DEN EUROPÆISKE UNION

EUROPA-PARLAMENTET **RÅDET**

Bruxelles, den 20. november 2024
(OR. en)

2023/0109(COD) **PE-CONS 94/24**

CYBER 208
TELECOM 218
CADREFIN 109
FIN 595
BUDGET 47
IND 328
JAI 1084
MI 633
DATAPROTECT 247
RELEX 881
CODEC 1588

LOVGIVNINGSMÆSSIGE RETSAKTER OG ANDRE INSTRUMENTER

Vedr.:	EUROPA-PARLAMENTETS OG RÅDETS FORORDNING om foranstaltninger til styrkelse af solidariteten og kapaciteten i Unionen til at opdage, forberede sig og reagere på cybertrusler og -hændelser og om ændring af forordning (EU) 2021/694 (forordning om cybersolidaritet)

EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) 2024/…

af …

om foranstaltninger til styrkelse af solidariteten og kapaciteten i Unionen til at opdage, forberede sig og reagere på cybertrusler og -hændelser og om ændring af forordning (EU) 2021/694 (forordning om cybersolidaritet)

EUROPA-PARLAMENTET OG RÅDET FOR DEN EUROPÆISKE UNION HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel 173, stk. 3, og artikel 322, stk. 1, litra a),

under henvisning til forslag fra Europa-Kommissionen,

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

under henvisning til udtalelse fra Revisionsretten[1],

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

under henvisning til udtalelse fra Regionsudvalget[3],

efter den almindelige lovgivningsprocedure[4], og

ud fra følgende betragtninger:

---

1 Udtalelse af 18.4.2023 (endnu ikke offentliggjort i EUT).
2 EUT C 349 af 29.9.2023, s. 167.
3 EUT C, C/2024/1049, 9.2.2024, ELI: http://data.europa.eu/eli/C/2024/1049/oj.
4 Europa-Parlamentets holdning af 24.4.2024 (endnu ikke offentliggjort i EUT) og Rådets afgørelse af ….

(1) Anvendelsen og afhængigheden af informations- og kommunikationsteknologier er blevet grundlæggende aspekter i alle sektorer af økonomien og samfundet i lyset af den stadig voksende indbyrdes forbundenhed og indbyrdes afhængighed mellem offentlige forvaltninger, virksomheder og borgere på tværs af sektorer og grænser, hvilket samtidig udsætter dem for forskellige sårbarheder.

(2) Cybersikkerhedshændelser er tiltagende både i omfang, hyppighed og virkning på EU-plan og globalt plan, herunder angreb mod forsyningskæden med henblik på cyberspionage, ransomware eller forstyrrelser. De udgør en alvorlig trussel mod netværks- og informationssystemernes funktion. Der ses et trusselsbillede i hastig udvikling, og truslen om mulige omfattende cybersikkerhedshændelser, der kan forårsage betydelige forstyrrelser og skader på kritisk infrastruktur, kræver et øget beredskab i Unionens cybersikkerhedsøkosystem. Truslen rækker langt videre end Ruslands angrebskrig mod Ukraine og er formentlig blivende, når man tager de mange forskellige aktører i betragtning, der er en del af de aktuelle geopolitiske spændinger. Sådanne hændelser kan hindre leveringen af offentlige tjenester, da cyberangreb ofte er rettet mod lokale, regionale eller nationale offentlige tjenester og infrastrukturer, hvor de lokale myndigheder er særligt sårbare, bl.a. på grund af deres begrænsede ressourcer. De kan også hindre udøvelsen af økonomiske aktiviteter, herunder i sektorer af særligt kritisk betydning eller andre kritiske sektorer, medføre betydelige finansielle tab, underminere brugernes tillid, forårsage betydelig skade på Unionens økonomi og demokratiske systemer og muligvis få sundhedsmæssige eller livstruende konsekvenser. Desuden er cybersikkerhedshændelser uforudsigelige, fordi de ofte opstår og udvikler sig hurtigt, fordi de ikke er begrænsede til et specifikt geografisk område, og fordi de forekommer samtidig eller spredes hurtigt til mange lande. Det er afgørende at sikre tæt samarbejde mellem den offentlige og den private sektor, den akademiske verden og medierne.

(3) Det er nødvendigt at styrke industriens og tjenesteydelsernes konkurrenceevne i Unionen på tværs af hele den digitale økonomi og støtte den digitale omstilling i sektorerne ved at styrke cybersikkerhedsniveauet på det digitale indre marked som anbefalet i tre forskellige forslag fra konferencen om Europas fremtid. Der er behov for at øge modstandsdygtigheden hos borgere, virksomheder, herunder mikrovirksomheder, små og mellemstore virksomheder og nystartede virksomheder og enheder, der driver kritisk infrastruktur, over for tiltagende cybertrusler, som kan have ødelæggende samfundsmæssige og økonomiske konsekvenser. Der er derfor behov for investeringer i infrastrukturer og tjenester og opbygning af kapacitet til at udvikle cybersikkerhedsfærdigheder, der muliggør en hurtigere opdagelse af og en hurtigere reaktion på cybertrusler og -hændelser. Desuden har medlemsstaterne har brug for hjælp til bedre at kunne forberede sig på og reagere på, samt brug for hjælp i den indledende genopretning efter væsentlige cybersikkerhedshændelser og omfattende cybersikkerhedshændelser. Ved at bygge videre på de eksisterende strukturer og i tæt samarbejde med disse bør Unionen også øge sin kapacitet på disse områder, navnlig med hensyn til indsamling og analyse af data om cybertrusler og -hændelser.

(4) Unionen har allerede truffet en række foranstaltninger for at mindske sårbarheder og øge kritiske infrastrukturers og enheders modstandsdygtighed over for risici, navnlig Europa-Parlamentets og Rådets forordning (EU) 2019/881[5], Europa-Parlamentets og Rådets direktiv 2013/40/EU[6] og (EU) 2022/2555[7] og Kommissionens henstilling (EU) 2017/1584[8]. Desuden opfordres medlemsstaterne i Rådets henstilling af 8. December 2022 om en EU-dækkende koordineret tilgang til styrkelse af kritisk infrastrukturs modstandsdygtighed til at træffe foranstaltninger og til at samarbejde med hinanden, Kommissionen og andre relevante offentlige myndigheder samt de berørte enheder for at øge modstandsdygtigheden i den kritiske infrastruktur, der anvendes til at levere væsentlige tjenester på det indre marked.

---

5 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).

6 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).

7 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 (EUT L 333 af 27.12.2022, s. 80).

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

(5) De voksende cybersikkerhedsrisici og det generelt komplekse trusselsbillede, hvor der er en klar risiko for, at hændelser spreder sig fra én medlemsstat til andre og fra et tredjeland til Unionen, kræver, at man styrker solidariteten på EU-niveau for bedre at kunne opdage, forberede sig og reagere på og komme sig efter cybertrusler og -hændelser, navnlig ved at styrke de eksisterende strukturers kapacitet. Endvidere opfordrede Rådets konklusioner af 23. maj 2022 om udviklingen af Den Europæiske Unions cyberposition Kommissionen til at fremsætte et forslag om en ny beredskabsfond for cybersikkerhed.

(6) I den fælles meddelelse fra Kommissionen og Unionens høje repræsentant for udenrigsanliggender og sikkerhedspolitik af 10. november 2022 til Europa-Parlamentet og Rådet om EU's politik for cyberforsvar blev EU's cybersolidaritetsinitiativ beskrevet med målsætninger om at styrke EU's fælles situationsbevidsthed og kapacitet til at opdage og reagere på hændelser ved at fremme etableringen af en EU-infrastruktur for sikkerhedsoperationscentre (SOC'er), støtte en gradvis opbygning af en cyberreserve på EU-plan med brug af tjenester fra betroede private udbydere og teste kritiske enheder for potentielle sårbarheder baseret på EU's risikovurderinger.

(7) Det er nødvendigt at styrke situationsbevidsthed og kapaciteten til at opdage cybertrusler og -hændelser i hele Unionen og styrke solidariteten ved at øge medlemsstaternes og Unionens beredskab og kapacitet til at forebygge og reagere på væsentlige cybersikkerhedshændelser og omfattende cybersikkerhedshændelser. Derfor bør et paneuropæisk netværk af cyberknudepunkter ("det europæiske cybersikkerhedsvarslingssystem") etableres for at opbygge koordineret situationsbevidsthed og kapacitet til at opdage hændelser og dermed styrke Unionens kapacitet til at afdække trusler og udveksle informationer; der bør oprettes en cybersikkerhedsberedskabsmekanisme, som efter anmodning fra medlemsstaterne hjælper dem med at forberede sig og reagere på, afbøde virkningen af og påbegynde genopretning efter væsentlige cybersikkerhedshændelser eller omfattende cybersikkerhedshændelser, og for at hjælpe andre brugere med at reagere på væsentlige cybersikkerhedshændelser og cybersikkerhedshændelser svarende til omfattende cybersikkerhedshændelser, og der bør oprettes en europæisk mekanisme til gennemgang af cybersikkerhedshændelser med henblik på at gennemgå og vurdere specifikke væsentlige cybersikkerhedshændelser eller omfattende cybersikkerhedshændelser. Foranstaltningerne i henhold til denne forordning bør gennemføres under behørig hensyntagen til medlemsstaternes kompetencer og bør supplere og ikke overlappe de aktiviteter, der udføres af CSIRT-netværket, det Europæiske Netværk af Forbindelsesorganisationer for Cyberkriser (EU-CyCLONe) eller samarbejdsgruppen (NIS-samarbejdsgruppen), der alle er oprettet ved direktiv (EU) 2022/2555. Disse foranstaltninger berører ikke artikel 107 og 108 i traktaten om Den Europæiske Unions funktionsmåde (TEUF).

(8) For at opfylde disse målsætninger er det nødvendigt at ændre Europa-Parlamentets og Rådets forordning (EU) 2021/694[9] på visse områder. Denne forordning bør navnlig ændre forordning (EU) 2021/694 for så vidt angår tilføjelsen af nye operationelle mål for det europæiske cybersikkerhedsvarslingssystem og cybersikkerhedsberedskabsmekanismen under specifikt mål nr. 3 i programmet for et digitalt Europa, hvis formål er at sikre det digitale indre markeds modstandsdygtighed, integritet og troværdighed, styrke kapaciteten til at overvåge cyberangreb og -trusler og reagere på dem og styrke det grænseoverskridende samarbejde og den grænseoverskridende koordination vedrørende cybersikkerhed. Det europæiske cybersikkerhedsvarslingssystem kan spille en vigtig rolle med hensyn til at støtte medlemsstaterne i at foregribe og beskytte sig mod cybertrusler, og EU's cybersikkerhedsreserve kan spille en vigtig rolle med hensyn til at støtte medlemsstaterne, EU's institutioner, organer, kontorer og agenturer og tredjelande, der er associeret til programmet for et digitalt Europa, i at reagere på og afbøde virkningerne af væsentlige cybersikkerhedshændelser, omfattende cybersikkerhedshændelser og cybersikkerhedshændelser svarende til omfattende cybersikkerhedshændelser. Disse virkninger kan omfatte betydelig materiel eller immateriel skade og alvorlige risici for den offentlige sikkerhed. I lyset af de specifikke roller, som det europæiske cybersikkerhedsvarslingssystem og EU's cybersikkerhedsreserve kan spille, bør denne forordning ændre forordning (EU) 2021/694 for så vidt angår deltagelse af retlige enheder, der er etableret i Unionen, men kontrolleres fra tredjelande, hvis der er en reel risiko for, at de nødvendige og tilstrækkelige værktøjer, infrastrukturer og tjenester eller teknologi, ekspertise og kapacitet ikke er tilgængelige i Unionen, og fordelene ved at medtage sådanne enheder opvejer sikkerhedsrisikoen. De særlige betingelser, hvorunder der kan ydes finansiel støtte til foranstaltninger til gennemførelse af det europæiske cybersikkerhedsvarslingssystem og EU's cybersikkerhedsreserve, bør fastlægges, og de forvaltnings- og koordineringsmekanismer, der er nødvendige for at nå de tilsigtede mål, bør defineres. Andre ændringer af forordning (EU) 2021/694 bør omfatte beskrivelse af foreslåede foranstaltninger under de nye operationelle målsætninger og målbare indikatorer til overvågning af gennemførelsen heraf.

---

[9] 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).

(9) Samarbejde med internationale organisationer samt med betroede, ligesindede internationale partnere er afgørende for at styrke Unionens reaktion på cybersikkerhedstrusler og -hændelser. I denne forbindelse bør pålidelige og ligesindede internationale partnere forstås som værende lande, der deler principperne, der førte til Unionens oprettelse, nemlig demokrati, retsstatsprincippet, menneskerettighedernes og de grundlæggende frihedsrettigheders universalitet og udelelighed, respekt for den menneskelige værdighed, principperne om lighed og solidaritet og respekt for principperne i De Forenede Nationers pagt og folkeretten, og som ikke underminerer Unionens eller dens medlemsstaters væsentlige sikkerhedsinteresser. Et sådant samarbejde kan også være gavnligt med hensyn til foranstaltningerne truffet i henhold til denne forordning, navnlig det europæiske cybersikkerhedsvarslingssystem og EU's cybersikkerhedsreserve. Forordning (EU) 2021/694 bør afhængig af visse tilgængeligheds- og sikkerhedsbetingelser fastsætte, at udbud vedrørende det europæiske cybersikkerhedsvarslingssystem og EU's cybersikkerhedsreserve er åbne for retlige enheder, der kontrolleres fra tredjelande, forudsat at sikkerhedskravene er opfyldt. I forbindelse med vurderingen af sikkerhedsrisikoen ved at åbne udbud på denne måde er det vigtigt at tage hensyn til de principper og værdier, som Unionen deler med ligesindede internationale partnere, når disse principper og værdier vedrører Unionens væsentlige sikkerhedsinteresser. Når sådanne sikkerhedskrav overvejes i henhold til forordning (EU) 2021/694, kan der desuden tages hensyn til flere elementer, såsom en enheds selskabsstruktur og beslutningsproces, datasikkerhed og sikkerheden af klassificerede eller følsomme oplysninger og sikring af, at foranstaltningens resultater ikke er underlagt kontrol eller begrænsninger fra tredjelande, der ikke er godkendt til deltagelse.

(10) Finansieringen af foranstaltninger under denne forordning bør fastsættes i forordning (EU) 2021/694, som fortsat bør være den relevante basisretsakt for disse foranstaltninger, der hører under specifik målsætning nr. 3 i programmet for et digitalt Europa. Der vil i de relevante arbejdsprogrammer blive fastsat særlige betingelser for deltagelse i de enkelte foranstaltninger i overensstemmelse med forordning (EU) 2021/694.

(11) Horisontale finansielle regler, der er vedtaget af Europa-Parlamentet og Rådet på grundlag af artikel 322 i TEUF, finder anvendelse på denne forordning. Disse regler er fastsat i Europa-Parlamentets og Rådets forordning (EU, Euratom) 2024/2509[10] og fastlægger navnlig proceduren for opstilling og gennemførelse af Unionens budget og indeholder bestemmelser om kontrol af de finansielle aktørers ansvar. Regler vedtaget på grundlag af artikel 322 i TEUF omfatter også en generel ordning vedrørende konditionalitet med henblik på beskyttelse af Unionens budget som fastsat i Europa-Parlamentets og Rådets forordning (EU, Euratom) 2020/2092[11].

---

[10] Europa-Parlamentets og Rådets forordning (EU, Euratom) 2024/2509 af 23. september 2024 om de finansielle regler vedrørende Unionens almindelige budget (OJ L, 2024/2509, 26.9.2024, ELI: http://data.europa.eu/eli/reg/2024/2509/oj).

[11] Europa-Parlamentets og Rådets forordning (EU, Euratom) 2020/2092 af 16. december 2020 om en generel ordning med konditionalitet til beskyttelse af Unionens budget (EUT L 433 I af 22.12.2020, s. 1, ELI: http://data.europa.eu/eli/reg/2020/2092/oj).

(12) Selv om forebyggelses- og beredskabsforanstaltninger er afgørende for at øge Unionens modstandsdygtighed over for væsentlige cybersikkerhedshændelser, omfattende cybersikkerhedshændelser og cybersikkerhedshændelser svarende til omfattende cybersikkerhedshændelser, er forekomsten, timingen og omfanget af sådanne hændelser i sagens natur uforudsigelige. De finansielle ressourcer, der er nødvendige for at sikre en passende reaktion, kan variere betydeligt fra år til år og bør kunne stilles til rådighed med det samme. Hvis budgetprincippet om forudsigelighed skal kunne forenes med nødvendigheden af at kunne reagere hurtigt på nye behov, er det nødvendigt at tilpasse den finansielle gennemførelse af arbejdsprogrammerne. I tillæg til fremførsel af bevillinger, der er godkendt i henhold til artikel 12, stk. 4, i forordning(EU, Euratom) 2024/2509, er det derfor hensigtsmæssigt at tillade fremførslen af uudnyttede bevillinger, men kun til det følgende år og udelukkende til EU's cybersikkerhedsreserve og de aktioner der støtter gensidig bistand.

(13) For mere effektivt at forebygge, vurdere, reagere på og sikre genopretning efter cybertrusler og -hændelser er det nødvendigt at opbygge en mere omfattende viden om truslerne mod kritiske aktiver og infrastrukturer på Unionens område, herunder geografiske fordeling, sammenhæng og mulige virkninger i tilfælde af cyberangreb, der påvirker disse infrastrukturer. En proaktiv tilgang til at udpege, afbøde og forebygge cybertrusler nødvendiggør en styrkelse af avancerede opdagelseskapaciteter. Det europæiske cybersikkerhedsvarslingssystem bør bestå af flere interoperable grænseoverskridende cyberknudepunkter, som hver samler tre eller flere nationale cyberknudepunkter. Infrastrukturen bør tjene nationale og europæiske cybersikkerhedsinteresser og -behov, den nyeste teknologi til avanceret indsamling af relevante data og information, anonymiseret hvor det er hensigtsmæssigt, og analyseværktøjer til behandling af anonymiserede data bør udnyttes, den koordinerede kapacitet til opdagelse og– forvaltning af cybertrusler bør styrkes, og en situationsbevidsthed i realtid bør opbygges. Infrastrukturen skal tjene til forbedring af cyberniveau ved at forbedre opdagelse samt aggregering og analyse af data og information med henblik på at forebygge cybertrusler og -hændelser og dermed supplere og støtte Unionens enheder og netværk med ansvar for cyberkrisestyring i Unionen, navnlig EU-CyCLONe.

