilder, foretager en risikovurdering for at vurdere alle relevante risici, der kunne forstyrre leveringen af deres væsentlige tjenester (»kritiske enheders risikovurderinger«).

2. Kritiske enheders risikovurderinger skal tage højde for alle relevante naturlige og menneskeskabte risici, der kunne føre til en hændelse, herunder af tværsektoriel eller grænseoverskridende karakter, ulykker, naturkatastrofer, folkesundhedskriser og hybride trusler og andre antagonistiske trusler, herunder terrorhandlinger som fastsat i direktiv (EU) 2017/541. En kritisk enheds risikovurdering skal tage hensyn til det omfang andre sektorer anført i bilaget afhænger af den væsentlige tjeneste, der leveres af den kritiske enhed, og det omfang den kritiske enheds afhænger af væsentlige tjenester, der leveres af andre enheder i sådanne andre sektorer, herunder i nabomedlemsstater og tredjelande hvor det er relevant.

Hvor en kritisk enhed har foretaget andre risikovurderinger eller udarbejdet dokumenter i henhold til forpligtelser i andre retsakter, der er relevante for dens risikovurdering, kan den anvende disse vurderinger og dokumenter til at opfylde de krav, der er fastsat i denne artikel. Ved udøvelsen af sine tilsynsfunktioner kan den kompetente myndighed erklære, at en kritisk enheds eksisterende risikovurdering, som behandler de risici og det omfang af afhængighed, der er omhandlet i dette stykkes første afsnit, helt eller delvist opfylder forpligtelserne i henhold til denne artikel.

Artikel 13

Kritiske enheders modstandsdygtighedsforanstaltninger

1. Medlemsstaterne sikrer, at kritiske enheder træffer passende og forholdsmæssige tekniske, sikkerhedsmæssige og organisatoriske foranstaltninger for at sikre deres modstandsdygtighed på grundlag af de relevante oplysninger, som medlemsstaterne har givet om medlemsstatsrisikovurderingen, og af resultaterne af de kritiske enheders risikovurderinger, herunder foranstaltninger, der er nødvendige for at:

a) forhindre hændelser i at indtræffe under behørig hensyntagen til katastroferisikoreduktions- og klimatilpasningsforanstaltninger

b) sikre tilstrækkelig fysisk beskyttelse af deres lokaler og kritiske infrastruktur under behørig hensyntagen til f.eks. hegn, barrierer, værktøjer og rutiner til overvågning af perimetre, detektionsudstyr og adgangskontrol

c) reagere på, modstå og afbøde følgerne af hændelser under behørig hensyntagen til gennemførelsen af risiko- og krisestyringsprocedurer og -protokoller samt varslingsrutiner

d) sikre genopretning efter hændelser under behørig hensyntagen til forretningskontinuitetsforanstaltninger og identifikation af alternative forsyningskæder for at genoptage leveringen af væsentlige tjenester

e) sikre passende medarbejdersikkerhedsstyring under behørig hensyntagen til foranstaltninger såsom fastsættelse af kategorier af personale, der udøver kritiske funktioner, fastlæggelse af adgangsrettigheder til lokaler, kritisk infrastruktur og følsomme oplysninger, fastsættelse af procedurer for baggrundskontrol i overensstemmelse med artikel 14 og udpegelse af kategorier af personer, som er forpligtet til at gennemgå sådanne baggrundskontrol, samt fastlæggelse af passende uddannelseskrav og kvalifikationer

f) øge bevidstheden blandt det relevante personale om de foranstaltninger, der er omhandlet i litra a)-e), under behørig hensyntagen til uddannelseskurser, informationsmateriale og øvelser.

Med henblik på første afsnits litra e) sikrer medlemsstaterne, at kritiske enheder tager hensyn til eksterne tjenesteudbyderes personale, når der fastsættes kategorier af personale, som udøver kritiske funktioner.

2. Medlemsstaterne sikrer, at kritiske enheder har indført og anvender en plan for modstandsdygtighed eller et eller flere tilsvarende dokumenter, der beskriver foranstaltningerne truffet i henhold til stk. 1. Hvis kritiske enheder har udarbejdet dokumenter eller truffet foranstaltninger i henhold til forpligtelser i andre retsakter, der er relevante for foranstaltningerne omhandlet i stk. 1, kan de anvende disse dokumenter og foranstaltninger til at opfylde de krav, der er fastsat i denne artikel. Den kompetente myndighed kan ved udøvelsen af sine tilsynsfunktioner erklære, at en kritisk enheds eksisterende modstandsdygtighedsstyrkende foranstaltninger, der på en passende og forholdsmæssig måde tager hånd om de tekniske, sikkerhedsmæssige og organisatoriske foranstaltninger, som er omhandlet i stk. 1, helt eller delvist opfylder forpligtelserne i henhold til denne artikel.

3. Medlemsstaterne sikrer, at hver kritisk enhed udpeger en forbindelsesofficer eller tilsvarende som kontaktpunkt for de kompetente myndigheder.

4. Efter anmodning fra en medlemsstat, der har identificeret en kritisk enhed, og med samtykke fra den berørte kritiske enhed tilrettelægger Kommissionen rådgivende missioner i overensstemmelse med de ordninger, som er fastsat i artikel 18, stk. 6, 8 og 9, for at rådgive den kritiske enhed om opfyldelsen af dens forpligtelser i henhold til kapitel III. Den rådgivende mission aflægger rapport til Kommissionen, den pågældende medlemsstat og den berørte kritiske enhed om sine resultater.

5. Kommissionen vedtager efter høring af Gruppen for Kritiske Enheders Modstandsdygtighed omhandlet i artikel 19 ikkebindende retningslinjer for nærmere at præcisere de tekniske, sikkerhedsmæssige og organisatoriske foranstaltninger, der kan træffes i henhold til denne artikels stk. 1.