(14) Deltagelse i det europæiske cybersikkerhedsvarslingssystem er frivilligt for medlemsstaterne. De enkelte medlemsstater bør udpege en enkelt enhed på nationalt plan, der har til opgave at koordinere aktiviteter til opdagelse af cybertrusler i den pågældende medlemsstat. Disse nationale cyberknudepunkter bør fungere som reference- og indgangspunkt på nationalt plan for deltagelse i det europæiske cybersikkerhedsvarslingssystem, og de bør sikre, at information om cybertrusler fra offentlige og private enheder deles og indsamles på nationalt plan på en effektiv og koordineret måde. De nationale cyberknudepunkter kan styrke samarbejdet og informationsudvekslingen mellem offentlige og private enheder og kan også støtte udvekslingen af relevante data og information med relevante sektorspecifikke og tværsektorielle fællesskaber, herunder relevante industrielle informationsudvekslings- og analysecentre (ISAC'er). Et tæt og koordineret samarbejde mellem offentlige og private enheder er centralt, hvis Unionens cybermodstandsdygtighed skal styrkes. Et sådant samarbejde er særlig værdifuldt i forbindelse med udvekslingen af cybermæssige trusselsefterretninger for at forbedre den aktive cyberbeskyttelse. Som led i et sådant samarbejde og sådan informationsudveksling kan de nationale cyberknudepunkter anmode om og modtage specifik information. De nationale cyberknudepunkter er hverken forpligtet eller bemyndiget i henhold til denne forordning til at følge op på sådanne anmodninger. Hvor det er relevant og i overensstemmelse med EU-retten og national ret, kan den information, der anmodes om eller modtages, omfatte telemetri-, sensor- og loggingdata fra enheder såsom udbydere af administrerede sikkerhedstjenester, der opererer i sektorer af særligt kritisk betydning eller andre kritiske sektorer i den pågældende medlemsstat, med henblik på at fremme en hurtig opdagelse af potentielle cybertrusler og -hændelser på et tidligere tidspunkt og dermed forbedre situationsbevidstheden. Hvis det nationale cyberknudepunkt ikke er den kompetente myndighed, der er udpeget eller oprettet af den relevante medlemsstat i henhold til artikel 8, stk. 1, i direktiv (EU) 2022/2555, er det afgørende, at det koordinerer med den pågældende kompetente myndighed i forbindelse med anmodninger om og modtagelse af sådanne data.

(15) Som en del af det europæiske cybersikkerhedsvarslingssystem bør der oprettes en række grænseoverskridende cyberknudepunkter. Disse grænseoverskridende cyberknudepunkter skal samle de nationale cyberknudepunkter fra mindst tre medlemsstater for at sikre, at fordelene ved grænseoverskridende trusselsopdagelse og informationsdeling og -styring udnyttes fuldt ud. Den overordnede målsætning for de grænseoverskridende cyberknudepunkter bør være at styrke kapaciteten til at analysere, forebygge og opdage cybersikkerhedstrusler og støtte frembringelsen af cybermæssige trusselsefterretninger af høj kvalitet, navnlig gennem deling af relevant information, anonymiseret hvor det er hensigtsmæssigt, i et pålideligt og sikkert miljø fra forskellige offentlige eller private kilder samt gennem udveksling og fælles anvendelse af avancerede værktøjer og fælles udvikling af opdagelses-, analyse- og forebyggelseskapaciteter i et pålideligt og sikkert miljø. Cyberknudepunkter bør stille ny supplerende kapacitet til rådighed, der bygger på og supplerer eksisterende SOC'er og CSIRT'er og andre relevante aktører, herunder CSIRT-netværket.

(16) En medlemsstat, der udvælges af Det Europæiske Industri-, Teknologi- og Forskningskompetencecenter for Cybersikkerhed (ECCC) oprettet ved Europa-Parlamentets og Rådets forordning (EU) 2021/887[12] efter en indkaldelse af interessetilkendegivelser med henblik på at oprette eller forbedre kapaciteten hos et nationalt cyberknudepunkt, bør i samarbejde med ECCC indkøbe relevante værktøjer, infrastrukturer og tjenester. En sådan medlemsstat bør være berettiget til at modtage tilskud til drift af værktøjer, infrastrukturer eller tjenester. Et værtskonsortium, bestående af mindst tre medlemsstater, som er blevet udvalgt af ECCC efter en indkaldelse af interessetilkendegivelser med henblik på at oprette eller forbedre kapaciteten hos et grænseoverskridende cyberknudepunkt, bør indkøbe relevante værktøjer, infrastrukturer eller tjenester i samarbejde med ECCC. Værtskonsortiet bør være berettiget til at modtage et tilskud til drift af værktøjer, infrastrukturer eller tjenester. Udbudsproceduren med henblik på indkøb af de relevante værktøjer, infrastrukturer eller tjenester bør gennemføres i fællesskab af ECCC og relevante ordregivende myndigheder fra medlemsstaterne, der udvælges efter sådanne indkaldelser af interessetilkendegivelser. Sådanne udbud bør overholde artikel 168, stk. 2, i forordning (EU) 2024/2509 og ECCC's finansielle regler. Private enheder bør derfor ikke være berettigede til at deltage i indkaldelser af interessetilkendegivelser med henblik på fælles indkøb af værktøjer, infrastrukturer eller tjenester med ECCC eller til at modtage tilskud til drift af disse værktøjer, infrastrukturer og tjenester. Medlemsstaterne bør dog kunne inddrage private enheder i oprettelsen, forbedringen og driften af deres nationale cyberknudepunkter og grænseoverskridende cyberknudepunkter på andre måder, som de finder hensigtsmæssige, i overensstemmelse med EU-retten og national ret. Private enheder kan også være berettigede til at modtage EU-finansiering i henhold til forordning (EU) 2021/887 med henblik på at yde støtte til nationale cyberknudepunkter.

---

[12] Europa-Parlamentets og Rådets forordning (EU) 2021/887 af 20. maj 2021 om oprettelse af Det Europæiske Industri-, Teknologi- og Forskningskompetencecenter for Cybersikkerhed og Netværket af Nationale Koordinationscentre (EUT L 202 af 8.6.2021, s. 1, ELI: http://data.europa.eu/eli/reg/2021/887/oj).

(17) For at øge opdagelsen af cybertrusler og forbedre situationsbevidstheden i Unionen bør en medlemsstat, der udvælges efter en indkaldelse af interessetilkendegivelser med henblik på at oprette eller styrke kapaciteten hos et nationalt cyberknudepunkt, forpligte sig til at ansøge om at deltage i et grænseoverskridende cyberknudepunkt. Hvis en medlemsstat ikke deltager i et grænseoverskridende cyberknudepunkt senest to år efter den dato, hvor værktøjerne, infrastrukturerne eller tjenesterne blev erhvervet, eller hvor den modtog tilskudsfinansiering, alt efter hvad der indtraf først, bør medlemsstaten ikke være berettiget til yderligere EU-støtteaktioner inden for rammerne af det europæiske cybersikkerhedsvarslingssystem med henblik på at øge det nationale cyberknudepunkts kapacitet. I sådanne tilfælde kan enheder fra medlemsstaterne stadig deltage i indkaldelser af forslag om andre emner under programmet for et digitalt Europa eller andre EU-finansieringsprogrammer, herunder indkaldelser vedrørende kapaciteter til opdagelse og informationsudveksling om cybertrusler og -hændelser, forudsat at disse enheder opfylder de støtteberettigelseskriterier, der er fastsat i disse programmer.

(18) CSIRT'er udveksler oplysninger i CSIRT-netværket i overensstemmelse med direktiv (EU) 2022/2555. Det europæiske cybersikkerhedsvarslingssystem skal udgøre en ny kapacitet, der supplerer CSIRT-netværket, ved at bidrage til at opbygge et EU-situationsbevidsthed, der gør det muligt at styrke CSIRT-netværkets kapacitet. Grænseoverskridende cyberknudepunkter bør koordinere og arbejde tæt sammen med CSIRT-netværket. De bør handle ved at samle data og dele relevant information, anonymiseret hvor det er hensigtsmæssigt, om cybersikkerhedstrusler fra offentlige og private enheder, øge værdien af sådanne data og information gennem ekspertanalyser og fælles erhvervede infrastrukturer og avancerede værktøjer og bidrage til Unionens teknologiske suverænitet, dens åbne strategiske autonomi, konkurrenceevne og modstandsdygtighed og til udviklingen af Unionens kapaciteter.

(19) Grænseoverskridende cyberknudepunkter bør fungere som centrale knudepunkter, hvor relevante data og cybermæssige trusselsefterretninger generelt sammenstilles, og de bør muliggøre udveksling af trusselsoplysninger blandt en lang række forskellige interessenter, såsom IT-beredskabsenheder (CERT'er), CSIRT'er, ISAC'er og operatører af kritisk infrastruktur. Medlemmerne af værtskonsortiet bør i konsortieaftalen angive de relevante oplysninger, der skal udveksles mellem deltagerne i det pågældende grænseoverskridende cyberknudepunkt. De oplysninger, der udveksles mellem deltagerne i et grænseoverskridende cyberknudepunkt, kan f.eks. omfatte data fra netværk og sensorer, trusselsefterretningsfeeds, kompromitteringsindikatorer og kontekstualiserede oplysninger om hændelser, cybertrusler, nærvedshændelser, sårbarheder, teknikker og procedurer, fjendtlige taktikker, specifikke oplysninger om trusselsaktører, cybersikkerhedsadvarsler og anbefalinger vedrørende konfigurationen af cybersikkerhedsværktøjer til at opdage cyberangreb. Desuden bør grænseoverskridende cyberknudepunkter også indgå samarbejdsaftaler med hinanden. Sådanne samarbejdsaftaler bør navnlig præcisere principperne for informationsudveksling og interoperabilitet. Deres bestemmelser om interoperabilitet, navnlig formater og protokoller for informationsudveksling, bør være vejledt af og derfor tage udgangspunkt i interoperationalitetsretningslinjer udstedt af Den Europæiske Unions Agentur for Cybersikkerhed oprettet ved forordning (EU) 2019/881 (ENISA). Disse retningslinjer bør udstedes hurtigt for at sikre, at de grænseoverskridende cyberknudepunkter kan tage dem i betragtning på et tidligt tidspunkt. De bør tage hensyn til internationale standarder og bedste praksis og funktionen af ethvert etableret grænseoverskridende cyberknudepunkt.

(20) Grænseoverskridende cyberknudepunkter og CSIRT-netværket bør arbejde tæt sammen for at sikre synergi og komplementaritet i aktiviteterne. Med henblik herpå bør de nå til enighed om proceduremæssige ordninger for samarbejde og udveksling af relevant information. Dette kan omfatte udveksling af relevant information om cybertrusler og væsentlige cybersikkerhedshændelser og sikring af, at erfaringer med avancerede værktøjer, navnlig kunstig intelligens og dataanalyseteknologi, der anvendes inden for de grænseoverskridende cyberknudepunkter, deles med CSIRT-netværket.

(21) At de relevante myndigheder opbygger et fælles situationsbevidsthed er en nødvendig forudsætning for EU-dækkende beredskab og koordinering vedrørende væsentlige cybersikkerhedshændelser og omfattende cybersikkerhedshændelser. Ved direktiv (EU) 2022/2555 oprettedes EU-CyCLONe for at støtte den koordinerede forvaltning af omfattende cybersikkerhedshændelser og -kriser på operationelt plan og for at sikre regelmæssig udveksling af relevante oplysninger mellem medlemsstaterne og EU's institutioner, organer, kontorer og agenturer. Ved direktiv (EU) 2022/2555 oprettedes også CSIRT-netværket med henblik på at fremme et hurtigt og effektivt operationelt samarbejde mellem medlemsstaterne. Med henblik på at øge situationsbevidstheden og styrke solidariteten bør de grænseoverskridende cyberknudepunkter i situationer, hvor de indhenter oplysninger vedrørende en potentiel eller igangværende omfattende cybersikkerhedshændelse, videregive relevante oplysninger til CSIRT-netværket og som en tidlig varsling underrette EU-CyCLONe. Afhængigt af situationen kan de oplysninger, der skal udveksles, især omfatte tekniske oplysninger, oplysninger om angriberens eller den mulige angriberes kendetegn og motiver og ikke-tekniske oplysninger på overordnet niveau om en potentiel eller igangværende omfattende cybersikkerhedshændelse. I den sammenhæng bør der tages behørigt hensyn til, hvilke oplysninger der er nødvendige, og til den eventuelt følsomme karakter af de udvekslede oplysninger. I direktiv (EU) 2022/2555 genpåpeges også Kommissionens ansvar i forbindelse med EU-civilbeskyttelsesmekanismen, der blev oprettet ved Europa-Parlamentets og Rådets afgørelse 1313/2013/EU[13], og dens ansvar for at udarbejde analytiske rapporter om ordningerne under EU's integrerede ordninger for politisk kriserespons i henhold til Rådets gennemførelsesafgørelse (EU) 2018/1993[14].

---

13 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, ELI: http://data.europa.eu/eli/dec/2013/1313/oj).

14 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, ELI: http://data.europa.eu/eli/dec_impl/2018/1993/oj).

Når grænseoverskridende cyberknudepunkter udveksler relevante oplysninger med og giver tidlige varslinger vedrørende en potentiel eller igangværende omfattende cybersikkerhedshændelse til EU-CyCLONe og CSIRT-netværket, er det afgørende, at disse oplysninger deles gennem disse netværk med medlemsstaternes myndigheder og Kommissionen. I denne forbindelse fastsætter direktiv (EU) 2022/2555, at EU-CyCLONe har til formål 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's institutioner, organer, kontorer og agenturer. EU-CyCLONes opgaver omfatter udvikling af en fælles situationsbevidsthed om sådanne hændelser og kriser. Det er af afgørende betydning, at EU-CyCLONe i overensstemmelse med dette formål og sine opgaver sikrer, at sådanne oplysninger straks deles med de relevante repræsentanter for medlemsstaterne og Kommissionen. Med henblik herpå er det afgørende, at EU-CyCLONes forretningsorden indeholder passende bestemmelser.

(22) Enheder, der deltager i det europæiske cybersikkerhedsvarslingssystem, bør sikre en høj grad af indbyrdes interoperabilitet, herunder, hvor det er relevant, for så vidt angår dataformater, taksonomi, datahåndterings- og dataanalyseværktøjer. De bør også sikre kommunikationskanaler, et minimumsniveau af sikkerhed i applikationslaget, en situationsbevidsthedsoversigtstavle samt indikatorer. Ved vedtagelse af en fælles taksonomi og udvikling af en skabelon til situationsrapporter til beskrivelse af årsagerne til opdagede cybertrusler og -risici bør der tages hensyn til det arbejde, der allerede er udført i forbindelse med gennemførelsen af direktiv (EU) 2022/2555.

(23) For at muliggøre udveksling af relevante data og oplysninger om cybersikkerhedstrusler fra forskellige kilder i stor skala i et pålideligt og sikkert miljø bør enheder, der deltager i det europæiske cybersikkerhedsvarslingssystem, udstyres med avancerede, særligt sikre værktøjer, udstyr og infrastrukturer samt kvalificeret personale. Dermed bør det blive muligt at forbedre den kollektive opdagelseskapacitet og tilvejebringe rettidige advarsler til myndigheder og relevante enheder, navnlig ved at anvende de nyeste teknologier inden for kunstig intelligens og dataanalyse.

(24) Gennem indsamling, analyse, deling og udveksling af relevante data og oplysninger bør det europæiske cybersikkerhedsvarslingssystem kunne styrke Unionens teknologiske suverænitet og åbne strategiske autonomi på områderne for cybersikkerhed, konkurrenceevne og modstandsdygtighed. Sammenlægning af udvalgte data af høj kvalitet kan også bidrage til udviklingen af avancerede teknologier inden for kunstig intelligens og dataanalyse. Menneskelig kontrol er afgørende, og med henblik herpå er en kvalificeret arbejdsstyrke fortsat vigtig for effektivt at samle data af høj kvalitet.

(25) Selv om det europæiske cybersikkerhedsvarslingssystem er et civilt projekt, kan cyberforsvarssektoren udnytte en større civil situationsbevidsthed og en stærkere civil opdagelseskapacitet, der er udviklet med henblik på beskyttelse af kritisk infrastruktur.

(26) Udveksling af oplysninger mellem deltagerne i det europæiske cybersikkerhedsvarslingssystem bør ske i overensstemmelse med eksisterende retlige krav og navnlig Unionens og den nationale databeskyttelseslovgivning samt Unionens konkurrenceregler vedrørende udveksling af oplysninger. Modtageren af oplysningerne bør, i det omfang behandlingen af personoplysninger er nødvendig, gennemføre tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og frihedsrettigheder og tilintetgøre data, så snart de ikke længere er nødvendige til det angivne formål, og underrette den enhed, der stiller oplysningerne til rådighed, om, at oplysningerne er blevet destrueret.

(27) Bevarelse af fortrolighed og informationssikkerhed er af afgørende betydning for alle tre søjler i denne forordning, hvad enten det drejer sig om at tilskynde til informationsdeling eller -udveksling inden for rammerne af det europæiske cybersikkerhedsvarslingssystem, bevare interesserne hos de enheder, der ansøger om støtte under cybersikkerhedsberedskabsmekanismen, eller sikre, at rapporter indgivet under den europæiske mekanisme til gennemgang af cybersikkerhedshændelser kan give nyttige erfaringer uden at indvirke negativt på de enheder, der er berørt af hændelserne. Medlemsstaternes og enhedernes deltagelse i disse mekanismer afhænger af tillidsforholdet mellem deres komponenter. Hvis oplysninger er fortrolige i henhold til EU-regler eller nationale regler, bør delingen eller udvekslingen heraf i henhold til denne forordning begrænses til det, der er relevant og står i rimeligt forhold til formålet med delingen eller udvekslingen. Delingen eller udvekslingen bør også sikre de nævnte oplysningers fortrolighed, herunder beskyttelse af alle berørte enheders sikkerhed og kommercielle interesser. Informationsdeling eller -udveksling i henhold til denne forordning kan finde sted ved hjælp af fortrolighedsaftaler eller vejledning om informationsdistribution såsom traffic light-protokollen (TLP). TLP 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 CSIRT'er og i nogle ISAC'er. Ud over disse generelle krav bør værtskonsortiets aftaler for så vidt angår det europæiske cybersikkerhedsvarslingssystem fastsætte specifikke regler vedrørende betingelserne for informationsdeling inden for det berørte grænseoverskridende cyberknudepunkt. Disse aftaler kan navnlig kræve, at oplysningerne kun deles i overensstemmelse med EU-retten og national ret.

(28) Med hensyn til anvendelsen af EU's cybersikkerhedsreserve er der behov for specifikke fortrolighedsregler. Den vil blive anmodet om, vurdere og yde støtte i en krisesituation og til enheder, der opererer i følsomme sektorer. For at EU's cybersikkerhedsreserve kan fungere effektivt, er det afgørende, at brugere og enheder er i stand til straks at dele og give adgang til alle oplysninger, der er nødvendige for, at hver enhed kan spille en rolle i vurderingen af anmodninger og leveringen af støtte. Denne forordning bør derfor fastsætte, at alle sådanne oplysninger kun anvendes eller deles, hvis det er nødvendigt for driften af EU's cybersikkerhedsreserve, og at oplysninger, der er fortrolige eller klassificerede i henhold til EU-retten eller national ret, kun må anvendes og deles i overensstemmelse med nævnte ret. Desuden bør brugerne altid, hvor det er relevant, kunne anvende informationsudvekslingsprotokoller såsom TLP til yderligere at præcisere begrænsninger. Selv om brugerne har skønsbeføjelser i denne henseende, er det vigtigt, at de ved anvendelsen af sådanne begrænsninger tager hensyn til de mulige konsekvenser, navnlig med hensyn til forsinket vurdering eller levering af de ønskede tjenester. For at sikre effektiviteten af EU's cybersikkerhedsreserve er det vigtigt, at den ordregivende myndighed præciserer disse konsekvenser for brugeren, inden den indgiver en anmodning. Disse beskyttelsesforanstaltninger er begrænset til anmodning om og levering af tjenester fra EU's cybersikkerhedsreserve og påvirker ikke informationsudveksling i andre sammenhænge, f.eks. i forbindelse med EU's cybersikkerhedsreserves indkøb.