6. Kommissionen vedtager gennemførelsesretsakter med henblik på at fastsætte de nødvendige tekniske og metodiske specifikationer vedrørende anvendelsen af de i denne artikels stk. 1 omhandlede foranstaltninger. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 24, stk. 2.

Artikel 14

Baggrundskontrol

1. Medlemsstaterne angiver, på hvilke betingelser en kritisk enhed i behørigt begrundede tilfælde og under hensyntagen til medlemsstatsrisikovurderingen har tilladelse til at indgive anmodninger om baggrundskontrol af personer, der:

a) varetager følsomme opgaver i eller til fordel for en kritisk enhed, navnlig vedrørende den kritiske enheds modstandsdygtighed

b) er bemyndiget til at få direkte adgang eller fjernadgang til en kritisk enheds lokaler, oplysninger eller kontrolsystemer, herunder i forbindelse med den kritiske enheds sikkerhed

c) overvejes ansat i stillinger, der hører under kriterierne i litra a) eller b).

2. Anmodningers som omhandlet i denne artikels stk. 1 vurderes inden for en rimelig frist og behandles 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 ([37]). Baggrundskontrol skal være forholdsmæssig og strengt begrænset til, hvad der er nødvendigt. Den foretages udelukkende med henblik på at vurdere en potentiel sikkerhedsrisiko for den berørte kritiske enhed.

3. En baggrundskontrol som omhandlet i stk. 1 skal mindst:

a) bekræfte identiteten af den person, der er genstand for baggrundskontrollen

b) kontrollere strafferegistrene for den pågældende person for så vidt angår lovovertrædelser, der ville være relevante for en bestemt stilling.

Når medlemsstater foretager baggrundskontrol, skal de anvende det europæiske informationssystem vedrørende strafferegistre i overensstemmelse med procedurerne i rammeafgørelse 2009/315/RIA og, hvor det er relevant og finder anvendelse, forordning (EU) 2019/816 med henblik på indhentning af oplysninger fra andre medlemsstaters strafferegistre. De centrale myndigheder omhandlet i artikel 3, stk. 1, i rammeafgørelse 2009/315/RIA og i artikel 3, nr. 5), i forordning (EU) 2019/816, besvarer anmodninger om sådanne oplysninger inden for ti arbejdsdage efter datoen for modtagelsen af anmodningen i overensstemmelse med artikel 8, stk. 1, i rammeafgørelse 2009/315/RIA.

([37]) 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).

Artikel 15

Underretning om hændelser

1. Medlemsstaterne sikrer, at kritiske enheder uden unødigt ophold underretter den kompetente myndighed om hændelser, der i betydelig grad forstyrrer eller har potentiale til i betydelig grad at forstyrre leveringen af væsentlige tjenester. Medlemsstaterne sikrer, at kritiske enheder, med mindre det operationelt ikke er muligt, indgiver en første underretning senest 24 timer, efter at være blevet opmærksom på en hændelse, efterfulgt, hvor det er relevant, af en detaljeret rapport senest en måned derefter. Med henblik på at fastslå en forstyrrelses omfang tages navnlig følgende kriterier i betragtning:

a) antallet og andelen af brugere, der er berørt af forstyrrelsen

b) forstyrrelsens varigheden

c) det geografiske område, der er berørt af forstyrrelsen, idet der tages hensyn til, om det er et geografisk isoleret område.

Hvor en hændelse har eller kunne have betydelig indvirkning på kontinuiteten i leveringen af væsentlige tjenester til eller i seks eller flere medlemsstater, underretter de kompetente myndigheder i de medlemsstater, der er berørt af hændelsen, Kommissionen om en denne hændelse.

2. Underretninger som omhandlet i stk. 1, første afsnit, skal indeholde alle tilgængelige oplysninger, der er nødvendige for, at den kompetente myndighed kan forstå hændelsens art, årsag og mulige konsekvenser, herunder alle tilgængelige oplysninger, der er nødvendige for at fastslå hændelsens eventuelle grænseoverskridende indvirkning. Sådanne underretninger medfører ikke et øget ansvar for kritiske enheder.

3. På grundlag af oplysningerne leveret af en kritisk enhed i en underretning som omhandlet i stk. 1 orienterer den relevante kompetente myndighed via det centrale kontaktpunkt andre berørte medlemsstaters centrale kontaktpunkter, hvis hændelsen har eller kunne have betydelig indvirkning på kritiske enheder og kontinuiteten i leveringen af væsentlige tjenester til eller i en eller flere andre medlemsstater.

Centrale kontaktpunkter, der fremsender og modtager oplysninger i medfør af første afsnit, behandler i overensstemmelse med EU-retten eller national ret disse oplysninger på en måde, der respekterer deres fortrolighed og beskytter den berørte kritiske enheds sikkerhed og kommercielle interesser.

4. Så snart som muligt efter modtagelse af en underretning som omhandlet i stk. 1 giver den kompetente myndighed den berørte kritiske enhed relevante opfølgende oplysninger, herunder oplysninger, som kunne understøtte en effektiv reaktion fra denne kritiske enhed på den pågældende hændelse. Medlemsstaterne orienterer offentligheden, hvor de vurderer, at det vil være i offentlighedens interesse at gøre det.

Artikel 16

Standarder

For at fremme en konvergerende gennemførelse af dette direktiv, og hvor det er hensigtsmæssigt og uden at pålægge, eller diskriminere til fordel for, anvendelse af en bestemt type teknologi, tilskynder medlemsstaterne til anvendelsen af europæiske og internationale standarder og tekniske specifikationer af relevans for sikkerheds- og modstandsdygtighedsforanstaltninger, som finder anvendelse på kritiske enheder.

KAPITEL IV

KRITISKE ENHEDER AF SÆRLIG EUROPÆISK BETYDNING

Artikel 17

Identifikation af kritiske enheder af særlig europæisk betydning

1. En enhed betragtes som en kritisk enhed af særlig europæisk betydning, hvor den:

a) er blevet identificeret som en kritisk enhed i henhold til artikel 6, stk. 1

b) leverer de samme eller lignende væsentlige tjenester til eller i seks eller flere medlemsstater og

c) er blevet underrettet i henhold til nærværende artikels stk. 3.