(29) I betragtning af de stigende risici og antallet af hændelser, der påvirker medlemsstaterne, er det nødvendigt at oprette et krisestøtteinstrument, nemlig cybersikkerhedsberedskabsmekanismen, for at forbedre Unionens modstandsdygtighed over for væsentlige cybersikkerhedshændelser, omfattende cybersikkerhedshændelser og cybersikkerhedshændelser svarende til omfattende cybersikkerhedshændelser og supplere medlemsstaternes foranstaltninger gennem finansiel nødhjælp til beredskab, indsats og den indledende genopretning af væsentlige tjenester. Da fuld genopretning efter en hændelse er en omfattende proces, hvor funktionen af den enhed, der er berørt af hændelsen, skal genetableres til den status, den havde før hændelsen, og dette kan være en langvarig proces, der medfører betydelige omkostninger, bør støtten fra EU's cybersikkerhedsreserve begrænses til den første fase af genopretningsprocessen, der fører til genetablering af systemernes grundlæggende funktioner. Cybersikkerhedsberedskabsmekanismen bør muliggøre hurtig og effektiv udsendelse af bistand under nærmere fastsatte omstændigheder og på klare betingelser og give mulighed for nøje overvågning og evaluering af, hvordan ressourcerne er blevet anvendt. Mens medlemsstaterne har det primære ansvar for forebyggelse, beredskab og indsats i tilfælde af cybersikkerhedshændelser og -kriser, skal cybersikkerhedsberedskabsmekanismen øge solidariteten mellem medlemsstaterne i overensstemmelse med artikel 3, stk. 3, i traktaten om Den Europæiske Union (TEU).

(30) Cybersikkerhedsberedskabsmekanismen bør yde støtte til medlemsstaterne som supplement til deres egne foranstaltninger og ressourcer og andre eksisterende støttemuligheder i tilfælde af reaktion på og den indledende genopretning efter væsentlige cybersikkerhedshændelser og omfattende cybersikkerhedshændelser såsom de tjenester, der leveres af ENISA i overensstemmelse med dets mandat, den koordinerede indsats og bistanden fra CSIRT-netværket, støtten til afbødende foranstaltninger fra EU-CyCLONe samt gensidig bistand mellem medlemsstaterne, herunder i medfør af artikel 42, stk. 7, i TEU og i det permanente strukturerede samarbejdes (PESCO) cyberberedskabshold oprettet i henhold til Rådets afgørelse (FUSP) 2017/2315[15].
Cybersikkerhedsberedskabsmekanismen bør indgå i løsning af behovet for at sikre, at der er specialiserede ressourcer til rådighed til støtte for beredskab, indsats og genopretning efter sådanne hændelser i hele Unionen og i tredjelande, der er associeret til programmet for et digitalt Europa.

[15] Rådets afgørelse (FUSP) 2017/2315 af 11. december 2017 om etablering af et permanent struktureret samarbejde (PESCO) og fastlæggelse af listen over deltagende medlemsstater (EUT L 331 af 14.12.2017, s. 57, ELI: http://data.europa.eu/eli/dec/2017/2315/2023-05-23).

(31) Denne forordning berører ikke procedurer og rammer for koordinering af kriserespons på EU-plan, navnlig direktiv (EU) 2022/2555, EU-civilbeskyttelsesmekanismen oprettet ved Europa-Parlamentets og Rådets afgørelse 1313/2013/EU[16], IPCR-ordninger og Kommissionens henstilling (EU) 2017/1584[17]. Støtte under cybersikkerhedsberedskabsmekanismen kan supplere den bistand, der ydes inden for rammerne af den fælles udenrigs- og sikkerhedspolitik og den fælles sikkerheds- og forsvarspolitik, herunder gennem cyberberedskabsholdene, under hensyntagen til cybersikkerhedsberedskabsmekanismens civile karakter. Støtte, der ydes inden for rammerne af cybersikkerhedsberedskabsmekanismen, kan supplere foranstaltninger, der gennemføres inden for rammerne af artikel 42, stk. 7, i TEU, herunder bistand fra en medlemsstat til en anden medlemsstat, eller udgøre en del af den fælles indsats mellem Unionen og medlemsstaterne eller i situationer, der er omhandlet i artikel 222 i TEUF. Gennemførelsen af denne forordning bør også koordineres med gennemførelsen af foranstaltninger i henhold til den cyberdiplomatiske værktøjskasse, hvor det er relevant.

---

16 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).

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

(32) Den bistand, der ydes i henhold til denne forordning, bør støtte og supplere de foranstaltninger, som medlemsstaterne træffer på nationalt plan. Med henblik herpå bør der sikres et tæt samarbejde og samråd mellem Kommissionen, ENISA, medlemsstaterne og, hvor det er relevant, ECCC. Når en medlemsstat anmoder om støtte i henhold til cybersikkerhedsberedskabsmekanismen, bør den fremlægge relevante oplysninger, der begrunder behovet for støtte.

(33) I henhold til direktiv (EU) 2022/2555 skal medlemsstaterne udpege eller oprette en eller flere cyberkrisestyringsmyndigheder og sikre, at de har tilstrækkelige ressourcer til at udføre deres opgaver effektivt og virkningsfuldt. I henhold til direktivet skal medlemsstaterne endvidere identificere kapaciteter, aktiver og procedurer, der kan indsættes i tilfælde af en krise, og vedtage en national omfattende beredskabsplan for cybersikkerhedshændelser og -kriser, hvor målsætningerne og ordningerne vedrørende håndtering af væsentlige cybersikkerhedshændelser og -kriser er fastsat. Medlemsstaterne skal også oprette en eller flere CSIRT'er, der har ansvar for håndtering af hændelser efter en veldefineret proces, der som minimum dækker de sektorer, delsektorer og typer af enhed, der er omfattet af nævnte direktivs anvendelsesområde, og sikre, at de har tilstrækkelige ressourcer til effektivt at udføre deres opgaver. Denne forordning berører ikke Kommissionens rolle med hensyn til at sikre, at medlemsstaterne overholder forpligtelserne i direktiv (EU) 2022/2555. Cybersikkerhedsberedskabsmekanismen bør yde bistand til foranstaltninger, der har til formål at styrke beredskabet og indsatsen i forbindelse med hændelser for at afbøde virkningerne af væsentlige cybersikkerhedshændelser og omfattende cybersikkerhedshændelser, støtte den indledende genopretning eller genetablere de grundlæggende funktioner af de tjenester, der leveres af enheder, der opererer i sektorer af særligt kritisk betydning eller enheder, der opererer i andre kritiske sektorer.

(34) For at fremme en konsekvent tilgang og styrke sikkerheden i hele Unionen og dens indre marked bør der som led i beredskabsforanstaltningerne ydes støtte til en koordineret afprøvning og vurdering af cybersikkerheden i enheder, der opererer i sektorer af særligt kritisk betydning, der er udpeget i direktiv (EU) 2022/2555, herunder gennem øvelser og uddannelse. Med henblik herpå bør Kommissionen efter høring af ENISA, NIS-samarbejdsgruppen og EU-CyCLONe regelmæssigt udpege relevante sektorer eller delsektorer, som bør være berettigede til at modtage finansiel støtte til koordineret beredskabstestning på EU-plan. Sektorerne eller delsektorerne bør udvælges fra sektorerne af særlig kritisk betydning anført i bilag I til direktiv (EU) 2022/2555. De koordinerede beredskabstest bør baseres på fælles risikoscenarier og -metoder.

Udvælgelsen af sektorer og udarbejdelsen af risikoscenarier bør tage højde for relevante risikovurderinger og risikoscenarier på EU-plan, herunder behovet for at undgå overlapning, såsom den risikoevaluering og de risikoscenarier, der anbefales i Rådets konklusioner om udviklingen af Den Europæiske Unions cyberniveau, foretaget af Kommissionen, Unionens højtstående repræsentant for udenrigsanliggender og sikkerhedspolitik ("den højtstående repræsentant") og NIS-samarbejdsgruppen i samarbejde med relevante civile og militære organer og agenturer og etablerede netværk, herunder EU-CyCLONe, samt den risikovurdering af kommunikationsnet og -infrastrukturer, der er anmodet om i den fælles ministerielle Nevers-indkaldelse, og som gennemføres af NIS-samarbejdsgruppen med støtte fra Kommissionen og ENISA og i samarbejde med Sammenslutningen af Europæiske Tilsynsmyndigheder inden for Elektronisk Kommunikation oprettet ved Europa-Parlamentets og Rådets forordning (EU) 2018/1971[18], de på EU-plan koordinerede sikkerhedsrisikovurderinger af kritiske forsyningskæder, der skal foretages i henhold til artikel 22 i direktiv (EU) 2022/2555, og afprøvning af digital operationel modstandsdygtighed, jf. Europa-Parlamentets og Rådets forordning (EU) 2022/2554[19]. Ved udvælgelse af sektorer bør der også tages hensyn til Rådets henstilling om en EU-dækkende koordineret tilgang til styrkelse af kritisk infrastrukturs modstandsdygtighed.

---

18 Europa-Parlamentets og Rådets forordning (EU) 2018/1971 af 11. december 2018 om oprettelse af Sammenslutningen af Europæiske Tilsynsmyndigheder inden for Elektronisk Kommunikation (BEREC) og Agenturet for Støtte til BEREC (BEREC-kontoret), om ændring af forordning (EU) 2015/2120 og om ophævelse af forordning (EF) nr. 1211/2009 (EUT L 321 af 17.12.2018, s. 1).

19 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).

(35) Derudover bør cybersikkerhedsberedskabsmekanismen yde støtte til andre beredskabsforanstaltninger og støtte beredskabet i andre sektorer, der ikke er omfattet af den koordinerede beredskabstest af enheder, der opererer i sektorer af særligt kritisk betydning, eller enheder, der opererer i andre kritiske sektorer. Disse foranstaltninger kan omfatte forskellige typer af national beredskabsaktivitet.

(36) Når medlemsstaterne modtager tilskud til støtte med henblik på at støtte beredskabsforanstaltninger, kan enheder i sektorer af særligt kritisk betydning deltage i disse foranstaltninger på frivillig basis. Det er god praksis, at de deltagende enheder efter sådanne foranstaltninger udarbejder en afhjælpningsplan med henblik på at gennemføre eventuelle anbefalinger om specifikke tiltag for i videst muligt omfang at kunne drage fordel af beredskabsforanstaltningen. Selv om det er vigtigt, at medlemsstaterne som led i foranstaltningerne anmoder om, at deltagende enheder udarbejder og gennemfører sådanne afhjælpningsplaner, er medlemsstaterne hverken forpligtet eller bemyndiget i henhold til denne forordning til at følge op på sådanne anmodninger. Sådanne anmodninger berører ikke kravene til enheder og de kompetente myndigheders tilsynsbeføjelser i overensstemmelse med direktiv (EU) 2022/2555.

(37) Cybersikkerhedsberedskabsmekanismen bør yde støtte til indsatsen i forbindelse med hændelser for at afbøde virkningerne af væsentlige cybersikkerhedshændelser, omfattende cybersikkerhedshændelser og cybersikkerhedshændelser svarende til omfattende cybersikkerhedshændelser for at støtte den indledende genopretning eller genoprette væsentlige tjenesters funktion. Den bør, hvor det er relevant, supplere EU-civilbeskyttelsesmekanismen for at sikre en samlet tilgang til indsatsen over for følgerne af hændelser for borgerne.

(38) Cybersikkerhedsberedskabsmekanismen bør støtte teknisk bistand fra en medlemsstat til en anden medlemsstat, der er berørt af en væsentlig cybersikkerhedshændelse eller en omfattende cybersikkerhedshændelse, herunder fra CSIRT'er som omhandlet i artikel 11, stk. 3, litra f), i direktiv (EU) 2022/2555. Medlemsstater, der yder sådan bistand, bør have mulighed for at indgive anmodning om dækning af omkostninger i forbindelse med udsendelse af eksperthold inden for rammerne af gensidig bistand. De støtteberettigede omkostninger kan omfatte udgifter til rejser, indkvartering og daglige udgifter for cybersikkerhedseksperter.

(39) I betragtning af den væsentlige rolle, som private virksomheder spiller i forbindelse med opdagelse, beredskab og reaktion på omfattende cybersikkerhedshændelser og cybersikkerhedshændelser svarende til omfattende cybersikkerhedshændelser, er det vigtigt at anerkende værdien af frivilligt pro bono-samarbejde med sådanne virksomheder, hvorved de tilbyder tjenester uden betaling i tilfælde af omfattende cybersikkerhedshændelser og kriser og cybersikkerhedshændelser svarende til omfattende cybersikkerhedshændelser og kriser. ENISA kan i samarbejde med EU-CyCLONe overvåge udviklingen af sådanne pro bono-initiativer og fremme overholdelsen af de kriterier, der gælder for betroede udbydere af administrerede sikkerhedstjenester i henhold til denne forordning, herunder med hensyn til private virksomhedernes troværdighed, deres erfaring samt deres evne til at håndtere følsomme oplysninger på en sikker måde.

(40) Som led i cybersikkerhedsberedskabsmekanismen bør der gradvist oprettes en cybersikkerhedsreserve på EU-plan bestående af tjenester fra betroede udbydere af administrerede sikkerhedstjenester til støtte for indsatsen og iværksættelse af de indledende genopretningsforanstaltninger i tilfælde af væsentlige cybersikkerhedshændelser, omfattende cybersikkerhedshændelser eller cybersikkerhedshændelser svarende til omfattende cybersikkerhedshændelser, der påvirker medlemsstaterne, EU's institutioner, organer eller agenturer eller tredjelande, der er associeret til programmet for et digitalt Europa. EU's cybersikkerhedsreserve bør sikre, at tjenesterne er tilgængelige og parate. Den bør derfor omfatte tjenester, der er omfattet af forhåndsforpligtelser, herunder f.eks. kapaciteter, der er på standby og kan indsættes med kort varsel. Tjenesterne fra EU's cybersikkerhedsreserve bør tjene til at støtte de nationale myndigheder i at yde bistand til berørte enheder, der opererer i sektorer af særligt kritisk betydning, eller til berørte enheder, der opererer i andre kritiske sektorer, som supplement til deres egne foranstaltninger på nationalt plan. Tjenesterne fra EU's cybersikkerhedsreserve bør også kunne tjene til at støtte EU's institutioner, organer, kontorer og agenturer på lignende betingelser. EU's cybersikkerhedsreserve kan også bidrag til at styrke industriens og tjenesteydelsernes konkurrenceevne i Unionen i hele den digitale økonomi, herunder mikrovirksomheder og små og mellemstore virksomheder samt nystartede virksomheder, bl.a. gennem tilvejebringelse af incitamenter til forskning og innovation. Det er vigtigt at tage hensyn til ENISA's europæiske ramme for cybersikkerhedsfærdigheder, når der indkøbes tjenester til EU's cybersikkerhedsreserve. Når brugere anmoder om støtte fra EU's cybersikkerhedsreserve, bør de i deres ansøgning medtage relevante oplysninger om den berørte enhed og potentielle virkninger, oplysninger om den tjeneste, der anmodes om fra EU's cybersikkerhedsreserve, og specificere hvilken støtte, der ydes til den berørte enhed på nationalt plan, og som der bør tages hensyn til ved vurderingen af ansøgerens anmodning. For at sikre komplementaritet med andre former for støtte, der er til rådighed for den berørte enhed, bør anmodningen også indeholde eventuelle oplysninger om indgåede kontrakter vedrørende reaktioner på hændelser og tjenester med henblik på den indledende genopretning, samt forsikringsaftaler, der eventuelt dækker den pågældende hændelsestype.

(41) For at sikre en effektiv anvendelse af EU-midler bør de tjenester, der er omfattet af EU's cybersikkerhedsreserve, i overensstemmelse med den relevante kontrakt kunne konverteres til beredskabstjenester i forbindelse med forebyggelse af og reaktion på hændelser i tilfælde, hvor disse tjenester ikke anvendes til at reagere på hændelser i det tidsrum, hvor disse tjenester er omfattet af forhåndsforpligtelser. Disse tjenester bør være supplerende til og bør ikke overlappe de beredskabsforanstaltninger, der forvaltes af ECCC.

(42) Anmodninger om støtte fra EU's cybersikkerhedsreserve fra medlemsstaternes cyberkrisestyringsmyndigheder og CSIRT'er eller CERT-EU på vegne af EU's institutioner, organer, kontorer og agenturer bør vurderes af den ordregivende myndighed. Hvis ENISA har fået overdraget forvaltningen og driften af EU's cybersikkerhedsreserve, er ENISA den ordregivende myndighed. Anmodninger om støtte fra tredjelande, der er associeret til programmet for et digitalt Europa, bør vurderes af Kommissionen. For at lette indgivelsen og vurderingen af anmodninger om støtte kan ENISA oprette en sikker platform.

(43) Hvis der modtages flere anmodninger samtidig, bør disse anmodninger prioriteres i overensstemmelse med de i denne forordning fastsatte kriterier. I lyset af denne forordnings generelle mål bør disse kriterier omfatte hændelsens størrelse og alvor, typen af berørt enhed, den potentielle indvirkning af hændelsen på berørte medlemsstater og brugere, hændelsens potentielle grænseoverskridende karakter og risikoen for afsmitning og de foranstaltninger, som brugeren allerede har truffet for at bidrage til indsatsen og den indledende genopretning. I lyset af disse mål og i betragtning af, at anmodninger fra brugere i medlemsstaterne udelukkende har til formål i Unionen at støtte enheder, der opererer i sektorer af særligt kritisk betydning, eller enheder, der opererer i andre kritiske sektorer, bør anmodninger fra brugere i medlemsstater prioriteres højest, hvis kriterierne fører til, at to eller flere anmodninger vurderes som ligestillede. Dette berører ikke eventuelle forpligtelser, som medlemsstaterne måtte have indgået i henhold til relevante værtsaftaler til at træffe foranstaltninger til at beskytte og bistå EU's institutioner, organer, kontorer og agenturer.

(44) Kommissionen bør have det overordnede ansvar for EU-cybersikkerhedsreservens gennemførelse. I betragtning af ENISA's omfattende erfaring med støtteforanstaltningen vedrørende cybersikkerhed er ENISA det mest egnede agentur til at gennemføre EU's cybersikkerhedsreserve, og Kommissionen bør derfor helt eller delvist overdrage driften og forvaltningen af EU's cybersikkerhedsreserve til ENISA, alt efter hvad Kommissionen finder mest hensigtsmæssigt. Overdragelsen bør udføres i overensstemmelse med de gældende regler i forordning (EU) 2024/2509 og bør navnlig være betinget af, at de relevante betingelser for undertegnelse af en bidragsaftale er opfyldt. Alle aspekter af driften og forvaltningen af EU's cybersikkerhedsreserve, der ikke overdrages til ENISA, bør være underlagt direkte forvaltning af Kommissionen, herunder forud for undertegnelsen af bidragsaftalen.

(45) Medlemsstaterne bør spille en central rolle i forbindelse med oprettelsen, udrulningen og perioden efter udrulning af EU's cybersikkerhedsreserve. Da forordning (EU) 2021/694 er den relevante basisretsakt for foranstaltninger til gennemførelse af EU's cybersikkerhedsreserve, bør foranstaltningerne under EU's cybersikkerhedsreserve fastsættes i de arbejdsprogrammer, der er omhandlet i artikel 24 i forordning (EU) 2021/694. I henhold til stk. 6 i nævnte artikel skal disse arbejdsprogrammer vedtages af Kommissionen ved hjælp af gennemførelsesretsakter efter undersøgelsesproceduren. Desuden bør Kommissionen i samarbejde med NIS-samarbejdsgruppen fastlægge prioriteterne for og udviklingen af EU's cybersikkerhedsreserve.

(46) De kontrakter, der indgås inden for rammerne af EU's cybersikkerhedsreserve, bør ikke påvirke forholdet mellem virksomheder og eksisterende forpligtelser mellem den berørte enhed eller brugere og tjenesteudbyderen.

(47) Med henblik på at udvælge private tjenesteudbydere, der skal levere tjenester i forbindelse med EU's cybersikkerhedsreserve, er det nødvendigt at fastsætte et sæt minimumskriterier og -krav, der bør indgå i udbuddet til udvælgelse af udbyderne, for at sikre, at behovene opfyldes hos medlemsstaternes myndigheder, enheder, der opererer i sektorer af særligt kritisk betydning og enheder, der opererer i andre kritiske sektorer. For at imødekomme medlemsstaternes specifikke behov bør den ordregivende myndighed, når den indkøber tjenester til EU's cybersikkerhedsreserve, hvor det er relevant, fastlægge yderligere udvælgelseskriterier og -krav ud over dem, der er fastsat i denne forordning. Det er vigtigt at tilskynde mindre udbydere, der er aktive på regionalt og lokalt plan, til at deltage.

(48) Ved udvælgelsen af udbydere til EU's cybersikkerhedsreserve bør den ordregivende myndighed sikre, at EU's cybersikkerhedsreserve som helhed omfatter udbydere, der er i stand til at imødekomme brugernes sprogkrav. Med henblik herpå bør den ordregivende myndighed, inden den udarbejder udbudsbetingelserne, undersøge, om de potentielle brugere af EU's cybersikkerhedsreserve har specifikke sprogkrav, så støttetjenester under EU's cybersikkerhedsreserve kan leveres på et af EU-institutionernes eller medlemsstaternes officielle sprog, som brugeren eller den berørte enhed sandsynligvis vil forstå. Hvis en bruger kræver, at støttetjenester under EU's cybersikkerhedsreserve leveres på mere end ét sprog, og disse tjenester er blevet indkøbt på disse sprog med tanke på den pågældende bruger, bør brugeren i anmodningen om støtte fra EU's cybersikkerhedsreserve kunne angive, på hvilke af disse sprog tjenesterne bør leveres i forbindelse med den specifikke hændelse, der giver anledning til anmodningen.

(49) For at støtte etableringen af EU's cybersikkerhedsreserve er det vigtigt, at Kommissionen anmoder ENISA om at udarbejde et forslag til en cybersikkerhedscertificeringsordning for kandidater i henhold til forordning (EU) 2019/881 for administrerede sikkerhedstjenester på de områder, der er omfattet af cybersikkerhedsberedskabsmekanismen.

(50) For at støtte målsætningerne i denne forordning om at fremme fælles situationsbevidsthed, styrke Unionens modstandsdygtighed og muliggøre en effektiv reaktion på væsentlige cybersikkerhedshændelser og omfattende cybersikkerhedshændelser bør Kommissionen eller EU-CyCLONe kunne anmode ENISA, med støtte fra CSIRT-netværket og efter godkendelse fra den berørte medlemsstat, om at gennemgå og vurdere cybertrusler, kendte sårbarheder, der kan udnyttes, og afbødende foranstaltninger i forbindelse med en specifik væsentlig cybersikkerhedshændelse eller omfattende cybersikkerhedshændelse. Efter gennemførelsen af en gennemgang og vurdering af en hændelse bør ENISA udarbejde en rapport om hændelsen i samarbejde med den berørte medlemsstat, relevante interessenter, herunder repræsentanter fra den private sektor, Kommissionen og andre relevante EU-institutioner, -organer, -kontorer og -agenturer. På grundlag af samarbejdet med interessenter, herunder den private sektor, bør rapporten om gennemgang af specifikke hændelser have til formål at vurdere årsagerne til, virkningerne af og modvirkningen af en hændelse, efter at den er indtruffet. Der bør lægges særlig vægt på oplysninger og erfaringer, der indmeldes af udbydere af administrerede sikkerhedstjenester, som opfylder betingelserne om højeste faglige integritet, upartiskhed og den nødvendige tekniske ekspertise som krævet i denne forordning. Rapporten bør leveres til EU-CyCLONe, CSIRT-netværket og Kommissionen og bør have for vane at underrette deres og ENISA's arbejde. Når hændelsen vedrører et tredjeland, der er associeret til programmet for et digitalt Europa, bør Kommissionen også udlevere rapporten til den højtstående repræsentant.

(51) I betragtning af cyberangrebs uforudsigelige karakter og det forhold, at de ofte ikke kun berører et specifikt geografisk område og medfører høj risiko for afsmittende virkninger, bidrager styrkelsen af nabolandenes modstandsdygtighed og deres evne til at reagere effektivt på væsentlige cybersikkerhedshændelser og cybersikkerhedshændelser svarende til omfattende cybersikkerhedshændelser til beskyttelsen af Unionen som helhed, og navnlig dens indre marked og industrien. Sådanne aktiviteter kan bidrage yderligere til EU's cyberdiplomati. Derfor bør tredjelande, der er associeret til programmet for et digitalt Europa, kunne anmode om støtte fra EU's cybersikkerhedsreserve på alle eller dele af deres områder, hvis dette er fastsat i den aftale, hvorigennem tredjelandet er associeret til programmet for et digitalt Europa. Finansieringen til tredjelande, der er associeret til programmet for et digitalt Europa, bør støttes af Unionen inden for rammerne af relevante partnerskaber og finansieringsinstrumenter for disse lande. Støtten bør omfatte tjenester inden for reaktion på og den indledende genopretning efter væsentlige cybersikkerhedshændelser eller cybersikkerhedshændelser svarende til omfattende cybersikkerhedshændelser.

(52) De betingelser, der er fastsat for EU's cybersikkerhedsreserve og betroede udbydere af administrerede sikkerhedstjenester i denne forordning, bør finde anvendelse, når der ydes støtte til tredjelande, der er associeret til programmet for et digitalt Europa. Tredjelande, der er associeret til programmet for et digitalt Europa, bør kunne anmode om støtte fra EU's cybersikkerhedsreserve, når de enheder, som tjenesterne skal rettes mod, og for hvilke tredjelandene anmoder om støtte fra EU's cybersikkerhedsreserve, er enheder, der opererer i sektorer af særligt kritisk betydning eller enheder, der opererer i andre kritiske sektorer, og når de opdagede hændelser fører til betydelige operationelle forstyrrelser eller kan have afsmittende virkninger i Unionen. Tredjelande, der er associeret til programmet for et digitalt Europa, bør kun være berettigede til at modtage støtte, hvis den aftale, hvorigennem de er associeret til programmet for et digitalt Europa, specifikt indeholder bestemmelser om en sådan støtte. Desuden bør sådanne tredjelande kun være støtteberettigede, så længe tre kriterier er opfyldt. For det første bør tredjelandet fuldt ud overholde de relevante betingelser i den pågældende aftale. For det andet bør tredjelandet i betragtning af EU's cybersikkerhedsreserves supplerende karakter have taget passende skridt til at forberede sig på væsentlige cybersikkerhedshændelser eller cybersikkerhedshændelser svarende til omfattende cybersikkerhedshændelser. For det tredje bør ydelsen af støtte fra EU's cybersikkerhedsreserve være i overensstemmelse med EU's politik over for og de overordnede forbindelser med det pågældende tredjeland og med andre EU-politikker på sikkerhedsområdet. I forbindelse med sin vurdering af overholdelsen af dette tredje kriterium bør Kommissionen rådføre sig med den højtstående repræsentant med henblik på at tilpasse ydelsen af en sådan støtte til den fælles udenrigs- og sikkerhedspolitik.

(53) Ydelsen af støtte til tredjelande, der er associeret til programmet for et digitalt Europa, kan påvirke forbindelserne med tredjelande og Unionens sikkerhedspolitik, herunder inden for rammerne af den fælles udenrigs- og sikkerhedspolitik og den fælles sikkerheds- og forsvarspolitik. Det er derfor hensigtsmæssigt, at Rådet tillægges gennemførelsesbeføjelser til at godkende og præcisere den periode, hvor der kan ydes sådan støtte. Rådet bør træffe afgørelse på grundlag af et forslag fra Kommissionen under behørig hensyntagen til Kommissionens vurdering af de tre kriterier. Det samme bør gælde for forlængelser og forslag om ændring eller ophævelse af sådanne retsakter. Hvis Rådet i særlige tilfælde finder, at der er sket en væsentlig ændring i omstændighederne med hensyn til det tredje kriterium, bør Rådet kunne handle på eget initiativ for at ændre eller ophæve en gennemførelsesretsakt uden at afvente et forslag fra Kommissionen. Sådanne væsentlige ændringer vil sandsynligvis kræve en hurtig indsats, have særligt stor indvirkning på relationerne med tredjelande og ikke kræve en detaljeret vurdering på forhånd fra Kommissionens side. Desuden bør Kommissionen samarbejde med den højtstående repræsentant i forbindelse med anmodninger om støtte fra tredjelande, der er associeret til programmet for et digitalt Europa, og gennemførelsen af støtte til sådanne tredjelande. Kommissionen bør også tage hensyn til ENISA's eventuelle synspunkter vedrørende sådanne anmodninger og sådan støtte. Kommissionen bør underrette Rådet om resultatet af vurderingen af anmodningerne, herunder relevante overvejelser i denne henseende, og om de tjenester, der leveres.

(54) Kommissionens meddelelse af 18. april 2023 om akademiet for cyberfærdigheder påpegede manglen på kvalificerede fagfolk. Der er behov for sådanne kvalifikationer for at nå målene i denne forordning. Unionen har akut behov for fagfolk med færdigheder og kompetencer til at forebygge, opdage og afværge cyberangreb og forsvare Unionen, herunder dets mest kritiske infrastruktur, mod sådanne angreb og sikre dets modstandsdygtighed. Med henblik herpå er det vigtigt at tilskynde til samarbejde mellem interessenter, herunder fra den private og den offentlige sektor og den akademiske verden. Det er også vigtigt at skabe synergier på hele Unionens område og sørge for, at uddannelsesinvesteringerne fremmer indførelsen af sikkerhedsforanstaltninger, der sigter mod at undgå hjerneflugt eller en udvidelse af kvalifikationskløften i nogle regioner mere end i andre. Det haster med at lukke kvalifikationskløften inden for cybersikkerhed med særligt fokus på at mindske kønsskævheden i arbejdsstyrken på dette område og fremme kvinders tilstedeværelse og deltagelse i udformningen af digital forvaltning.

(55) For at sætte skub i innovationen på det digitale indre marked er det vigtigt at styrke forskning og innovation inden for cybersikkerhed for at bidrage til at øge medlemsstaternes modstandsdygtighed og Unionens åbne strategiske autonomi, som er nogle af målene med denne forordning. Synergier er afgørende for at styrke samarbejdet og koordineringen mellem de forskellige interessenter, herunder den private sektor, civilsamfundet og den akademiske verden.

(56) Denne forordning bør tage hensyn til forpligtelsen fastsat i den fælles erklæring af 26. Januar 2022 fra Europa-Parlamentet, Rådet og Kommissionen med titlen "Europæisk erklæring om digitale rettigheder og principper for det digitale årti" med hensyn til at beskytte Unionens demokratier, befolkninger, virksomheder og offentlige institutioner mod cybersikkerhedsrisici og cyberkriminalitet, herunder brud på datasikkerheden og identitetstyveri eller manipulation.

(57) Med henblik på at supplere visse ikke-væsentlige bestemmelser i denne forordning bør Kommissionen tillægges beføjelse til at vedtage retsakter i overensstemmelse med artikel 290 i TEUF med henblik på at præcisere, hvilke typer og hvor mange beredskabstjenester der er nødvendige i EU's cybersikkerhedsreserve. 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[20]. 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 forberedelsen af delegerede retsakter.

[20] EUT L 123 af 12.5.2016, s. 1, ELI: http://data.europa.eu/eli/agree_interinstit/2016/512/oj.

(58) For at sikre ensartede betingelser for gennemførelse af denne forordning bør Kommissionen tillægges gennemførelsesbeføjelser til yderligere at præcisere de detaljerede proceduremæssige ordninger for fordelingen af EU-cybersikkerhedsreservens støttetjenester. Disse beføjelser bør udøves i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) nr. 182/2011[21].

(59) Med forbehold af reglerne vedrørende Unionens årlige budget i henhold til traktaterne bør Kommissionen tage hensyn til de forpligtelser, der følger af denne forordning, når den vurderer ENISA's budgetterings- og personalebehov.

(60) Kommissionen bør regelmæssigt foretage en evaluering af de foranstaltninger, der er fastsat i denne forordning. Den første sådan evaluering bør finde sted i de første to år efter datoen for denne forordnings ikrafttræden og derefter mindst hvert fjerde år under hensyntagen til tidsplanen for revisionen af den flerårige finansielle ramme oprettet i henhold til TFEU artikel 312. Kommissionen bør forelægge Europa-Parlamentet og Rådet en rapport om de fremskridt, der er gjort. For at vurdere de forskellige nødvendige elementer, herunder omfanget af de oplysninger, der udveksles inden for det europæiske cybersikkerhedsvarslingssystem, bør Kommissionen udelukkende basere sig på oplysninger, der er umiddelbart tilgængelige eller gives frivilligt. I lyset af den geopolitiske udvikling og for at sikre kontinuitet og videreudvikling efter 2027 af de foranstaltninger, der er fastsat i denne forordning, er det vigtigt, at Kommissionen vurderer, om det er nødvendigt at oprette en særlig budgetpost i den flerårige finansielle ramme for 2028-2034.

---

[21] 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, ELI: http://data.europa.eu/eli/reg/2011/182/oj).

(61) Målene for denne forordning, nemlig at styrke industri- og tjenesteydelses konkurrencedygtighed i Unionen gennem en digital økonomi og at bidrage til Unionens teknologiske suverænitet og åbne strategisk uafhængighed på området for cybersikkerhed, kan ikke i tilstrækkelig grad opfyldes af medlemsstaterne, men kan på grund af handlingens omfang og virkninger bedre nås på EU-plan; Unionen kan derfor vedtage foranstaltninger i overensstemmelse med nærhedsprincippet, jf. artikel 5 i TEU. I overensstemmelse med proportionalitetsprincippet går denne forordning går ikke videre, end hvad der er nødvendigt for at opfylde disse mål —

VEDTAGET DENNE FORORDNING:

Kapitel I
Generelle bestemmelser

Artikel 1

Genstand og formål

1. Ved denne forordning fastsættes foranstaltninger til styrkelse af Unionens kapacitet til at opdage, forberede sig og reagere på cybertrusler og -hændelser, navnlig gennem oprettelse af:

   a) et paneuropæisk netværk af cyberknudepunkter (et europæisk cybersikkerhedsvarslingssystem) for at opbygge og styrke en koordineret kapacitet til at opdage hændelser og den fælles situationsbevidsthed

   b) en cybersikkerhedsberedskabsmekanisme som støtte til medlemsstaterne til at forberede sig og reagere på, afbøde virkningerne af og påbegynde den indledende genopretning efter væsentlige cybersikkerhedshændelser og omfattende cybersikkerhedshændelser og som støtte til andre brugere til at reagere på omfattende cybersikkerhedshændelser og cybersikkerhedshændelser svarende til omfattende cybersikkerhedshændelser

   c) en europæisk mekanisme til gennemgang af cybersikkerhedshændelser med henblik på at gennemgå og vurdere væsentlige cybersikkerhedshændelser eller omfattende cybersikkerhedshændelser.

2. De overordnede mål med denne forordning er at styrke industriens og tjenesteydelsernes konkurrenceevne i Unionen i hele den digitale økonomi, herunder mikrovirksomheder og små og mellemstore virksomheder samt nystartede virksomheder, og bidrage til Unionens teknologiske suverænitet og åbne strategiske autonomi på cybersikkerhedsområdet, bl.a. ved at fremme innovationen inden for det digitale indre marked. Forordningen forfølger disse mål ved at styrke solidariteten på EU-plan, styrke cybersikkerhedsøkosystemet, øge medlemsstaternes cyberrobusthed og udvikle arbejdsstyrkens færdigheder, knowhow, evner og kompetencer med hensyn til cybersikkerhed.

3. Opfyldelsen af de overordnede mål som omhandlet i stk. 2 forfølges gennem følgende specifikke mål:

   a) at styrke Unionens fælles situationsbevidsthed og koordinerede kapacitet til at opdage cybertrusler og -hændelser

   b) at styrke beredskabet hos enheder, der opererer i sektorer af særligt kritisk betydning eller enheder, der opererer i andre kritiske sektorer i hele Unionen, og styrke solidariteten ved at udvikle koordinerede beredskabstest og bedre indsats- og genopretningskapaciteter med henblik på at håndtere væsentlige cybersikkerhedshændelser, omfattende cybersikkerhedshændelser eller cybersikkerhedshændelser svarende til omfattende cybersikkerhedshændelser, herunder muligheden for at stille indsatsstøtte fra Unionen ved cybersikkerhedshændelser til rådighed for tredjelande, der er associeret til programmet for et digitalt Europa

c) at øge Unionens modstandsdygtighed og bidrage til en effektiv reaktion på hændelser ved at gennemgå og vurdere væsentlige cybersikkerhedshændelser eller omfattende cybersikkerhedshændelser, herunder ved at trække på indhøstede erfaringer og henstillinger, hvor det er relevant.

4. Foranstaltningerne i henhold til denne forordning gennemføres under behørig hensyntagen til medlemsstaternes kompetencer og supplerer de aktiviteter, der udføres af CSIRT-netværket, EU-CyCLONe og NIS-samarbejdsgruppen.

5. Denne forordning berører ikke medlemsstaternes væsentlige statslige funktioner, herunder sikring af statens territoriale integritet, opretholdelse af lov og orden og beskyttelse af den nationale sikkerhed. Navnlig forbliver den nationale sikkerhed den enkelte medlemsstats eneansvar.

6. Delingen eller udvekslingen efter denne forordning af oplysninger, der er fortrolige i henhold til EU-regler eller nationale regler, begrænses til det omfang, der er relevant og står i rimeligt forhold til formålet med denne deling eller udveksling. Sådan deling eller udveksling af oplysninger sikrer oplysningernes fortrolighed og beskytter de berørte enheders sikkerhed og kommercielle interesser. Den omfatter ikke meddelelse af oplysninger, hvis videregivelse strider mod medlemsstaternes væsentlige nationale sikkerhedsinteresser, offentlige sikkerhed eller forsvar.