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

Kommissionen konsulterer den kompetente myndighed i den medlemsstat, der identificerede en kritisk enhed som omhandlet i første afsnit, andre berørte medlemsstaters kompetente myndigheder og den pågældende kritiske enhed. Under disse konsultationer oplyser hver medlemsstat Kommissionen, såfremt den finder, at de tjenester, som leveres til denne medlemsstat af den kritiske enhed, er væsentlige tjenester.

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

4. Dette kapitel finder anvendelse på den berørte kritiske enhed af særlig europæisk betydning fra datoen for modtagelse af den underretning, der er omhandlet i denne artikels stk. 3.

Artikel 18

Rådgivende missioner

1. Efter anmodning fra en medlemsstat, som har identificeret en kritisk enhed af særlig europæisk betydning som en kritisk enhed i henhold til artikel 6, stk. 1, tilrettelægger Kommissionen en rådgivende mission for at vurdere de foranstaltninger, som denne kritiske enhed har truffet for at opfylde sine forpligtelser i henhold til kapitel III.

2. På eget initiativ eller efter anmodning fra en eller flere medlemsstater, hvortil eller hvori den væsentlige tjeneste leveres, og forudsat at den medlemsstat, som har identificeret en kritisk enhed af særlig europæisk betydning som en kritisk enhed i henhold til artikel 6, stk. 1, giver sit samtykke dertil, tilrettelægger Kommissionen en rådgivende mission som omhandlet i nærværende artikels stk. 1.

3. Efter en begrundet anmodning fra Kommissionen eller en eller flere medlemsstater, hvortil eller hvori den væsentlige tjeneste leveres, giver den medlemsstat, som har identificeret en kritisk enhed af særlig europæisk betydning som en kritisk enhed i henhold til artikel 6, stk. 1, Kommissionen følgende:

a) de relevante dele af den kritiske enheds risikovurdering

b) en oversigt over relevante foranstaltninger, der er truffet i overensstemmelse med artikel 13

c) tilsyns- eller håndhævelsestiltag, herunder vurderinger af overholdelse eller udstedte påbud, som den kompetente myndighed har taget i henhold til artikel 21 og 22 med hensyn til den pågældende kritiske enhed.

4. Den rådgivende mission aflægger inden for tre måneder efter afslutningen af den rådgivende mission rapport om sine resultater til Kommissionen, til den medlemsstat, der har identificeret en kritisk enhed af særlig europæisk betydning som en kritisk enhed i henhold til artikel 6, stk. 1, til de medlemsstater, hvortil eller hvori den væsentlige tjeneste leveres, og til den pågældende kritiske enhed.

De medlemsstater, hvortil eller hvori den væsentlige tjeneste leveres, analyserer den i første afsnit omhandlede rapport og rådgiver, hvor det er nødvendigt, Kommissionen om, hvorvidt den kritiske enhed af særlig europæisk betydning opfylder sine forpligtelser i henhold til kapitel III, og, hvis det er relevant, hvilke foranstaltninger der kunne træffes for at forbedre den pågældende kritiske enheds modstandsdygtighed.

Kommissionen meddeler på grundlag af den rådgivning, der er omhandlet i dette stykkes andet afsnit, den medlemsstat, som har identificeret en kritisk enhed af særlig europæisk betydning som en kritisk enhed i henhold til artikel 6, stk. 1, de medlemsstater, hvortil og hvori den væsentlige tjeneste leveres, og den pågældende kritiske enhed en udtalelse om, hvorvidt den pågældende kritiske enhed opfylder sine forpligtelser i henhold til kapitel III, og, hvis det er relevant, hvilke foranstaltninger der kunne træffes for at forbedre den pågældende kritiske enheds modstandsdygtighed.

Den medlemsstat, der har identificeret en kritisk enhed af særlig europæisk betydning som en kritisk enhed i henhold til artikel 6, stk. 1, sikrer, at dens kompetente myndighed og den berørte kritiske enhed tager hensyn til den i dette stykkes tredje afsnit omhandlede udtalelse, og giver Kommissionen og de medlemsstater, hvortil eller hvori den væsentlige tjeneste leveres, oplysninger om de foranstaltninger, som den har truffet i medfør af denne udtalelse.

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

Kommissionen tilrettelægger programmet for hver rådgivende mission i samråd med medlemmerne af den pågældende rådgivende mission og efter aftale med den medlemsstat, som har identificeret en kritisk enhed af særlig europæisk betydning som en kritisk enhed i henhold til artikel 6, stk. 1.

6. Kommissionen vedtager en gennemførelsesretsakt med regler for de proceduremæssige ordninger for anmodninger om tilrettelæggelse af rådgivende missioner, for behandling af sådanne anmodninger, for gennemførelse af og rapporter om rådgivende missioner og for behandling af meddelelsen om Kommissionens udtalelse omhandlet i denne artikels stk. 4, tredje afsnit, og om de foranstaltninger, der er truffet, under behørig hensyntagen til de pågældende oplysningers fortrolighed og kommercielle følsomhed. Denne gennemførelsesretsakt vedtages efter undersøgelsesproceduren, jf. artikel 24, stk. 2.

7. Medlemsstaterne sikrer, at kritiske enheder af særlig europæisk betydning giver rådgivende missioner adgang til oplysninger, systemer og faciliteter, der vedrører levering af deres væsentlige tjenester, og som er nødvendige for at gennemføre den pågældende rådgivende mission.

8. Rådgivende missioner gennemføres i overensstemmelse med gældende national ret i den medlemsstat, hvor de finder sted, idet den pågældende medlemsstats ansvar for national sikkerhed og beskyttelse af sine sikkerhedsmæssige interesser respekteres.