Artikel 2

Definitioner

I denne forordning forstås ved:

1) "grænseoverskridende cyberknudepunkt": en platform for flere lande, som er oprettet i henhold til en skriftlig konsortieaftale, der i en koordineret netværksstruktur samler nationale cyberknudepunkter fra mindst tre medlemsstater, og som er udformet med henblik på at styrke overvågningen, opdagelsen og analysen af cybertrusler og forebygge hændelser og støtte tilvejebringelse af cybermæssige trusselsefterretninger, navnlig gennem udveksling af relevante data og oplysninger, anonymiserede hvor det er hensigtsmæssigt, samt gennem deling af avancerede værktøjer og fælles udvikling af cybermæssige opdagelses-, analyse-, forebyggelses- og beskyttelseskapaciteter i et pålideligt miljø

2) "værtskonsortium": et konsortium bestående af deltagende medlemsstater, der har indvilliget i at etablere og at bidrage til erhvervelse af værktøjer, infrastruktur eller tjenester til og driften af et grænseoverskridende cyberknudepunkt

3) "CSIRT": en CSIRT som defineret i artikel 10 i direktiv (EU) 2022/2555

4) "enhed": en enhed som defineret i artikel 6, nr. 38), i direktiv (EU) 2022/2555

5) "enheder, der opererer i sektorer af særligt kritisk betydning": den type enhed, der er opført i bilag I til direktiv (EU) 2022/2555

6) "enheder, der opererer i andre kritiske sektorer": den type enhed, der er opført i bilag II til direktiv (EU) 2022/2555

7) "risiko": en risiko som defineret i artikel 6, nr. 9), i direktiv (EU) 2022/2555

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

9) "hændelse": en hændelse som defineret i artikel 6, nr. 6), i direktiv (EU) 2022/2555

10) "væsentlig cybersikkerhedshændelse": en hændelse, der opfylder kriterierne i artikel 23, stk. 3, i direktiv (EU) 2022/2555

11) "større hændelse": en større hændelse som defineret i artikel 3, nr. 8), i Europa-Parlamentets og Rådets forordning (EU, Euratom) 2023/2841[22]

12) "omfattende cybersikkerhedshændelse": en omfattende cybersikkerhedshændelse som defineret i artikel 6, nr. 7), i direktiv (EU) 2022/2555

[22] Europa-Parlamentets og Rådets forordning (EU, Euratom) 2023/2841 af 13. december 2023 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i Unionens institutioner, organer, kontorer og agenturer (EUT L, 2023/2841, 18.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2841/oj).

13) "cybersikkerhedshændelse svarende til en omfattende cybersikkerhedshændelse": for så vidt angår EU's institutioner, organer, kontorer og agenturer, en større hændelse og, for så vidt angår tredjelande, der er associeret til programmet for et digitalt Europa, en hændelse, der forårsager en forstyrrelse på et niveau, der overstiger kapaciteten i det berørte tredjeland, der er associeret til programmet for et digitalt Europa, til at reagere på den

14) "tredjeland, der er associeret til programmet for et digitalt Europa": et tredjeland, der er part i en aftale med Unionen, der giver mulighed for dets deltagelse i programmet for et digitalt Europa i henhold til artikel 10 i forordning (EU) 2021/694

15) "ordregivende myndighed": Kommissionen eller, i det omfang driften og forvaltningen af EU's cybersikkerhedsreserve er overdraget til ENISA i henhold til artikel 14, stk. 5, ENISA

16) "udbyder af administrerede sikkerhedstjenester": en udbyder af administrerede sikkerhedstjenester som defineret i artikel 6, nr. 40), i direktiv (EU) 2022/2555

17) "betroede udbydere af administrerede sikkerhedstjenester": betroede udbydere af administrerede sikkerhedstjenester, der er udvalgt til at indgå i EU's cybersikkerhedsreserve i overensstemmelse med artikel 17.

Kapitel II

Det europæiske cybersikkerhedsvarslingssystem

Artikel 3

Oprettelse af det europæiske cybersikkerhedsvarslingssystem

1. Det europæiske cybersikkerhedsvarslingssystem oprettes som et paneuropæisk infrastrukturnet, der består af nationale cyberknudepunkter og grænseoverskridende cyberknudepunkter, der tilslutter sig på frivillig basis, for at støtte udviklingen af avancerede kapaciteter for Unionen med henblik på at forbedre opdagelses-, analyse- og databehandlingsfærdighederne i forbindelse med cybertrusler og forebyggelsen af hændelser i Unionen.

2. Det europæiske cybersikkerhedsvarslingssystem skal:

   a) bidrage til bedre beskyttelse imod og reaktion på cybertrusler ved at støtte, samarbejde med og styrke kapaciteten hos relevante enheder, navnlig CSIRT'er, CSIRT-netværket, EU-CyCLONe og de kompetente myndigheder, der er udpeget eller oprettet i henhold til artikel 8, stk. 1, i direktiv (EU) 2022/2555

   b) samle relevante data og oplysninger om cybertrusler og -hændelser fra forskellige kilder inden for de grænseoverskridende cyberknudepunkter og dele analyserede eller aggregerede oplysninger gennem grænseoverskridende cyberknudepunkter, hvor det er relevant, med CSIRT-netværket

c) indsamle og støtte tilvejebringelsen af anvendelige oplysninger af høj kvalitet og cybermæssige trusselsefterretninger ved hjælp af de nyeste værktøjer og avancerede teknologier og dele disse oplysninger og cybermæssige trusselsefterretninger

d) bidrage til at forbedre koordineret opdagelse af cybertrusler og fælles situationsbevidsthed i hele Unionen og til udstedelse af varslinger, herunder, hvor det er relevant, ved at fremsætte konkrete anbefalinger til enheder

e) levere tjenester og aktiviteter til cybersikkerhedssektoren i Unionen, herunder bidrage til udviklingen af avancerede værktøjer og teknologier såsom kunstig intelligens og dataanalyseværktøjer.

3. Foranstaltninger til gennemførelse af det europæiske cybersikkerhedsvarslingssystem støttes med midler fra programmet for et digitalt Europa og gennemføres i overensstemmelse med forordning (EU) 2021/694, navnlig specifikt mål nr. 3.

Artikel 4

Nationale cyberknudepunkter

1. Hvis en medlemsstat beslutter at deltage i det europæiske cybersikkerhedsvarslingssystem, udpeger eller opretter den, hvor det er relevant, et nationalt cyberknudepunkt med henblik på denne forordning.

2. Det nationale cyberknudepunkt er en enkelt enhed, der handler under en medlemsstats myndighed. Det kan være en CSIRT eller, hvor det er relevant, en national cyberkrisestyringsmyndighed eller en anden kompetent myndighed, der er udpeget eller oprettet i henhold til artikel 8, stk. 1, i direktiv (EU) 2022/2555, eller en anden enhed. Det nationale cyberknudepunkt skal:

   a) have kapacitet til at fungere som referencepunkt og portal til andre offentlige og private organisationer på nationalt plan med henblik på at indsamle og analysere information om cybertrusler og -hændelser og bidrage til et grænseoverskridende cyberknudepunkt som omhandlet i artikel 5 i denne forordning, og

   b) være i stand til at finde, aggregere og analysere data og oplysninger om cybertrusler og -hændelser, såsom cybermæssige trusselsefterretninger, ved navnlig at anvende de nyeste teknologier med henblik på at forebygge hændelser.

3. Som en del af de funktioner, der er omhandlet i nærværende artikels stk. 2, kan nationale cyberknudepunkter samarbejde med enheder i den private sektor om at udveksle relevante data og oplysninger med henblik på at opdage og forebygge cybertrusler og -hændelser, herunder med sektorielle og tværsektorielle fællesskaber af væsentlige og vigtige enheder som omhandlet i artikel 3 i direktiv (EU) 2022/2555. Hvis det er relevant og i overensstemmelse med EU-retten og national ret, kan de oplysninger, som de nationale cyberknudepunkter anmoder om eller modtager, omfatte telemetri-, sensor- og logningsdata.

4. En medlemsstat, der er udvalgt i henhold til artikel 9, stk. 1, forpligter sig til at ansøge om, at dens nationale cyberknudepunkt deltager i et grænseoverskridende cyberknudepunkt.

Artikel 5

Grænseoverskridende cyberknudepunkter

1. Hvis mindst tre medlemsstater har forpligtet sig til at sikre, at deres nationale cyberknudepunkter samarbejder om at koordinere deres cybersporings- og trusselsovervågningsaktiviteter, kan disse medlemsstater oprette et værtskonsortium med henblik på denne forordning.

2. Et værtskonsortium består af mindst tre deltagende medlemsstater, der har indvilliget i at etablere og bidrage til erhvervelse af værktøjer, infrastruktur eller tjenester til og drift af et grænseoverskridende cyberknudepunkt i overensstemmelse med stk. 4.

3. Hvis et værtskonsortium udvælges i overensstemmelse med artikel 9, stk. 3, indgår dets medlemmer en skriftlig konsortieaftale, som:

   a) fastlægger den interne ordninger for gennemførelse af værts- og brugsaftalen, der er omhandlet i artikel 9, stk. 3,

   b) opretter værtskonsortiets grænseoverskridende cyberknudepunkt, og

   c) omfatter de specifikke bestemmelser, der kræves i henhold til artikel 6, stk. 1 og 2.

4. Et grænseoverskridende cyberknudepunkt er en platform for flere lande, der er oprettet ved en skriftlig konsortieaftale som omhandlet i stk. 3. Det samler de nationale cyberknudepunkter i værtskonsortiets medlemsstater i en koordineret netværksstruktur. Det skal være udformet med henblik på at forbedre overvågning, opdagelse og analyse af cybertrusler, forebygge hændelser og støtte tilvejebringelsen af cybermæssige trusselsefterretninger, navnlig gennem udveksling af relevante data og information, anonymiseret hvor det er hensigtsmæssigt, samt gennem deling af avancerede værktøjer og fælles udvikling af cybermæssige opdagelses-, analyse-, forebyggelses- og beskyttelseskapaciteter i et pålideligt miljø.

5. Et grænseoverskridende cyberknudepunkt repræsenteres i juridisk henseende af et medlem af det tilsvarende værtskonsortium, der fungerer som koordinator, eller af værtskonsortiet, hvis det har status som juridisk person. Ansvaret for, at det grænseoverskridende cyberknudepunkt overholder denne forordning og værts- og brugsaftalen, tildeles i den skriftlige konsortieaftale, der er omhandlet i stk. 3.

6. En medlemsstat kan tilslutte sig et eksisterende værtskonsortium efter aftale med værtskonsortiets medlemmer. Den skriftlige konsortieaftale, der er omhandlet i stk. 3, og værts- og brugsaftalen ændres i overensstemmelse hermed. Dette berører ikke Det Europæiske Industri-, Teknologi- og Forskningskompetencecenter for Cybersikkerheds ejendomsrettigheder (ECCC) over de værktøjer, infrastrukturer eller tjenester, der allerede er indkøbt i fællesskab med det pågældende værtskonsortium.

Artikel 6

Samarbejde og informationsudveksling inden for og mellem grænseoverskridende cyberknudepunkter

1. Medlemmerne af et værtskonsortium sikrer, at deres nationale cyberknudepunkter i overensstemmelse med den konsortieaftale, der er omhandlet i artikel 5, stk. 3, udveksler relevant information, anonymiseret hvor det er hensigtsmæssigt, med hinanden inden for det grænseoverskridende cyberknudepunkt, såsom information om cybertrusler, nærvedhændelser, sårbarheder, teknikker og procedurer, indikatorer for kompromittering, fjendtlige taktikker, trusselsspecifikke oplysninger, cybersikkerhedsadvarsler og anbefalinger vedrørende konfiguration af cybersikkerhedsværktøjer til afsløring af cyberangreb, hvor en sådan informationsudveksling:

   a) fremmer og forbedrer opdagelse af cybertrusler og styrker CSIRT-netværkets kapacitet til at forebygge og reagere på hændelser eller afbøde deres virkninger

   b) øger cybersikkerhedsniveauet, f.eks. ved at øge kendskabet til cybertrusler, begrænse eller hindre muligheden for, at sådanne trusler spreder sig, støtte en række forsvarskapaciteter, afhjælpe og afsløre sårbarheder, støtte teknikker til opdagelse, begrænsning og forebyggelse af trusler, støtte afbødningsstrategier, indsats- og genopretningsfaserne eller fremme samarbejde mellem offentlige og private enheder om forskning i trusler.

2. Den skriftlige konsortieaftale i henhold til artikel 5, stk. 3, skal indeholde:

a) en forpligtelse til at udveksle information mellem værtskonsortiets medlemmer, jf. stk. 1, og betingelserne for udveksling af denne information.

b) en forvaltningsramme, der præciserer og tilskynder alle deltagere til at udveksle relevant information, anonymiseret hvor det er hensigtsmæssigt, som omhandlet i stk. 1

c) mål for bidrag til udvikling af avancerede værktøjer og teknologier, såsom kunstig intelligens og dataanalyseværktøjer.

Den skriftlige konsortieaftale kan præcisere, at oplysningerne omhandlet i stk. 1 skal deles i overensstemmelse med EU-retten og national ret.

3. Grænseoverskridende cyberknudepunkter indgår samarbejdsaftaler med hinanden, hvor principperne for interoperabilitet og informationsudveksling mellem de grænseoverskridende cyberknudepunkter fastlægges. Grænseoverskridende cyberknudepunkter underretter Kommissionen om de indgåede samarbejdsaftaler.

4. Informationsudveksling som omhandlet i stk. 1 mellem grænseoverskridende cyberknudepunkter sikres gennem en høj grad af interoperabilitet. For at støtte en sådan interoperabilitet udsteder ENISA uden unødig forsinkelse og under alle omstændigheder senest den … [12 måneder efter datoen for denne forordnings ikrafttræden] i tæt samråd med Kommissionen interoperabilitetsretningslinjer, der navnlig præciserer formater og protokoller for informationsudveksling, under hensyntagen til internationale standarder og bedste praksis, samt funktionen af etablerede grænseoverskridende cyberknudepunkter. Interoperabilitetskravene fastsat i samarbejdsaftaler om grænseoverskridende cyberknudepunkter baseres på de retningslinjer, der er udstedt af ENISA.

Artikel 7

Samarbejde og informationsudveksling med netværk på EU-plan

1. Grænseoverskridende cyberknudepunkter og CSIRT-netværket arbejder tæt sammen, navnlig med henblik på udveksling af oplysninger. Med henblik herpå aftaler de proceduremæssige ordninger for samarbejde og udveksling af relevante oplysninger og, med forbehold af stk. 2, hvilke typer oplysninger der skal udveksles.

2. Hvis grænseoverskridende cyberknudepunkter indhenter oplysninger om en mulig eller igangværende væsentlig cybersikkerhedshændelse, sikrer de med henblik på fælles situationsbevidsthed, at der uden unødig forsinkelse gives relevante oplysninger og tidlige varslinger til medlemsstaternes myndigheder og Kommissionen via EU-CyCLONe og CSIRT-netværket.

Artikel 8

Sikkerhed

1. Medlemsstater, der deltager i det europæiske cybersikkerhedsvarslingssystem, sikrer et højt cybersikkerhedsniveau, herunder fortrolighed og datasikkerhed, samt fysisk sikkerhed i netværket for det europæiske cybersikkerhedsvarslingssystem, og sikrer, at netværket forvaltes og styres hensigtsmæssigt, så det beskyttes mod trusler, og så sikkerheden i netværket og i systemerne, herunder de data og oplysninger, der deles via netværket, garanteres.

2. Medlemsstater, der deltager i det europæiske cybersikkerhedsvarslingssystem, sikrer, at udvekslingen af information, der er omhandlet i artikel 6, stk. 1, inden for det europæiske cybersikkerhedsvarslingssystem med andre enheder end en offentlig myndighed eller et offentligt organ i en medlemsstat ikke har en negativ indvirkning på Unionens eller medlemsstaternes sikkerhedsinteresser.

Artikel 9

Finansiering af det europæiske cybersikkerhedsvarslingssystem

1. Efter en indkaldelse af interessetilkendegivelser for medlemsstater, der har til hensigt at deltage i det europæiske cybersikkerhedsvarslingssystem, udvælger ECCC medlemsstater til at deltage sammen med ECCC i det fælles indkøb af værktøjer, infrastruktur eller tjenester med henblik på at oprette eller styrke færdighederne hos nationale cyberknudepunkter, som er udpeget eller oprettet i henhold til artikel 4, stk. 1. ECCC kan yde tilskud til de udvalgte medlemsstater til finansiering af driften af sådanne værktøjer, sådan infrastruktur eller sådanne tjenester. Unionens finansielle bidrag dækker op til 50 % af omkostningerne ved erhvervelse af værktøjer, infrastruktur eller tjenester og op til 50 % af driftsomkostningerne. De udvalgte medlemsstater afholder de resterende omkostninger. Inden iværksættelsen af proceduren for erhvervelse af værktøjer, infrastruktur eller tjenester indgår ECCC og medlemsstaten en værts- og brugsaftale, der regulerer brugen af værktøjerne, infrastrukturen eller tjenesterne.

2. Hvis en medlemsstats nationale cyberknudepunkt ikke deltager i et grænseoverskridende cyberknudepunkt senest to år efter den dato, hvor værktøjerne, infrastrukturen eller tjenesterne blev erhvervet, eller hvor den modtog tilskudsfinansiering, alt efter hvad der indtraf først, er medlemsstaten ikke berettiget til yderligere EU-støtte i henhold til dette kapitel, før den har tilsluttet sig et grænseoverskridende cyberknudepunkt.

3. Efter en indkaldelse af interessetilkendegivelser udvælges et værtskonsortium af ECCC til at deltage i fælles indkøb af værktøjer, infrastruktur eller tjenester i samarbejde med ECCC. ECCC kan yde tilskud til værtskonsortiet til finansiering af driften af værktøjerne, infrastrukturen eller tjenesterne. Unionens finansielle bidrag dækker op til 75 % af omkostningerne ved erhvervelse af værktøjer, infrastruktur eller tjenester og op til 50 % af driftsomkostningerne. Værtskonsortiet afholder de resterende omkostninger. Inden iværksættelsen af proceduren for erhvervelse af værktøjer, infrastruktur eller tjenester indgår ECCC og værtskonsortiet en værts- og brugsaftale, der regulerer brugen af værktøjerne, infrastrukturen eller tjenesterne.

4. ECCC udarbejder mindst hvert andet år en kortlægning af de værktøjer, den infrastruktur eller de tjenester, der er nødvendige og af tilstrækkelig kvalitet til at etablere eller forbedre færdighederne hos nationale cyberknudepunkter og grænseoverskridende cyberknudepunkter og deres tilgængelighed, herunder hos retlige enheder, der er etableret eller anses for at være etableret i medlemsstaterne, og som kontrolleres af medlemsstaterne eller af statsborgere i medlemsstaterne. Ved udarbejdelsen af kortlægningen hører ECCC CSIRT-netværket, eventuelle eksisterende grænseoverskridende cyberknudepunkter, ENISA og Kommissionen.