9. Ved tilrettelæggelsen af rådgivende missioner tager Kommissionen hensyn til rapporter om eventuelle inspektioner foretaget af Kommissionen i henhold til forordning (EF) nr. 725/2004 og (EF) nr. 300/2008 og til rapporter om enhver overvågning, som Kommissionen har foretaget i henhold til direktiv 2005/65/EF vedrørende den berørte kritiske enhed.

10. Kommissionen orienterer Gruppen for Kritiske Enheders Modstandsdygtighed omhandlet i artikel 19, når der tilrettelægges en rådgivende mission. Den medlemsstat, hvor en rådgivende mission har fundet sted, og Kommissionen orienterer også Gruppen for Kritiske Enheders Modstandsdygtighed om den rådgivende missions vigtigste resultater og de indhøstede erfaringer med henblik på at fremme gensidig læring.

KAPITEL V

SAMARBEJDE OG RAPPORTERING

Artikel 19

Gruppen for Kritiske Enheders Modstandsdygtighed

1. Der nedsættes hermed en Gruppe for Kritiske Enheders Modstandsdygtighed. Gruppen for Kritiske Enheders Modstandsdygtighed støtter Kommissionen og letter samarbejdet mellem medlemsstaterne og udvekslingen af oplysninger om spørgsmål vedrørende dette direktiv.

2. Gruppen for Kritiske Enheders Modstandsdygtighed består af repræsentanter for medlemsstaterne og Kommissionen, hvor det er hensigtsmæssigt med en sikkerhedsgodkendelse. Hvor det er relevant for udførelsen af Gruppen for Kritiske Enheders Modstandsdygtigheds opgaver, kan den indbyde relevante interessenter til at deltage i sit arbejde. Hvis Europa-Parlamentet anmoder herom, kan Kommissionen indbyde eksperter fra Europa-Parlamentet til at deltage i møder i Gruppen for Kritiske Enheders Modstandsdygtighed.

Kommissionens repræsentant er formand for Gruppen for Kritiske Enheders Modstandsdygtighed.

3. Gruppen for Kritiske Enheders Modstandsdygtighed har følgende opgaver:

a) at støtte Kommissionen med at bistå medlemsstaterne med at styrke deres kapacitet til at bidrage til at sikre kritiske enheders modstandsdygtighed i overensstemmelse med dette direktiv

b) at analysere strategierne med henblik på at identificere bedste praksis med hensyn til strategierne

c) at lette udveksling af bedste praksis med hensyn til medlemsstaternes identifikation af kritiske enheder i henhold til artikel 6, stk. 1, herunder vedrørende grænseoverskridende og tværsektoriel afhængighed og med hensyn til risici og hændelser

d) hvis det er relevant, at bidrage med hensyn til spørgsmål vedrørende dette direktiv til dokumenter om modstandsdygtighed på EU-plan

e) at bidrage til udarbejdelsen af de i artikel 7, stk. 3, og artikel 13, stk. 5, omhandlede retningslinjer og efter anmodning eventuelle delegerede retsakter eller gennemførelsesretsakter vedtaget i henhold til dette direktiv

f) at analysere de i artikel 9, stk. 3, omhandlede sammenfattende rapporter med henblik på at fremme udveksling af bedste praksis om de tiltag, der er taget i overensstemmelse med artikel 15, stk. 3

g) at udveksle bedste praksis vedrørende underretning om hændelser omhandlet i artikel 15

h) at drøfte de sammenfattende rapporter om rådgivende missioner og de indhøstede erfaringer i overensstemmelse med artikel 18, stk. 10

i) at udveksle oplysninger og bedste praksis om innovation, forskning og udvikling vedrørende kritiske enheders modstandsdygtighed i overensstemmelse med dette direktiv

j) hvis det er relevant, at udveksle oplysninger om spørgsmål vedrørende kritiske enheders modstandsdygtighed med relevante EU-institutioner, -organer, -kontorer og -agenturer.

4. Senest den 17. januar 2025 og derefter hvert andet år udarbejder Gruppen for Kritiske Enheders Modstandsdygtighed et arbejdsprogram vedrørende tiltag, der skal iværksættes for at gennemføre dens mål og opgaver. Dette arbejdsprogram skal være i overensstemmelse med målene i dette direktiv.

5. Gruppen for Kritiske Enheders Modstandsdygtighed mødes regelmæssigt og under alle omstændigheder mindst én gang om året med den samarbejdsgruppe, der er nedsat i henhold til direktiv (EU) 2022/2555, for at fremme og lette samarbejde og udveksling af oplysninger.

6. Kommissionen kan vedtage gennemførelsesretsakter, hvori der fastlægges proceduremæssige ordninger, som er nødvendige for Gruppen for Kritiske Enheders Modstandsdygtigheds funktion, med respekt af artikel 1, stk. 4. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 24, stk. 2.

7. Kommissionen forelægger Gruppen for Kritiske Enheders Modstandsdygtighed en sammenfattende rapport om de oplysninger, som medlemsstaterne har givet i henhold til artikel 4, stk. 3, og artikel 5, stk. 4, senest den 17. januar 2027, når det er nødvendigt efterfølgende, og mindst hvert fjerde år.

Artikel 20

Støtte fra Kommissionen til kompetente myndigheder og kritiske enheder

1. Kommissionen støtter, hvor det er relevant, medlemsstaterne og kritiske enheder med at opfylde deres forpligtelser i henhold til dette direktiv. Kommissionen udarbejder en oversigt på EU-plan over grænseoverskridende og tværsektorielle risici ved levering af væsentlige tjenester, tilrettelægger de i artikel 13, stk. 4, og artikel 18 omhandlede rådgivende missioner og letter udveksling af oplysninger mellem medlemsstaterne og eksperter i hele Unionen.

2. Kommissionen supplerer medlemsstaternes aktiviteter som omhandlet i artikel 10 ved at udvikle bedste praksis, vejledningsmaterialer og –metoder, og grænseoverskridende uddannelsesaktiviteter og øvelser for at afprøve kritiske enheders modstandsdygtighed.

3. Kommissionen orienterer medlemsstaterne om de finansielle midler på EU-plan, der er til rådighed for medlemsstaterne til at styrke kritiske enheders modstandsdygtighed.

KAPITEL VI

TILSYN OG HÅNDHÆVELSE

Artikel 21

Tilsyn og håndhævelse

1. Med henblik på at vurdere, om de enheder, som medlemsstaterne har identificeret som kritiske enheder i henhold til artikel 6, stk. 1, opfylder forpligtelserne i dette direktiv, sikrer medlemsstaterne, at de kompetente myndigheder har beføjelser og midler til:

a) at foretage inspektioner på stedet af den kritiske infrastruktur og de lokaler, som den kritiske enhed anvender til at levere sine væsentlige tjenester, og eksternt tilsyn med de foranstaltninger, som kritiske enheder har truffet i overensstemmelse med artikel 13

b) at foretage eller kræve revision af kritiske enheder.

2. Medlemsstaterne sikrer, at de kompetente myndigheder har beføjelser og midler til, hvor det er nødvendigt for udførelsen af deres opgaver i henhold til dette direktiv, at kræve, at enhederne i henhold til direktiv (EU) 2022/2555, som medlemsstaterne har identificeret som kritiske enheder i henhold til nærværende direktiv, inden for en rimelig tidsfrist, der fastsættes af disse myndigheder, giver:

a) de oplysninger, der er nødvendige for at vurdere, hvorvidt de foranstaltninger, der træffes af disse enheder for at sikre deres modstandsdygtighed, opfylder kravene i artikel 13

b) dokumentation for faktisk gennemførelse af disse foranstaltninger, herunder resultaterne af en revision foretaget af en uafhængig og kvalificeret revisor udvalgt af denne enhed og foretaget på dennes regning.

Når der anmodes om disse oplysninger, angiver de kompetente myndigheder formålet med kravet og anfører, hvilke oplysninger der kræves.

3. Uden at det berører muligheden for at pålægge sanktioner i overensstemmelse med artikel 22, kan de kompetente myndigheder efter de i denne artikels stk. 1 omhandlede tilsynsforanstaltninger eller vurderingen af de i denne artikels stk. 2 omhandlede oplysninger pålægge de berørte kritiske enheder at træffe de nødvendige og forholdsmæssige foranstaltninger for at afhjælpe enhver konstateret overtrædelse af dette direktiv inden for en rimelig frist, der fastsættes af disse myndigheder, og give disse myndigheder oplysninger om de trufne foranstaltninger. Disse påbud skal navnlig tage hensyn til overtrædelsens grovhed.

4. Medlemsstaterne sikrer, at de i stk. 1, 2 og 3 omhandlede beføjelser kun kan udøves med forbehold af passende garantier. Disse garantier skal navnlig sikre, at en sådan udøvelse finder sted på en objektiv, gennemsigtig og forholdsmæssig måde, og at de berørte kritiske enheders rettigheder og legitime interesser såsom beskyttelse af forretningshemmeligheder garanteres behørigt, herunder deres ret til at blive hørt, til et forsvar og til effektive retsmidler ved en uafhængig domstol.

5. Medlemsstaterne sikrer, at en kompetent myndighed i henhold til dette direktiv, hvor den vurderer en kritisk enheds overholdelse i henhold til denne artikel, orienterer denne kompetente myndighed de kompetente myndigheder i de berørte medlemsstater i henhold til direktiv (EU) 2022/2555. Med henblik herpå sikrer medlemsstaterne, at kompetente myndigheder i henhold til nærværende direktiv kan anmode de kompetente myndigheder i henhold til direktiv (EU) 2022/2555 om at udøve deres tilsyns- og håndhævelsesbeføjelser over for en enhed i henhold til nævnte direktiv, som er identificeret som en kritisk enhed i henhold til nærværende direktiv. Med henblik herpå sikrer medlemsstaterne, at kompetente myndigheder i henhold til nærværende direktiv samarbejder og udveksler oplysninger med de kompetente myndigheder i henhold til direktiv (EU) 2022/2555.

Artikel 22

Sanktioner

Medlemsstaterne fastsætter regler om sanktioner, der skal anvendes i tilfælde af overtrædelser af de nationale foranstaltninger, der er vedtaget i medfør af dette direktiv, og træffer alle nødvendige foranstaltninger for at sikre, at de gennemføres. Sanktionerne skal være effektive, stå i et rimeligt forhold til overtrædelsen og have afskrækkende virkning. Medlemsstaterne giver senest den 17. oktober 2024 Kommissionen meddelelse om disse regler og foranstaltninger, og underretter den straks om alle senere ændringer, der berører dem.

KAPITEL VII

DELEGEREDE RETSAKTER OG GENNEMFØRELSESRETSAKTER

Artikel 23

Udøvelse af de delegerede beføjelser

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

2. Beføjelsen til at vedtage delegerede retsakter, jf. artikel 5, stk. 1, tillægges Kommissionen for en periode på fem år fra den 16. januar 2023.

3. Den i artikel 5, stk. 1, omhandlede delegation af beføjelser kan til enhver tid tilbagekaldes af Europa-Parlamentet eller Rådet. En afgørelse om tilbagekaldelse bringer delegationen af de beføjelser, der er angivet i den pågældende afgørelse, til ophør. Den får virkning dagen efter offentliggørelsen af afgørelsen i *Den Europæiske Unions Tidende* eller på et senere tidspunkt, der angives i afgørelsen. Den berører ikke gyldigheden af delegerede retsakter, der allerede er i kraft.

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

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

6. En delegeret retsakt vedtaget i henhold til artikel 5, stk. 1, træder kun i kraft, hvis hverken Europa-Parlamentet eller Rådet har gjort indsigelse inden for en frist på to måneder fra meddelelsen af den pågældende retsakt til Europa-Parlamentet og Rådet, eller hvis Europa-Parlamentet og Rådet inden udløbet af denne frist begge har underrettet Kommissionen om, at de ikke agter at gøre indsigelse. Fristen forlænges med to måneder på Europa-Parlamentets eller Rådets initiativ.