Kapitel III
Cybersikkerhedsberedskabsmekanisme

Artikel 10

Oprettelse af cybersikkerhedsberedskabsmekanismen

1. Der etableres en cybersikkerhedsberedskabsmekanisme for at støtte forbedringen af Unionens modstandsdygtighed over for cybertrusler samt forberede Unionen på og på solidarisk vis afbøde de kortsigtede virkninger af væsentlige cybersikkerhedshændelser, omfattende cybersikkerhedshændelser og cybersikkerhedshændelser svarende til omfattende cybersikkerhedshændelser.

2. For så vidt angår medlemsstaterne, skal foranstaltninger, der ydes inden for rammerne af cybersikkerhedsberedskabsmekanismen, stilles til rådighed efter anmodning og skal supplere medlemsstaternes indsats og foranstaltninger for at forberede sig på, reagere på og komme sig efter hændelser.

3. Foranstaltningerne til gennemførelse af cybersikkerhedsberedskabsmekanismen støttes med midler fra programmet for et digitalt Europa og gennemføres i overensstemmelse med forordning (EU) 2021/694, navnlig specifikt mål nr. 3.

4. Foranstaltningerne under cybersikkerhedsberedskabsmekanismen gennemføres primært gennem ECCC i overensstemmelse med forordning (EU) 2021/887. Dog gennemføres foranstaltninger til gennemførelse af EU's cybersikkerhedsreserve som omhandlet i nærværende forordnings artikel 11, litra b), af Kommissionen og ENISA.

Artikel 11

Foranstaltningstyper

Under cybersikkerhedsberedskabsmekanismen støttes følgende foranstaltningstyper:

a) beredskabsforanstaltninger, nemlig:

   i) koordineret beredskabstest af enheder, der opererer i sektorer af særligt kritisk betydning i hele Unionen, jf. artikel 12

   ii) andre beredskabsforanstaltninger for enheder, der opererer i sektorer af særligt kritisk betydning eller enheder, der opererer i andre kritiske sektorer, jf. artikel 13

b) foranstaltninger, der støtter reaktion på og den indledende genopretning efter væsentlige cybersikkerhedshændelser, omfattende cybersikkerhedshændelser og cybersikkerhedshændelser svarende til en omfattende cybersikkerhedshændelse, der leveres af betroede udbydere af administrerede sikkerhedstjenester, der deltager i EU's cybersikkerhedsreserve, som er oprettet i henhold til artikel 14

c) foranstaltninger til støtte for gensidig bistand som omhandlet i artikel 18.

Artikel 12

Koordineret beredskabstest af enheder

1. Cybersikkerhedsberedskabsmekanismen skal støtte frivillig koordineret beredskabstest af enheder, der opererer i sektorer af særligt kritisk betydning.

2. Den koordinerede beredskabstest kan bestå af beredskabsaktiviteter såsom penetrationstest og trusselsvurdering.

3. Støtte til beredskabsforanstaltninger i henhold til denne artikel ydes primært til medlemsstaterne i form af tilskud og på de betingelser, der er fastsat i de relevante arbejdsprogrammer som omhandlet i artikel 24 i forordning (EU) 2021/694.

4. Med henblik på at støtte den koordinerede beredskabstest af de enheder, der er omhandlet i nærværende forordnings artikel 11, litra a), nr. i), i hele Unionen identificerer Kommissionen efter høring af NIS-samarbejdsgruppen, EU-CyCLONe og ENISA de berørte sektorer eller delsektorer blandt de sektorer af særligt kritisk betydning, der er anført i bilag I til direktiv (EU) 2022/2555, for hvilke der kan udsendes en indkaldelse af forslag om ydelse af tilskud. Medlemsstaternes deltagelse i disse forslagsindkaldelser er frivillig.

5. Når Kommissionen identificerer sektorerne eller delsektorerne omhandlet i stk. 4, tager den hensyn til koordinerede risikovurderinger og afprøvning af modstandsdygtighed på EU-plan og resultaterne heraf.

6. NIS-samarbejdsgruppen udarbejder i samarbejde med Kommissionen, Unionens højtstående repræsentant for udenrigs- og sikkerhedspolitik ("den højtstående repræsentant") og ENISA og, inden for rammerne af dets mandat, EU-CyCLONe fælles risikoscenarier og metoder til gennemførelse af de koordinerede beredskabstest omhandlet i artikel 11, litra a), nr. i), og, hvor det er relevant, for andre beredskabsforanstaltninger omhandlet i nævnte artikels litra a), nr. ii).

7. Når en enhed, der opererer i en sektor af særligt kritisk betydning, frivilligt deltager i koordinerede beredskabstest, og disse test resulterer i anbefalinger om specifikke foranstaltninger, som den deltagende enhed kan integrere i en afhjælpningsplan, skal den myndighed i medlemsstaten, der er ansvarlig for den koordinerede beredskabstest, hvor det er relevant, gennemgå de deltagende enheders opfølgning på disse foranstaltninger med henblik på at styrke beredskabet.

Artikel 13

Andre beredskabsforanstaltninger

1. Cybersikkerhedsberedskabsmekanismen støtter beredskabsforanstaltninger, der ikke er omfattet af denne forordnings artikel 12. Sådanne foranstaltninger skal omfatte beredskabsforanstaltninger for enheder i sektorer, der ikke er udpeget til koordineret beredskabstest i henhold til artikel 12. Sådanne foranstaltninger kan støtte sårbarhedsovervågning, risikoovervågning, øvelser og uddannelse.

2. Støtte til beredskabsforanstaltninger i henhold til denne artikel ydes til medlemsstaterne efter anmodning og primært i form af tilskud og på de betingelser, der er fastsat i de relevante arbejdsprogrammer som omhandlet i artikel 24 i forordning (EU) 2021/694.

Artikel 14

Oprettelse af EU's cybersikkerhedsreserve

1. Der oprettes en EU-cybersikkerhedsreserve med henblik på efter anmodning at bistå de brugere, der er omhandlet i stk. 3, med at reagere på eller yde støtte til at reagere på væsentlige cybersikkerhedshændelser, omfattende cybersikkerhedshændelser eller cybersikkerhedshændelser svarende til en omfattende cybersikkerhedshændelse og den indledende genopretning efter sådanne hændelser.

2. EU's cybersikkerhedsreserve består af beredskabstjenester fra betroede udbydere af administrerede sikkerhedstjenester, der er udvalgt i overensstemmelse med kriterierne i artikel 17, stk. 2. EU's cybersikkerhedsreserve kan omfatte tjenester omfattet af forhåndsforpligtelser. En betroet udbyder af administrerede sikkerhedstjenesters tjenester omfattet af forhåndsforpligtelser skal kunne konverteres til beredskabstjenester i forbindelse med forebyggelse af og reaktioner på hændelser i tilfælde, hvor disse tjenester omfattet af forhåndsforpligtelser ikke anvendes til at reagere på hændelser i det tidsrum, hvor disse tjenester er omfattet af forhåndsforpligtelser. EU's cybersikkerhedsreserve kan efter anmodning indsættes i alle medlemsstater, i EU's institutioner, organer, kontorer og agenturer og i tredjelande, der er associeret til programmet for et digitalt Europa som omhandlet i artikel 19, stk. 1.

3. Brugerne af tjenester leveret af EU's cybersikkerhedsreserve er følgende:

a) medlemsstaternes cyberkrisestyringsmyndigheder og CSIRT'er som anført i henholdsvis artikel 9, stk. 1 og 2, og artikel 10 i direktiv (EU) 2022/2555

b) CERT-EU i overensstemmelse med artikel 13 i forordning (EU, Euratom) 2023/2841

c) kompetente myndigheder såsom enheder, der håndterer IT-sikkerhedshændelser, og cyberkrisestyringsmyndigheder i tredjelande, der er associeret til programmet for et digitalt Europa, i overensstemmelse med artikel 19, stk. 8.

4. Kommissionen har det overordnede ansvar for gennemførelsen af EU's cybersikkerhedsreserve. Kommissionen fastlægger prioriteterne for og udviklingen af EU's cybersikkerhedsreserve i samarbejde med NIS-samarbejdsgruppen og i overensstemmelse med kravene til de brugere, der er omhandlet i stk. 3, overvåger gennemførelsen og sikrer komplementaritet, sammenhæng, synergi og forbindelser med andre støtteaktioner i henhold til denne forordning samt andre EU-foranstaltninger og -programmer. Disse prioriteter gennemgås hvert andet år og revideres om nødvendigt. Kommissionen underretter Europa-Parlamentet og Rådet om disse prioriteter og om enhver revision heraf.

5. Uden at det berører Kommissionens overordnede ansvar for gennemførelsen af EU's cybersikkerhedsreserve som omhandlet i denne artikels stk. 4, og med forbehold af en bidragsaftale som defineret i artikel 2, nr. 19), i forordning (EU, Euratom) 2024/2509 overdrager Kommissionen helt eller delvist driften og forvaltningen af EU's cybersikkerhedsreserve til ENISA. Aspekter, der ikke overdrages til ENISA, forvaltes fortsat direkte af Kommissionen.

6. ENISA udarbejder mindst hvert andet år en kortlægning af de tjenester, som de brugere, der er omhandlet i nærværende artikels stk. 3, litra a) og b), har brug for. Kortlægningen skal også omfatte tilgængeligheden af sådanne tjenester, herunder fra retlige enheder, der er etableret eller anses for at være etableret i medlemsstaterne, og som kontrolleres af medlemsstaterne eller af statsborgere i medlemsstaterne. Ved kortlægningen af denne tilgængelighed vurderer ENISA de færdigheder og den kapacitet hos Unionens cybersikkerhedsarbejdsstyrke, der er relevante for målene for EU's cybersikkerhedsreserve. Ved udarbejdelsen af kortlægningen hører ENISA NIS-samarbejdsgruppen, EU-CyCLONe, Kommissionen og, hvor det er relevant, Det Interinstitutionelle Råd for Cybersikkerhed oprettet i henhold til artikel 10 i forordning (EU, Euratom) 2023/2841 (IICB). Ved kortlægningen af tilgængeligheden af tjenester hører ENISA også relevante interessenter inden for cybersikkerhedsindustrien, herunder udbydere af administrerede sikkerhedstjenester. ENISA udarbejder en lignende kortlægning efter at have underrettet Rådet og efter at have hørt EU-CyCLONe, Kommissionen og, hvor det er relevant, den højtstående repræsentant for at identificere brugernes behov som omhandlet i nærværende artikels stk. 3, litra c).

7. Kommissionen tillægges beføjelser til at vedtage delegerede retsakter i overensstemmelse med artikel 23 med henblik på at supplere denne forordning ved at præcisere de typer og det antal af beredskabstjenester, der kræves i EU's cybersikkerhedsreserve. Ved udarbejdelsen af disse delegerede retsakter tager Kommissionen hensyn til den kortlægning, der er omhandlet i nærværende artikels stk. 6, og kan udveksle rådgivning og samarbejde med NIS-samarbejdsgruppen og ENISA.

Artikel 15

Anmodninger om støtte fra EU's cybersikkerhedsreserve

1. De brugere, der er omhandlet i artikel 14, stk. 3, kan anmode om tjenester fra EU's cybersikkerhedsreserve til støtte for en reaktion på og den indledende genopretning efter væsentlige cybersikkerhedshændelser, omfattende cybersikkerhedshændelser eller cybersikkerhedshændelser svarende til en omfattende cybersikkerhedshændelse.

2. For at modtage støtte fra EU's cybersikkerhedsreserve træffer de brugere, der er omhandlet i artikel 14, stk. 3, alle passende foranstaltninger til at afbøde virkningerne af den hændelse, der er årsag til anmodningen om støtte, herunder, hvor det er relevant, ydelse af direkte teknisk bistand og andre ressourcer som en del af reaktionen på hændelsen og genopretningsindsatsen.

3. Anmodninger om støtte sendes til den ordregivende myndighed som følger:

   a) for så vidt angår de brugere, der er omhandlet i denne forordnings artikel 14, stk. 3, litra a), via det centrale kontaktpunkt, der er udpeget eller oprettet i henhold til artikel 8, stk. 3, i direktiv (EU) 2022/2555

b) for så vidt angår den bruger, der er omhandlet i artikel 14, stk. 3, litra b), af denne bruger

c) for så vidt angår de brugere, der er omhandlet i artikel 14, stk. 3, litra c), via det centrale kontaktpunkt, der er omhandlet i artikel 19, stk. 9.

4. I tilfælde af anmodninger fra brugere som omhandlet i artikel 14, stk. 3, litra a), underretter medlemsstaterne CSIRT-netværket og, hvor det er relevant, EU-CyCLONe om deres brugeres anmodninger om støtte til reaktioner på hændelser og den første genopretning i henhold til denne artikel.

5. Anmodninger om støtte til reaktioner på hændelser og den indledende genopretning omfatter:

a) relevante oplysninger om den berørte enhed og mulige virkninger af hændelsen på:

i) for så vidt angår de brugere, der er omhandlet i artikel 14, stk. 3, litra a), de berørte medlemsstater og brugere, herunder risikoen for afsmittende virkninger på en anden medlemsstat

ii) for så vidt angår den bruger, der er omhandlet i artikel 14, stk. 3, litra b), de berørte EU-institutioner, -organer, -kontorer og -agenturer

iii) for så vidt angår de brugere, der er omhandlet i denne forordnings artikel 14, stk. 3, litra c), de berørte tredjelande, der er associeret til programmet for et digitalt Europa

b) oplysninger om den ønskede tjeneste, sammen med den planlagte anvendelse af den støtte, der anmodes om, herunder en angivelse af de anslåede behov

c) relevante oplysninger om foranstaltninger, der er truffet for at afbøde den hændelse, der er årsag til anmodningen om støtte, jf. stk. 2

d) hvis det er relevant, tilgængelige oplysninger om andre former for støtte, der er til rådighed for den berørte enhed.

6. ENISA udarbejder i samarbejde med Kommissionen og EU-CyCLONe en skabelon for at lette indgivelsen af anmodninger om støtte fra EU's cybersikkerhedsreserve.

7. Kommissionen kan i gennemførelsesretsakter yderligere præcisere de detaljerede proceduremæssige ordninger for den måde, hvorpå der skal anmodes om og reageres på støttetjenester fra EU's cybersikkerhedsreserve, og den måde hvorpå der skal reageres på disse anmodninger i henhold til denne artikel, til artikel 16, stk. 1, og til artikel 19, stk. 10, herunder ordninger for indgivelse af sådanne anmodninger og levering af reaktioner og skabeloner for de rapporter, der er omhandlet i artikel 16, stk. 9. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 24, stk. 2.

Artikel 16

Gennemførelse af støtte fra EU's cybersikkerhedsreserve

1. For så vidt angår anmodninger fra de brugere, der er omhandlet i artikel 14, stk. 3, litra a) og b), vurderes anmodninger om støtte fra EU's cybersikkerhedsreserve af den ordregivende myndighed. Et svar sendes til de brugere, der er omhandlet i artikel 14, stk. 3, litra a) og b), straks og under alle omstændigheder senest 48 timer efter indgivelsen af anmodningen for at sikre støttens effektivitet. Den ordregivende myndighed underretter Rådet og Kommissionen om resultaterne af processen.

2. For så vidt angår oplysninger, der udveksles i forbindelse med anmodning om og levering af tjenester fra EU's cybersikkerhedsreserve, skal alle parter, der er involveret i anvendelsen af denne forordning:

   a) begrænse anvendelsen og udvekslingen af disse oplysninger til, hvad der er nødvendigt for at opfylde deres forpligtelser eller funktioner i henhold til denne forordning

   b) kun anvende og udveksle oplysninger, der er fortrolige eller klassificeret i henhold til EU-retten og national ret, i overensstemmelse med denne ret

   c) sikre effektiv og sikker informationsudveksling, hvor det er relevant, ved at anvende og respektere relevante protokoller for informationsudveksling, herunder traffic light-protokollen.

3. Ved vurderingen af individuelle anmodninger i henhold til artikel 16, stk. 1, og artikel 19, stk. 10, vurderer den ordregivende myndighed eller Kommissionen, alt efter hvad der er relevant, først, om kriterierne i artikel 15, stk. 1 og 2, er opfyldt. Hvis dette er tilfældet, vurderer den varigheden og arten af den støtte, der er hensigtsmæssig, under hensyntagen til det mål, der er omhandlet i artikel 1, stk. 3, litra b), og følgende kriterier, hvor det er relevant:

a) omfanget og alvorligheden af hændelsen

b) typen af berørt enhed, idet der gives højere prioritet til hændelser, der påvirker væsentlige enheder som omhandlet i artikel 3, stk. 1, i direktiv (EU) 2022/2555

c) mulig indvirkning af hændelsen på de berørte medlemsstater, EU-institutioner, -organer, -kontorer eller -agenturer eller tredjelande, der er associeret til programmet for et digitalt Europa

d) hændelsens mulige grænseoverskridende karakter og risikoen for afledte effekter for andre medlemsstater, EU-institutioner, -organer, -kontorer eller -agenturer eller tredjelande, der er associeret til programmet for et digitalt Europa

e) foranstaltninger truffet af brugeren for at medvirke til reaktionen herpå og den indledende genopretningsindsats, jf. artikel 15, stk. 2.

4. Med henblik på at prioritere anmodninger i tilfælde af samtidige anmodninger fra de brugere, der er omhandlet i artikel 14, stk. 3, tages der, hvor det er relevant, hensyn til de kriterier, der er omhandlet i nærværende artikels stk. 3, uden at det berører princippet om loyalt samarbejde mellem medlemsstaterne og EU's institutioner, organer, kontorer og agenturer. Hvis to eller flere anmodninger vurderes at være ens i henhold til disse kriterier, gives der højere prioritet til anmodninger fra brugere i medlemsstaterne. Hvis driften og forvaltningen af EU's cybersikkerhedsreserve helt eller delvist er blevet overdraget til ENISA i henhold til artikel 14, stk. 5, arbejder ENISA og Kommissionen tæt sammen om at prioritere anmodninger i overensstemmelse med dette stykke.

5. Tjenesterne under EU's cybersikkerhedsreserve leveres i overensstemmelse med særaftaler mellem den betroede udbyder af administrerede sikkerhedstjenester og den bruger, som støtten under EU's cybersikkerhedsreserve ydes til. Disse tjenester kan leveres i overensstemmelse med særaftaler mellem den betroede udbyder af administrerede sikkerhedstjenester, brugeren og den berørte enhed. Alle aftaler, der er omhandlet i dette stykke, skal bl.a. indeholde ansvarsbetingelser.

6. De i stk. 5 omhandlede aftaler baseres på skabeloner udarbejdet af ENISA efter høring af medlemsstaterne og, hvor det er relevant, andre brugere af EU's cybersikkerhedsreserve.

7. Kommissionen, ENISA og brugerne af EU's cybersikkerhedsreserve bærer intet kontraktligt ansvar for skader påført tredjepart som følge af de tjenester, der leveres inden for rammerne af gennemførelsen af EU's cybersikkerhedsreserve.