Artikel 24

Udvalgsprocedure

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

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

KAPITEL VIII

AFSLUTTENDE BESTEMMELSER

Artikel 25

Rapportering og evaluering

Senest den 17. juli 2027 forelægger Kommissionen en rapport for Europa-Parlamentet og Rådet, hvori vurderes det omfang, hvori de enkelte medlemsstater har truffet de nødvendige foranstaltninger med henblik på at efterleve dette direktiv.

Kommissionen evaluerer regelmæssigt, hvorledes dette direktiv fungerer, og forelægger en rapport til Europa-Parlamentet og Rådet. Denne rapport skal navnlig vurdere dette direktivs merværdi, dets indvirkning med hensyn til at sikre kritiske enheders modstandsdygtighed, og hvorvidt bilaget til direktivet bør ændres. Kommissionen forelægger den første rapport senest den 17. juni 2029. Med henblik på rapportering i henhold til denne artikel tager Kommissionen hensyn til relevante dokumenter fra Gruppen for Kritiske Enheders Modstandsdygtighed.

Artikel 26

Gennemførelse

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

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

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

Artikel 27

Ophævelse af direktiv 2008/114/EF

Direktiv 2008/114/EF ophæves med virkning fra den 18. oktober 2024.

Henvisninger til det ophævede direktiv gælder som henvisninger til nærværende direktiv.

Artikel 28

Ikrafttræden

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

Artikel 29

Adressater

Dette direktiv er rettet til medlemsstaterne.

Udfærdiget i Strasbourg, den 14. december 2022.

På Europa-Parlamentets vegne	*På Rådets vegne*
R. METSOLA	M. BEK
Formand	*Formand*

BILAG

SEKTORER, DELSEKTORER OG ENHEDSKATEGORIER

Sektor	Delsektor	Enhedskategori
1. Energi	a) Elektricitet	— Elektricitetsvirksomheder som defineret i artikel 2, nr. 57), i Europa-Parlamentets og Rådets direktiv (EU) 2019/944 ([1]), der varetager funktionen »levering« som defineret i nævnte direktivs artikel 2, nr. 12)
		— Distributionssystemoperatører som defineret i artikel 2, nr. 29), i direktiv (EU) 2019/944
		— Transmissionssystemoperatører som defineret i artikel 2, nr. 35), i direktiv (EU) 2019/944
		— Producenter som defineret i artikel 2, nr. 38), i direktiv (EU) 2019/944
		— Udpegede elektricitetsmarkedsoperatører som defineret i artikel 2, nr. 8), i Europa-Parlamentets og Rådets forordning (EU) 2019/943 ([2])
		— Markedsdeltagere som defineret i artikel 2, nr. 25), i forordning (EU) 2019/943, der leverer tjenester, der vedrører aggregering, fleksibelt elforbrug eller energilagring som defineret i artikel 2, nr. 18), 20) og 59), i direktiv (EU) 2019/944
	b) Fjernvarme og fjernkøling	— Operatører af fjernvarme eller fjernkøling som defineret i artikel 2, nr. 19), i Europa-Parlamentets og Rådets direktiv (EU) 2018/2001 ([3])
	c) Olie	— Olierørledningsoperatører
		— Operatører af olieproduktionsanlæg, -raffinaderier og -behandlingsanlæg, olielagre og olietransmission
		— Centrale lagerenheder som defineret i artikel 2, litra f), i Rådets direktiv 2009/119/EF ([4])

Sektor	Delsektor	Enhedskategori
	d) Gas	— Forsyningsvirksomheder som defineret i artikel 2, nr. 8), i Europa-Parlamentets og Rådets direktiv 2009/73/EF ([5])
		— Distributionssystemoperatører som defineret i artikel 2, nr. 6), i direktiv 2009/73/EF
		— Transmissionssystemoperatører som defineret i artikel 2, nr. 4), i direktiv 2009/73/EF
		— Lagersystemoperatører som defineret i artikel 2 nr. 10), i direktiv 2009/73/EF
		— LNG-systemoperatører som defineret i artikel 2, nr. 12), i direktiv 2009/73/EF
		— Naturgasvirksomheder som defineret i artikel 2, nr. 1), i direktiv 2009/73/EF
		— Operatører inden for naturgasraffinaderier og -behandlingsanlæg
	e) Brint	— Operatører inden for brintproduktion, -lagring og -transmission
2. Transport	a) Luft	— Luftfartsselskaber som defineret i artikel 3, nr. 4), i forordning (EF) nr. 300/2008, der anvendes til kommercielle formål
		— Lufthavnsdriftsorganer som defineret i artikel 2, nr. 2), i Europa-Parlamentets og Rådets direktiv 2009/12/EF ([6]), lufthavne som defineret i nævnte direktivs artikel 2, nr. 1), herunder de hovedlufthavne, der er anført i afsnit 2 i bilag II, til Europa-Parlamentets og Rådets forordning (EU) nr. 1315/2013 ([7]), og enheder med tilknyttede anlæg i lufthavne
		— Trafikledelses- og kontroloperatører, der udøver flyvekontroltjenester som defineret i artikel 2, nr. 1), i Europa-Parlamentets og Rådets forordning (EF) nr. 549/2004 ([8])