8. Brugere må kun anvende tjenesterne under EU's cybersikkerhedsreserve, der leveres som reaktion på en anmodning i henhold til artikel 15, stk. 1, med henblik på at støtte en reaktion på og sikre den indledende genopretning efter væsentlige cybersikkerhedshændelser, omfattende cybersikkerhedshændelser og cybersikkerhedshændelser svarende til en omfattende cybersikkerhedshændelse. De må kun anvende disse tjenester til:

   a) enheder, der opererer i sektorer af særligt kritisk betydning, eller enheder, der opererer i andre kritiske sektorer, for så vidt angår de brugere, der er omhandlet i artikel 14, stk. 3, litra a), og tilsvarende enheder for så vidt angår de brugere, der er omhandlet i artikel 14, stk. 3, litra c), og

   b) EU's institutioner, organer, kontorer og agenturer, for så vidt angår den bruger, der er omhandlet i artikel 14, stk. 3, litra b).

9. Senest to måneder efter afslutningen af en støtte skal brugere, der har modtaget støtte, forelægge en sammenfattende rapport om den leverede tjeneste, de opnåede resultater og de indhøstede erfaringer for:

   a) Kommissionen, ENISA, CSIRT-netværket og EU-CyCLONe for så vidt angår de brugere, der er omhandlet i denne forordnings artikel 14, stk. 3, litra a)

   b) Kommissionen, ENISA og Det Interinstitutionelle Råd for Cybersikkerhed for så vidt angår den bruger, der er omhandlet i denne forordnings artikel 14, stk. 3, litra b)

c) Kommissionen for så vidt angår de brugere, der er omhandlet i denne forordnings artikel 14, stk. 3, litra c).

Kommissionen fremsender enhver sammenfattende rapport modtaget fra de i artikel 14, stk. 3, omhandlede brugere i henhold til nærværende stykkes første afsnits litra c) til Rådet og den højtstående repræsentant.

10. Hvis driften og forvaltningen af EU's cybersikkerhedsreserve helt eller delvist er blevet overdraget til ENISA i henhold til denne forordnings artikel 14, stk. 5, aflægger ENISA regelmæssigt rapport til og hører Kommissionen herom. I den forbindelse sender ENISA straks Kommissionen alle anmodninger, det modtager fra de brugere, der er omhandlet i denne forordnings artikel 14, stk. 3, litra c), og, hvis det er nødvendigt med henblik på prioritering i henhold til denne artikel, alle anmodninger, det har modtaget fra de brugere, der er omhandlet i denne forordnings artikel 14, stk. 3, litra a) eller b). Forpligtelserne i dette stykke berører ikke artikel 14 i forordning (EU) 2019/881.

11. For så vidt angår de brugere, der er omhandlet i artikel 14, stk. 3, litra a) og b), aflægger den ordregivende myndighed regelmæssigt og mindst to gange om året rapport til NIS-samarbejdsgruppen om anvendelsen og resultaterne af støtten.

12. For så vidt angår de brugere, der er omhandlet i artikel 14, stk. 3, litra c), aflægger Kommissionen regelmæssigt og mindst to gange om året rapport til Rådet og underretter den højtstående repræsentant om anvendelsen og resultaterne af støtten.

Artikel 17

Betroede udbydere af administrerede sikkerhedstjenester

1. I forbindelse med udbudsprocedurer med henblik på etablering af EU's cybersikkerhedsreserve handler den ordregivende myndighed i overensstemmelse med principperne i forordning (EU, Euratom) 2024/2509 og i overensstemmelse med følgende principper:

   a) sikre, at de tjenester, der indgår i EU's cybersikkerhedsreserve, som helhed er af en sådan art, at EU's cybersikkerhedsreserve omfatter tjenester, der kan udrulles i alle medlemsstater, idet der navnlig tages hensyn til nationale krav til levering af sådanne tjenester, herunder sprog, certificering eller akkreditering

   b) sikre beskyttelse af Unionens og dens medlemsstaters væsentlige sikkerhedsinteresser

   c) sikre, at EU's cybersikkerhedsreserve skaber merværdi for Unionen ved at bidrage til de målsætninger, der er fastsat i artikel 3 i forordning (EU) 2021/694, herunder ved at fremme udviklingen af cybersikkerhedsfærdigheder i Unionen.

2. Ved indkøb af tjenesteydelser til EU's cybersikkerhedsreserve medtager den ordregivende myndighed følgende kriterier og krav i udbudsdokumenterne:

a) udbyderen skal påvise, at personalet har den højeste grad af faglig integritet, selvstændighed og ansvar samt den nødvendige tekniske kompetence til at udføre aktiviteterne inden for de specifikke områder, og udbyderen skal sikre, at ekspertisen samt de nødvendige tekniske ressourcer er til rådighed permanent og uden afbrydelse

b) udbyderen og eventuelle relevante datterselskaber og underleverandører skal overholde gældende regler om beskyttelse af klassificerede informationer og skal have indført passende foranstaltninger, herunder, hvor det er relevant, aftaler mellem hinanden, til beskyttelse af fortrolige oplysninger vedrørende tjenesten, navnlig dokumentation, undersøgelser og rapporter

c) udbyderen skal fremlægge tilstrækkelig dokumentation for en transparent ledelsesstruktur, hvor der ikke er sandsynlighed for, at upartiskheden og kvaliteten af tjenesterne kan anfægtes eller interessekonflikter opstå

d) udbyderen skal have en passende sikkerhedsgodkendelse, i det mindste for personale, der arbejder med udrulning af tjenesterne, hvis en medlemsstat kræver det

e) udbyderens IT-systemer skal være sikret med et relevant sikkerhedsniveau

f) udbyderen skal være udstyret med den nødvendige hardware og software til at understøtte den ønskede tjeneste, som ikke må indeholde kendte sårbarheder, der kan udnyttes, skal omfatte de seneste sikkerhedsopdateringer og skal under alle omstændigheder overholde alle gældende bestemmelser i Europa-Parlamentets og Rådets forordning (EU) 2024/…[23+]

g) udbyderen skal kunne dokumentere erfaring med at levere lignende tjenester til relevante nationale myndigheder, enheder, der opererer i sektorer af særligt kritisk betydning, eller enheder, der opererer i andre kritiske sektorer

h) udbyderen skal være i stand til at levere tjenesten hurtigt i den eller de medlemsstater, hvor udbyderen kan levere tjenesten

i) udbyderen skal kunne levere tjenesten på et eller flere af EU-institutionernes eller en medlemsstats officielle sprog som krævet af den eller de medlemsstater eller brugere, der er omhandlet i artikel 14, stk. 3, litra b) og c), hvor udbyderen kan levere tjenesten

j) når en europæisk cybersikkerhedscertificeringsordning for administrerede sikkerhedstjenester i henhold til forordning (EU) 2019/881 er indført, skal udbyderen certificeres i overensstemmelse med denne ordning inden for to år fra datoen, hvor ordningen finder anvendelse

---

[23] Europa-Parlamentets og Rådets forordning (EU) 2024/… af … om … (EUT L, …, ELI: …).

[+] EUT: Indsæt venligst nummeret på forordningen i dokument PE-CONS 100/23 (2022/0272(COD)) i teksten og indsæt forordningens nummer, dato, EUT-henvisning og ELI-henvisning i fodnoten.

k) udbyderen skal i udbuddet medtage konverteringsbetingelserne for eventuelle ubrugte hændelsesberedskabstjenester, der kan konverteres til beredskabstjenester, der er tæt knyttet til reaktioner på hændelser, såsom øvelser eller kurser.

3. Med henblik på indkøb af tjenester til EU's cybersikkerhedsreserve kan den ordregivende myndighed, hvor det er relevant, udvikle kriterier og krav ud over dem, der er omhandlet i stk. 2, i tæt samarbejde med medlemsstaterne.

Artikel 18

Foranstaltninger til støtte for ensidig bistand

1. Cybersikkerhedsberedskabsmekanismen yder støtte til teknisk bistand fra en medlemsstat til en anden medlemsstat, der er berørt af en væsentlig cybersikkerhedshændelse eller en omfattende cybersikkerhedshændelse, herunder i de tilfælde, der er omhandlet i artikel 11, stk. 3, litra f), i direktiv (EU) 2022/2555.

2. Støtten til den i denne artikels stk. 1 omhandlede tekniske gensidige bistand ydes i form af tilskud og på de betingelser, der er fastsat i de relevante arbejdsprogrammer som omhandlet i artikel 24 i forordning (EU) 2021/694.

Artikel 19

Støtte til tredjelande, der er associeret til programmet for et digitalt Europa

1. Et tredjeland, der er associeret til programmet for et digitalt Europa, kan anmode om støtte fra EU's cybersikkerhedsreserve, hvis aftalen, hvorigennem det er associeret til programmet for et digitalt Europa, indeholder bestemmelser om deltagelse i EU's cybersikkerhedsreserve. Denne aftale skal indeholde bestemmelser om, at det berørte tredjeland, der er associeret til programmet for et digitalt Europa, skal overholde de forpligtelser, der er fastsat i denne artikels stk. 2 og 9. Med henblik på et tredjelands deltagelse i EU's cybersikkerhedsreserve kan et tredjelands delvise associering til programmet for et digitalt Europa omfatte en associering, der er begrænset til det operationelle mål, der er omhandlet i artikel 6, stk. 1, litra g), i forordning (EU) 2021/694.

2. Senest tre måneder efter indgåelsen af den i stk. 1 omhandlede aftale og under alle omstændigheder forud for modtagelse af støtte fra EU's cybersikkerhedsreserve forelægger det tredjeland, der er associeret til programmet for et digitalt Europa, Kommissionen oplysninger om sin cyberrobusthed og risikostyringskapacitet, herunder som minimum oplysninger om nationale foranstaltninger, der er truffet for at forberede sig på væsentlige cybersikkerhedshændelser, omfattende cybersikkerhedshændelser og cybersikkerhedshændelser svarende til en omfattende cybersikkerhedshændelse, samt oplysninger om ansvarlige nationale enheder, herunder enheder, der håndterer IT-sikkerhedshændelser eller tilsvarende enheder, deres kapaciteter og de ressourcer, de har fået tildelt. Det tredjeland, der er associeret til programmet for et digitalt Europa, skal regelmæssigt og mindst én gang om året ajourføre disse oplysninger. Kommissionen forelægger disse oplysninger for den højtstående repræsentant og ENISA med henblik på anvendelsen af stk. 11.

3. Kommissionen vurderer regelmæssigt og mindst én gang om året følgende kriterier for hvert af de i stk. 1 omhandlede tredjelande, der er associeret til programmet for et digitalt Europa:

a) om det pågældende land overholder betingelserne i den i stk. 1 omhandlede aftale, for så vidt som disse vilkår vedrører deltagelse i EU's cybersikkerhedsreserve

b) om det pågældende land har taget passende skridt til at forberede sig på væsentlige cybersikkerhedshændelser eller cybersikkerhedshændelser svarende til en omfattende cybersikkerhedshændelse på grundlag af de oplysninger, der er omhandlet i stk. 2, og

c) om ydelsen af støtte er i overensstemmelse med Unionens politik over for og de overordnede relationer med dette land, og om den er i overensstemmelse med andre EU-politikker på sikkerhedsområdet.

Kommissionen hører i forbindelse med den i første afsnit omhandlede vurdering den højtstående repræsentant med hensyn til kriteriet i nævnte afsnits litra c).

Hvis Kommissionen konkluderer, at et tredjeland, der er associeret til programmet for et digitalt Europa, opfylder alle betingelserne i første afsnit, forelægger Kommissionen Rådet et forslag om vedtagelse af en gennemførelsesretsakt i overensstemmelse med stk. 4 om bemyndigelse til at yde støtte fra EU's cybersikkerhedsreserve til det pågældende land.

4. Rådet kan vedtage de gennemførelsesretsakter, der er omhandlet i stk. 3. Disse nævnte gennemførelsesretsakter finder anvendelse i højst ét år. De kan fornyes. De kan omfatte en grænse på mindst 75 dage for det antal dage, for hvilke der kan ydes støtte som svar på en enkelt anmodning.

Med henblik på denne artikel træffer Rådet en afgørelse hurtigt, og det vedtager som hovedregel de i dette stykke omhandlede gennemførelsesretsakter senest otte uger efter vedtagelsen af det relevante forslag fra Kommissionen i henhold til stk. 3, tredje afsnit.

5. Rådet kan til enhver tid på forslag af Kommissionen ændre eller ophæve en gennemførelsesretsakt vedtaget i henhold til stk. 4.

Hvis Rådet finder, at der er sket en væsentlig ændring vedrørende kriteriet i stk. 3, første afsnit, litra c), kan Rådet ændre eller ophæve en gennemførelsesretsakt vedtaget i henhold til stk. 4 på behørigt begrundet initiativ fra en eller flere medlemsstater.

6. Ved udøvelsen af sine gennemførelsesbeføjelser i henhold til denne artikel anvender Rådet de i stk. 3, første afsnit, omhandlede kriterier og redegør for sin vurdering af disse kriterier. Navnlig når Rådet handler på eget initiativ i henhold til stk. 5, andet afsnit, redegør det for den væsentlige ændring, der er omhandlet i nævnte afsnit.

7. Støtte fra EU's cybersikkerhedsreserve til et tredjeland, der er associeret til programmet for et digitalt Europa, er i overensstemmelse med denne forordning og opfylder eventuelle specifikke betingelser, der er fastsat i den aftale, der er omhandlet i stk. 1.

8. Brugere fra tredjelande, der er associeret til programmet for et digitalt Europa, der er berettigede til levering af tjenester fra EU's cybersikkerhedsreserve, omfatter kompetente myndigheder såsom enheder, der håndterer IT-sikkerhedshændelser eller tilsvarende enheder, og cyberkrisestyringsmyndigheder.

9. Tredjelande, der er associeret til programmet for et digitalt Europa, og som er berettiget til støtte fra EU's cybersikkerhedsreserve, udpeger en myndighed, der skal fungere som et centralt kontaktpunkt med henblik på denne forordning.

10. Anmodninger om støtte fra EU's cybersikkerhedsreserve i henhold til denne artikel vurderes af Kommissionen. Den ordregivende myndighed må kun yde støtte til et tredjeland, hvis og så længe en gennemførelsesretsakt fra Rådet om bemyndigelse af en sådan støtte til det pågældende land vedtaget i henhold til nærværende artikels stk. 4 er i kraft. Et svar sendes uden unødig forsinkelse til de brugere, der er omhandlet i artikel 14, stk. 3, litra c).

11. Når Kommissionen modtager en anmodning om støtte i henhold til denne artikel, underretter den straks Rådet herom. Kommissionen holder Rådet underrettet om vurderingen af anmodningen. Kommissionen samarbejder også med den højtstående repræsentant om de modtagne anmodninger og gennemførelsen af den støtte, der ydes til tredjelande, der er associeret til programmet for et digitalt Europa, fra EU's cybersikkerhedsreserve. Desuden tager Kommissionen også hensyn til ENISA's eventuelle synspunkter vedrørende disse anmodninger.

Artikel 20

Koordinering med EU-krisestyringsmekanismer

1. Hvis en væsentlig cybersikkerhedshændelse, en omfattende cybersikkerhedshændelse eller en cybersikkerhedshændelse svarende til en omfattende cybersikkerhedshændelse skyldes eller resulterer i en katastrofe som defineret i artikel 4, nr. 1), i afgørelse nr. 1313/2013/EU, supplerer støtten til reaktioner på en sådan hændelse, der ydes i henhold til denne forordning, foranstaltninger i henhold til nævnte afgørelse uden at berøre nævnte afgørelse.

2. I tilfælde af en omfattende cybersikkerhedshændelse eller en cybersikkerhedshændelse svarende til en omfattende cybersikkerhedshændelse, hvor EU's integrerede ordninger for politisk kriserespons i henhold til gennemførelsesafgørelse (EU) 2018/1993 (IPCR-ordninger) aktiveres, skal støtten, der ydes i henhold til denne forordning til at reagere på en sådan hændelse, håndteres i overensstemmelse med de relevante procedurer i henhold til IPCR-ordningerne.

Kapitel IV

Europæisk mekanisme til gennemgang af cybersikkerhedshændelser

Artikel 21

Europæisk mekanisme til gennemgang af cybersikkerhedshændelser

1. Efter anmodning fra Kommissionen eller EU-CyCLONe gennemgår og vurderer ENISA med støtte fra CSIRT-netværket og med de berørte medlemsstaters godkendelse cybertrusler, kendte sårbarheder, der kan udnyttes, og afbødende foranstaltninger ved specifikke, væsentlige cybersikkerhedshændelser eller omfattende cybersikkerhedshændelser. Efter afsluttet gennemgang og vurdering af en hændelse fremsender ENISA med henblik på at indhøste erfaringer for at undgå eller afbøde fremtidige hændelser en rapport om hændelsen til EU-CyCLONe, CSIRT-netværket, de berørte medlemsstater og Kommissionen som støtte til udførelsen af deres opgaver, navnlig opgaver fastsat i artikel 15 og 16 i direktiv (EU) 2022/2555. Når en hændelse har indvirkning på et tredjeland, der er associeret til programmet for et digitalt Europa, forelægger ENISA også rapporten for Rådet. I sådanne tilfælde forelægger Kommissionen rapporten for den højtstående repræsentant.

2. Ved udarbejdelse af den i denne artikels stk. 1 omhandlede rapport om gennemgang af en hændelse samarbejder ENISA med og indsamler feedback fra alle relevante interessenter, herunder repræsentanter for medlemsstaterne, Kommissionen, andre relevante EU-institutioner, -organer, -kontorer og -agenturer, industrien, herunder udbydere af administrerede sikkerhedstjenester og brugere af cybersikkerhedstjenester. Hvor det er relevant, arbejder ENISA, i samarbejde med CSIRT'er og i givet fald kompetente myndigheder udpeget eller oprettet i henhold til artikel 8, stk. 1, i direktiv (EU) 2022/2555, også sammen med enheder, der er berørt af væsentlige cybersikkerhedshændelser eller omfattende cybersikkerhedshændelser. De hørte repræsentanter skal oplyse om eventuelle interessekonflikter.

3. Rapporten om gennemgang af en hændelse omhandlet i denne artikels stk. 1, omfatter en gennemgang og analyse af den specifikke væsentlige cybersikkerhedshændelse eller omfattende cybersikkerhedshændelse, herunder de vigtigste årsager, kendte sårbarheder, der kan udnyttes, og indhøstede erfaringer. ENISA sikrer, at rapporten er i overensstemmelse med EU-retten eller national ret vedrørende beskyttelse af følsomme eller klassificerede informationer. Hvis de relevante medlemsstater eller andre brugere, der er omhandlet i artikel 14, stk. 3, som er berørt af hændelsen anmoder herom, skal data of oplysninger i rapporten være anonymiserede. Den må ikke indeholde oplysninger om aktivt udnyttede sårbarheder, der ikke er blevet udbedret.

4. Rapporten om gennemgang af en hændelse skal, hvor det er relevant, indeholde anbefalinger til forbedring af Unionens cyberposition og kan omfatte bedste praksis og erfaringer fra relevante interessenter.

5. ENISA kan udstede en offentligt tilgængelig udgave af rapporten om gennemgang af en hændelse. Denne udgave af rapporten må kun indeholde pålidelige offentlige oplysninger eller andre pålidelige oplysninger med den eller de berørte medlemsstaters samtykke og, for så vidt angår oplysninger om en bruger som omhandlet i artikel 14, stk. 3, litra b) eller c), med den pågældende brugers samtykke.