Sektor	Delsektor	Enhedskategori
	b) Jernbane	— Infrastrukturforvaltere som defineret i artikel 3, nr. 2), i Europa-Parlamentets og Rådets direktiv 2012/34/EU ([9])
		— Jernbanevirksomheder som defineret i artikel 3, nr. 1), i direktiv 2012/34/EU og operatører af servicefaciliteter som defineret i nævnte direktivs artikel 3, nr. 12)
	c) Vand	— Rederier, som udfører passager- og godstransport ad indre vandveje, i højsøfarvand eller i kystnært farvand som defineret for søtransport i bilag I til forordning (EF) nr. 725/2004, bortset fra de enkelte fartøjer, som drives af disse rederier
		— Driftsorganer i havne som defineret i artikel 3, nr. 1), i direktiv 2005/65/EF, herunder deres havnefaciliteter som defineret i artikel 2, nr. 11), i forordning (EF) nr. 725/2004, og enheder, der driver anlæg og udstyr i havne
		— Operatører af skibstrafiktjenester som defineret i artikel 3, litra o), i Europa-Parlamentets og Rådets direktiv 2002/59/EF ([10])
	d) Vejtransport	— Vejmyndigheder som defineret i artikel 2, nr. 12), i Kommissionens delegerede forordning (EU) 2015/962 ([11]), der er ansvarlige for trafikledelseskontrol, med undtagelse af offentlige enheder, for hvilke trafikledelse eller drift af intelligente transportsystemer er en ikkevæsentlig del af deres generelle aktivitet
		— Operatører af intelligente transportsystemer som defineret i artikel 4, nr. 1), i Europa-Parlamentets og Rådets direktiv 2010/40/EU ([12])
	e) Offentlig transport	— Operatører af offentlig trafikbetjening som defineret i artikel 2, litra d), i Europa-Parlamentets og Rådets forordning (EF) nr. 1370/2007 ([13])
3. Bankvirksomhed		— Kreditinstitutter som defineret i artikel 4, nr. 1), i forordning (EU) nr. 575/2013
4. Finansiel markedsinfrastruktur		— Operatører af markedspladser som defineret i artikel 4, nr. 24), i direktiv 2014/65/EU
		— Centrale modparter (CCP'er) som defineret i artikel 2, nr. 1), i forordning (EU) nr. 648/2012

Sektor	Delsektor	Enhedskategori
5. Sundhed		— Sundhedstjenesteydere som defineret i artikel 3, litra g), i Europa-Parlamentets og Rådets direktiv 2011/24/EU ([14])
		— EU-referencelaboratorier som omhandlet i artikel 15 i Europa-Parlamentets og Rådets forordning (EU) 2022/2371 ([15])
		— Enheder, der udfører forsknings- og udviklingsaktiviteter vedrørende lægemidler som defineret i artikel 1, nr. 2), i Europa-Parlamentets og Rådets direktiv 2001/83/EF ([16])
		— Enheder, der fremstiller farmaceutiske råvarer og farmaceutiske præparater som omhandlet i hovedafdeling C, hovedgruppe 21, i NACE rev. 2
		— Enheder, som fremstiller medicinsk udstyr, der betragtes som kritisk i en folkesundhedsmæssig-krisesituation (»liste over kritisk medicinsk udstyr til folkesundhedsmæssige krisesituationer«) i den i artikel 22 i Europa-Parlamentets og Rådets forordning (EU) 2022/123 ([17]) anvendte betydning
		— Enheder, der er indehavere af en forhandlingstilladelse som omhandlet i artikel 79 i direktiv 2001/83/EF
6. Drikkevand		— Leverandører og distributører af drikkevand som defineret i artikel 2, nr. 1), litra a), i Europa-Parlamentets og Rådets direktiv (EU) 2020/2184 ([18]), bortset fra distributører, for hvilke distribution af drikkevand er en ikkevæsentlig del af deres generelle aktivitet med distribution af andre råvarer og varer
7. Spildevand		— Virksomheder, der indsamler, bortskaffer eller behandler byspildevand, husspildevand eller industrispildevand som defineret i artikel 2, nr. 1), 2) og 3), i Rådets direktiv 91/271/EØF ([19]), bortset fra virksomheder, for hvilke indsamling, bortskaffelse eller behandling af byspildevand, husspildevand eller industrispildevand er en ikkevæsentlig del af deres generelle aktivitet

Sektor	Delsektor	Enhedskategori
8. Digital infrastruktur		— Udbydere af internetudvekslingspunkter som defineret i artikel 6, nr. 18), i direktiv (EU) 2022/2555
		— DNS-tjenesteudbydere omhandlet i artikel 6, nr. 20), i direktiv (EU) 2022/2555, bortset fra operatører af rodnavneservere
		— topdomænenavneadministratorer som defineret i artikel 6, nr. 21), i direktiv (EU) 2022/2555
		— Udbydere af cloudcomputingtjenester som defineret i artikel 6, nr. 30), i direktiv (EU) 2022/2555
		— Udbydere af datacentertjenester som defineret i artikel 6, nr. 31), i direktiv (EU) 2022/2555
		— Udbydere af indholdsleveringsnetværk som defineret i artikel 6, nr. 32), i direktiv (EU) 2022/2555
		— Tillidstjenesteudbydere som defineret i artikel 3, nr. 19), i Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 ([20])
		— Udbydere af offentlige elektroniske kommunikationsnet som defineret i artikel 2, nr. 8), i Europa-Parlamentets og Rådets direktiv (EU) 2018/1972 ([21])
		— Udbydere af elektroniske kommunikationstjenester i den i artikel 2, nr. 4), i direktiv (EU) 2018/1972 anvendte betydning, for så vidt deres tjenester er offentligt tilgængelige
9. Offentlig forvaltning		— Offentlige forvaltningsenheder under den centrale forvaltning som defineret af medlemsstaterne i overensstemmelse med national ret
10. Rummet		— Operatører af jordbaseret infrastruktur, der ejes, forvaltes og drives af medlemsstater eller private parter, og som understøtter levering af rumbaserede tjenester, undtagen udbydere af offentlige elektroniske kommunikationsnet som defineret i artikel 2, nr. 8), i direktiv (EU) 2018/1972

Sektor	Delsektor	Enhedskategori
11. Produktion, tilvirkning og distribution af fødevarer		— Fødevarevirksomheder som defineret i artikel 3, nr. 2), i Europa-Parlamentets og Rådets forordning (EF) nr. 178/2002 ([22]), der udelukkende beskæftiger sig med logistik og engrosdistribution samt industriel produktion og tilvirkning i stor skala

([1]) Europa-Parlamentets og Rådets direktiv (EU) 2019/944 af 5. juni 2019 om fælles regler for det indre marked for elektricitet og om ændring af direktiv 2012/27/EU (EUT L 158 af 14.6.2019, s. 125).
([2]) Europa-Parlamentets og Rådets forordning (EU) 2019/943 af 5. juni 2019 om det indre marked for elektricitet (EUT L 158 af 14.6.2019, s. 54).
([3]) Europa-Parlamentets og Rådets direktiv (EU) 2018/2001 af 11. december 2018 om fremme af anvendelsen af energi fra vedvarende energikilder (EUT L 328 af 21.12.2018, s. 82).
([4]) Rådets direktiv 2009/119/EF af 14. september 2009 om forpligtelse for medlemsstaterne til at holde minimumslagre af råolie og/eller olieprodukter (EUT L 265 af 9.10.2009, s. 9).
([5]) Europa-Parlamentets og Rådets direktiv 2009/73/EF af 13. juli 2009 om fælles regler for det indre marked for naturgas og om ophævelse af direktiv 2003/55/EF (EUT L 211 af 14.8.2009, s. 94).
([6]) Europa-Parlamentets og Rådets direktiv 2009/12/EF af 11. marts 2009 om lufthavnsafgifter (EUT L 70 af 14.3.2009, s. 11).
([7]) Europa-Parlamentets og Rådets forordning (EU) nr. 1315/2013 af 11. december 2013 om Unionens retningslinjer for udvikling af det transeuropæiske transportnet og om ophævelse af afgørelse nr. 661/2010/EU (EUT L 348 af 20.12.2013, s. 1).
([8]) Europa-Parlamentets og Rådets forordning (EF) nr. 549/2004 af 10. marts 2004 om rammerne for oprettelse af et fælles europæisk luftrum (»rammeforordningen«) (EUT L 96 af 31.3.2004, s. 1).
([9]) Europa-Parlamentets og Rådets direktiv 2012/34/EU af 21. november 2012 om oprettelse af et fælles europæisk jernbaneområde (EUT L 343 af 14.12.2012, s. 32).
([10]) Europa-Parlamentets og Rådets direktiv 2002/59/EF af 27. juni 2002 om oprettelse af et trafikovervågnings- og trafikinformationssystem for skibsfarten i Fællesskabet og om ophævelse af Rådets direktiv 93/75/EØF (EFT L 208 af 5.8.2002, s. 10).
([11]) Kommissionens delegerede forordning (EU) 2015/962 af 18. december 2014 om supplerende regler til Europa-Parlamentets og Rådets direktiv 2010/40/EU for så vidt angår tilrådighedsstillelse af EU-dækkende tidstro trafikinformationstjenester (EUT L 157 af 23.6.2015, s. 21).
([12]) Europa-Parlamentets og Rådets direktiv 2010/40/EU af 7. juli 2010 om rammerne for indførelse af intelligente transportsystemer på vejtransportområdet og for grænsefladerne til andre transportformer (EUT L 207 af 6.8.2010, s. 1).
([13]) Europa-Parlamentets og Rådets forordning (EF) nr. 1370/2007 af 23. oktober 2007 om offentlig personbefordring med jernbane og ad vej og om ophævelse af Rådets forordning (EØF) nr. 1191/69 og (EØF) nr. 1107/70 (EUT L 315 af 3.12.2007, s. 1).
([14]) Europa-Parlamentets og Rådets direktiv 2011/24/EU af 9. marts 2011 om patientrettigheder i forbindelse med grænseoverskridende sundhedsydelser (EUT L 88 af 4.4.2011, s. 45).
([15]) Europa-Parlamentets og Rådets forordning (EU) 2022/2371 af 23. november 2022 om alvorlige grænseoverskridende sundhedstrusler og om ophævelse af afgørelse nr. 1082/2013/EU (EUT L 314 af 6.12.2022, s. 26).
([16]) Europa-Parlamentets og Rådets direktiv 2001/83/EF af 6. november 2001 om oprettelse af en fællesskabskodeks for humanmedicinske lægemidler (EFT L 311 af 28.11.2001, s. 67).
([17]) Europa-Parlamentets og Rådets forordning (EU) 2022/123 af 25. januar 2022 om styrkelse af Det Europæiske Lægemiddelagenturs rolle i forbindelse med kriseberedskab og krisestyring med hensyn til lægemidler og medicinsk udstyr (EUT L 20 af 31.1.2022, s. 1).
([18]) Europa-Parlamentets og Rådets direktiv (EU) 2020/2184 af 16. december 2020 om kvaliteten af drikkevand (EUT L 435 af 23.12.2020, s. 1).
([19]) Rådets direktiv 91/271/EØF af 21. maj 1991 om rensning af byspildevand (EFT L 135 af 30.5.1991, s. 40).
([20]) Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF (EUT L 257 af 28.8.2014, s. 73).
([21]) Europa-Parlamentets og Rådets direktiv (EU) 2018/1972 af 11. december 2018 om oprettelse af en europæisk kodeks for elektronisk kommunikation (EUT L 321 af 17.12.2018, s. 36).
([22]) Europa-Parlamentets og Rådets forordning (EF) nr. 178/2002 af 28. januar 2002 om generelle principper og krav i fødevarelovgivningen, om oprettelse af Den Europæiske Fødevaresikkerhedsautoritet og om procedurer vedrørende fødevaresikkerhed (EFT L 31 af 1.2.2002, s. 1).

ISSN 1977-0634 (elektronisk udgave)
ISSN 1725-2520 (papirudgave)

Den Europæiske Unions
Publikationskontor
L-2985 Luxembourg
LUXEMBOURG

DA