Kapitel V

Afsluttende bestemmelser

Artikel 22

Ændringer af forordning (EU) 2021/694

I forordning (EU) 2021/694 foretages følgende ændringer:

1) Artikel 6 ændres således:

a) Stk. 1 ændres således:

i) Følgende litra indsættes:

"aa) støtte udviklingen af det europæiske cybersikkerhedsvarslingssystem, der er oprettet ved artikel 3 i Europa-Parlamentets og Rådets forordning (EU) …/…[*+] ("det europæiske cybersikkerhedsvarslingssystem"), herunder udvikling, udrulning og drift af nationale cyberknudepunkter og grænseoverskridende cyberknudepunkter, der bidrager til et øget situationsbevidsthed i Unionen og til at styrke Unionens cybermæssige trusselsefterretningskapacitet.

---

[*] Europa-Parlamentets og Rådets forordning (EU) …/… om foranstaltninger til styrkelse af solidariteten og kapaciteten i Unionen til at opdage, forberede sig og reagere på cybersikkerhedstrusler og -hændelser og om ændring af forordning (EU) 2021/694 (forordning om cybersolidaritet) (EUT L, …, ELI: …)."

[+] EUT: Indsæt venligst nummeret på forordningen i dokument PE-CONS 94/24 (2023/0109(COD)) i teksten, og indsæt forordningens nummer, dato, EUT-henvisning og ELI-henvisning i fodnoten.

ii) Følgende litra tilføjes:

"g) etablere og drive en cybersikkerhedsberedskabsmekanisme, der er oprettet ved artikel 10 i forordning (EU) …/…[+], herunder EU-cybersikkerhedsreserven, der er oprettet ved artikel 14 i nævnte forordning ("EU's cybersikkerhedsreserve") for at hjælpe medlemsstaterne med at forberede sig og reagere på væsentlige cybersikkerhedshændelser og omfattende cybersikkerhedshændelser som supplement til nationale ressourcer og kapaciteter og andre former for støtte, der er til rådighed på EU-plan, og for at støtte andre brugere i at reagere på væsentlige cybersikkerhedshændelser og omfattende cybersikkerhedshændelser".

b) Stk. 2 affattes således:

"2. Foranstaltningerne under specifikt mål nr. 3 gennemføres primært gennem det europæiske industri-, teknologi- og forskningskompetencecenter for cybersikkerhed og netværket af nationale koordinationscentre i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) 2021/887[*]. Dog gennemføres EU's cybersikkerhedsreserve af Kommissionen og, i overensstemmelse med artikel 14, stk. 6, i forordning (EU) …/…[**+], af ENISA.

---

[*] Europa-Parlamentets og Rådets forordning (EU) 2021/887 af 20. maj 2021 om oprettelse af Det Europæiske Industri-, Teknologi- og Forskningskompetencecenter for Cybersikkerhed og Netværket af Nationale Koordinationscentre (EUT L 202 af 8.6.2021, s. 1)."

[+] EUT: Indsæt venligst nummeret på forordningen i dokument PE-CONS 94/24 (2023/0109(COD)) i teksten.

2) Artikel 9 ændres således:

a) Stk. 2, litra b), c) og d), affattes således:

"b) 1 760 806 000 EUR til specifikt mål nr. 2 – Kunstig intelligens

c) 1 372 020 000 EUR til specifikt mål nr. 3 – Cybersikkerhed og tillid

d) 482 640 000 EUR til specifikt mål nr. 4 – Højtudviklede digitale færdigheder."

b) Følgende stykke tilføjes:

"8. Uanset artikel 12, stk. 1, i finansforordningen overføres uudnyttede forpligtelses- og betalingsbevillinger til foranstaltninger i forbindelse med gennemførelsen af EU's cybersikkerhedsreserve og de aktioner der støtter gensidig bistand i henhold til forordning …/…[+], der forfølger de mål, der er fastsat i nærværende forordnings artikel 6, stk. 1, litra g), automatisk, og der kan indgås forpligtelser og betales frem til den 31. december i det følgende regnskabsår. Europa-Parlamentet og Rådet underrettes om bevillinger, der overføres i henhold til artikel 12, stk. 6, i finansforordningen."

[+] EUT: Indsæt venligst nummeret på forordningen i dokument PE-CONS 94/24 (2023/0109(COD)) i teksten.

3) I artikel 12 foretages følgende ændringer:

a) Følgende stykker indsættes:

"5a. Stk. 5 finder for så vidt angår retlige enheder, der er etableret i Unionen, men som kontrolleres fra tredjelande, ikke anvendelse på tiltagene til gennemførelse af det europæiske cybersikkerhedsvarslingssystem, hvis begge følgende betingelser er opfyldt med hensyn til det pågældende tiltag:

"a) der er en reel risiko for, under hensyntagen til resultaterne af den kortlægning, der er foretaget i henhold til artikel 9, stk. 4, i forordning (EU) …/…[+], at de værktøjer, infrastrukturer eller tjenester, der er nødvendige og tilstrækkelige til, at dette tiltag i tilstrækkelig grad kan bidrage til målet for det europæiske cybersikkerhedsvarslingssystem, ikke vil være tilgængelige hos retlige enheder, der er etableret eller anses for at være etableret i medlemsstaterne, og som kontrolleres af medlemsstaterne eller af statsborgere i medlemsstaterne

b) sikkerhedsrisikoen ved indkøb fra sådanne retlige enheder inden for det europæiske cybersikkerhedsvarslingssystem står i et rimeligt forhold til fordelene og underminerer ikke Unionens og dens medlemsstaters væsentlige sikkerhedsinteresser.

[+] EUT: Indsæt venligst nummeret på forordningen i dokument PE-CONS 94/24 (2023/0109(COD)) i teksten.

5b. Stk. 5 finder for så vidt angår retlige enheder, der er etableret i Unionen, men som kontrolleres fra tredjelande, ikke anvendelse på tiltagene til gennemførelse af EU's cybersikkerhedsreserve, hvis begge følgende betingelser er opfyldt med hensyn til det pågældende tiltag:

"a) der er en reel risiko for, under hensyntagen til resultaterne af den kortlægning, der er foretaget i henhold til artikel 14, stk. 6, i forordning (EU) …/…[+], at den teknologi, ekspertise eller kapacitet, der er nødvendig og tilstrækkelig til, at EU's cybersikkerhedsreserve kan udføre sine funktioner på passende vis, ikke vil være tilgængelig hos retlige enheder, der er etableret eller anses for at være etableret i medlemsstaterne, og som kontrolleres af medlemsstaterne eller af statsborgere i medlemsstaterne

b) sikkerhedsrisikoen ved at medtage sådanne retlige enheder i EU's cybersikkerhedsreserve står i et rimeligt forhold til fordelene og underminerer ikke Unionens og dens medlemsstaters væsentlige sikkerhedsinteresser."

b) Stk. 6 affattes således:

"6. Hvis det er behørigt begrundet af sikkerhedsmæssige årsager, kan det i arbejdsprogrammet også fastsættes, at retlige enheder, der er etableret i associerede lande, og retlige enheder, der er etableret i Unionen, men som kontrolleres fra tredjelande, kun er berettigede til at deltage i alle eller nogle af tiltagene under specifikt mål nr. 1 og 2, hvis de opfylder de krav, der skal opfyldes af disse retlige enheder for at garantere beskyttelsen af Unionens og medlemsstaternes væsentlige sikkerhedsinteresser og for at sikre beskyttelsen af oplysninger i klassificerede dokumenter. Disse krav fastsættes i arbejdsprogrammet.

Første afsnit finder for så vidt angår retlige enheder, der er etableret i Unionen, men som kontrolleres fra tredjelande, også anvendelse på tiltagene under specifikt mål nr. 3:

a) at gennemføre det europæiske cybersikkerhedsvarslingssystem, hvor stk. 5a finder anvendelse, og

b) at gennemføre EU's cybersikkerhedsreserve, hvor stk. 5b finder anvendelse."

4) Artikel 14, stk. 2, affattes således:

"2. Programmet kan yde finansiering i enhver af de former, der er fastsat i finansforordningen, herunder navnlig gennem udbud som den primære form eller tilskud og priser.

Hvor det er nødvendigt at indkøbe innovative varer og tjenester for at opfylde målsætningen for en foranstaltning, må der kun ydes tilskud til støttemodtagere, der er ordregivende myndigheder eller ordregivende enheder som defineret i Europa-Parlamentets og Rådets direktiv 2014/24/EU* og 2014/25/EU**.

Hvor levering af innovative varer eller tjenester, som endnu ikke er kommercielt tilgængelige i stor skala, er nødvendig for at opfylde målsætningen for en foranstaltning, kan den ordregivende myndighed eller den ordregivende enhed godkende tildelingen af flere kontrakter inden for samme udbudsprocedure.

Ud fra behørigt begrundede hensyn til den offentlige sikkerhed kan den ordregivende myndighed eller den ordregivende enhed kræve, at kontraktens opfyldelsessted skal være inden for Unionens område.

Ved gennemførelse af udbudsprocedurer vedrørende EU's cybersikkerhedsreserve, kan Kommissionen og ENISA fungere som indkøbscentral på vegne af tredjelande, der er associeret til programmet i overensstemmelse med denne forordnings artikel 10. Kommissionen og ENISA kan også fungere som grossist ved at købe, oplagre og videresælge eller donere varer og tjenesteydelser, herunder leje, til disse tredjelande. Uanset artikel 168, stk. 3, i Europa-Parlamentets og Rådets forordning (EU, Euratom) 2024/2509[***] er en anmodning fra et enkelt tredjeland tilstrækkelig til at give Kommissionen eller ENISA mandat til at handle.

Ved gennemførelse af udbudsprocedurer vedrørende EU's cybersikkerhedsreserve, kan Kommissionen og ENISA fungere som indkøbscentral på vegne af EU's institutioner, organer, kontorer eller agenturer. Kommissionen og ENISA kan også fungere som grossist ved at købe, oplagre og videresælge eller donere varer og tjenesteydelser, herunder leje, til EU's institutioner, organer, kontorer og agenturer. Uanset artikel 168, stk. 3, i forordning (EU, Euratom) 2024/2509[+] er en anmodning fra en enkelt EU-institution, et enkelt EU-organ, -kontor eller -agentur tilstrækkeligt til at give Kommissionen eller ENISA mandat til at handle.

Programmet kan også stille finansiering til rådighed i form af finansielle instrumenter under blandingsoperationer.

---

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

** Europa-Parlamentets og Rådets direktiv 2014/25/EU af 26. februar 2014 om fremgangsmåderne ved indgåelse af kontrakter inden for vand- og energiforsyning, transport samt posttjenester og om ophævelse af direktiv 2004/17/EF (EUT L 94 af 28.3.2014, s. 243).

*** Europa-Parlamentets og Rådets forordning (EU, Euratom) 2024/2509 af 23. september 2024 om de finansielle regler vedrørende Unionens almindelige budget (EUT L, 2024/2509, ELI: http://data.europa.eu/eli/reg/2024/2509/oj)."

5) Følgende artikel indsættes:

"*Artikel 16a*

Regelkonflikter

For så vidt angår foranstaltninger til gennemførelse af det europæiske cybersikkerhedsvarslingssystem, er reglerne fastsat i artikel 4, 5 og 9 i forordning (EU) …/…[+]. I tilfælde af konflikt mellem bestemmelserne i nærværende forordning og artikel 4, 5 og 9 i forordning (EU) …/…[+] har sidstnævnte forrang og finder anvendelse på disse specifikke foranstaltninger.

[+] EUT: Indsæt venligst nummeret på forordningen i dokument PE-CONS 94/24 (2023/0109(COD)) i teksten.

For så vidt angår EU's cybersikkerhedsreserve, er der fastsat specifikke regler for deltagelse af tredjelande, der er associeret til programmet, i artikel 19 i forordning (EU) …/…[+]. I tilfælde af konflikt mellem bestemmelserne i nærværende forordning og artikel 19 i forordning (EU) …/…[+] har sidstnævnte forrang og finder anvendelse på disse specifikke foranstaltninger."

6) Artikel 19 affattes således:

"*Artikel 19*
Tilskud

Tilskud i henhold til programmet tildeles og forvaltes i overensstemmelse med afsnit VIII i finansforordningen og kan dække op til 100 % af de støtteberettigede omkostninger, uden at dette berører artikel 190 i finansforordningen. Sådanne tilskud tildeles og forvaltes som nærmere angivet for hvert specifikt mål.

Støtte i form af tilskud kan ydes direkte af ECCC uden forslagsindkaldelse til de medlemsstater, der er udvalgt i henhold til artikel 9 i forordning (EU) …/…[+], og værtskonsortiet, der er omhandlet i artikel 5 i forordning (EU) …/…[+], i overensstemmelse med artikel 195, stk. 1, litra d), i finansforordningen.

Støtte i form af tilskud til cybersikkerhedsberedskabsmekanismen, kan tildeles direkte af ECCC til medlemsstaterne uden forslagsindkaldelse i overensstemmelse med artikel 195, stk. 1, litra d), i finansforordningen.

[+] EUT: Indsæt venligst nummeret på forordningen i dokument PE-CONS 94/24 (2023/0109(COD)) i teksten.

For så vidt angår foranstaltninger til støtte for gensidig bistand fastsat i artikel 18 i forordning (EU) …/…[+] underretter ECCC Kommissionen og ENISA om medlemsstaternes anmodninger om direkte tilskud uden indkaldelse af forslag.

For så vidt angår foranstaltninger til støtte for gensidig bistand fastsat i artikel 18 i forordning (EU) …/…[+] og i overensstemmelse med artikel 193, stk. 2, andet afsnit, litra a), i finansforordningen, kan omkostningerne i behørigt begrundede tilfælde betragtes som støtteberettigede, selv om de blev afholdt, inden ansøgningen om tilskud blev indgivet."

7) Bilag I og II ændres som anført i bilaget til denne forordning.

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 14, stk. 7, tillægges Kommissionen for en periode på fem år fra den … [datoen for denne forordnings ikrafttræden]. 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.

[+] EUT: Indsæt venligst nummeret på forordningen i dokument PE-CONS 94/24 (2023/0109(COD)) i teksten.

3. Den i artikel 14, stk. 7, 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 14, stk. 7, 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 koordinationsudvalget for programmet for et digitalt Europa, der er omhandlet i artikel 31, stk. 1, i forordning (EU) 2021/694. 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.

Artikel 25

Evaluering og revision

1. Senest den … [to år efter datoen for denne forordnings anvendelse] og derefter mindst hvert fjerde år evaluerer Kommissionen, hvordan foranstaltningerne fastsat i denne forordning fungerer, og forelægger en rapport for Europa-Parlamentet og Rådet.

2. Den i stk. 1 omhandlede evaluering skal navnlig vurdere følgende:

a) antallet af oprettede nationale cyberknudepunkter og grænseoverskridende cyberknudepunkter, omfanget af den udvekslede information, herunder om muligt indvirkningen på CSIRT-netværkets arbejde, og i hvilket omfang disse har bidraget til at styrke Unionens fælles opdagelse af og situationsbevidsthed vedrørende cybertrusler og -hændelser og til udviklingen af de nyeste teknologier samt anvendelsen af midler fra programmet for et digitalt Europa til cybersikkerhedsværktøjer, infrastruktur eller tjenester, der indkøbes i fællesskab, og, hvis oplysningerne er tilgængelige, graden af samarbejde mellem nationale cyberknudepunkter og sektorielle og tværsektorielle fællesskaber af væsentlige og vigtige enheder som omhandlet i artikel 3 i direktiv (EU) 2022/2555

b) anvendelsen og effektiviteten af foranstaltninger under cybersikkerhedsberedskabsmekanismen til støtte for beredskab, herunder uddannelse, reaktion på den indledende genopretning eftervæsentlige cybersikkerhedshændelser, omfattende cybersikkerhedshændelser og cybersikkerhedshændelser svarende til omfattende cybersikkerhedshændelser, herunder anvendelse af midler fra programmet for et digitalt Europa og de indhøstede erfaringer og anbefalinger fra gennemførelsen af cybersikkerhedsberedskabsmekanismen

c) anvendelsen og effektiviteten af EU's cybersikkerhedsreserve i forhold til typen af brugere, herunder anvendelsen af midler fra programmet for et digitalt Europa, udbredelsen af tjenester, herunder deres type, den gennemsnitlige tid til at besvare anmodninger og indsætte EU's cybersikkerhedsreserve, procentdelen af tjenester, der konverteres til beredskabstjenester i forbindelse med forebyggelse af og reaktioner på hændelser, og de indhøstede erfaringer og anbefalinger fra gennemførelsen af EU's cybersikkerhedsreserve

d) denne forordnings bidrag til at styrke industriens og tjenesteydelsernes konkurrenceevne i Unionen i hele den digitale økonomi, herunder mikrovirksomheder og små og mellemstore virksomheder samt nystartede virksomheder, og bidraget til det overordnede mål om at styrke arbejdsstyrkens færdigheder og kapacitet inden for cybersikkerhed.

3. På grundlag af de rapporter, der er omhandlet i stk. 1, forelægger Kommissionen i givet fald Europa-Parlamentet og Rådet et lovgivningsforslag om ændring af denne forordning.

Artikel 26

Ikrafttræden

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

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

Udfærdiget i …, den …

På Europa-Parlamentets vegne	*På Rådets vegne*
Formand	*Formand*

BILAG

I forordning (EU) 2021/694 foretages følgende ændringer:

1) I bilag I affattes afsnittet "Specifikt mål nr. 3 – Cybersikkerhed og tillid" således:

"Specifikt mål nr. 3 – Cybersikkerhed og tillid

Programmet skal fremme styrkelse, opbygning og erhvervelse af afgørende kapacitet til at sikre Unionens digitale økonomi, samfund og demokrati ved at styrke Unionens industrielle potentiale og konkurrenceevne inden for cybersikkerhed samt ved at forbedre både den private og den offentlige sektors kapacitet til at beskytte borgere og virksomheder mod cybertrusler, herunder ved at understøtte gennemførelsen af direktiv (EU) 2016/1148.

De indledende og, hvor det er relevant, efterfølgende tiltag under dette mål omfatter:

1. Investeringer i fællesskab med medlemsstaterne i højtudviklet cybersikkerhedsudstyr, -infrastruktur og -knowhow, som er afgørende for beskyttelsen af kritiske infrastrukturer og det digitale indre marked generelt. Sådanne fælles investeringer kan omfatte investeringer i kvantefaciliteter og dataressourcer til cybersikkerhed, situationsbevidsthed vedrørende cyberspace, herunder nationale cyberknudepunkter og grænseoverskridende cyberknudepunkter, der udgør det europæiske cybersikkerhedsvarslingssystem, samt andre værktøjer, som skal gøres tilgængelige for offentlige og private sektorer i hele Europa.

2. Opskalering af eksisterende teknologisk kapacitet og netværkssamarbejde mellem kompetencecentrene i medlemsstaterne, idet det sikres, at nævnte kapacitet opfylder den offentlige sektors og industriens behov, herunder gennem produkter og tjenester, som styrker cybersikkerhed og tillid inden for det digitale indre marked.

3. Sikring af en bred udrulning af effektive, avancerede cybersikkerheds- og tillidsløsninger i alle medlemsstater. En sådan udrulning omfatter styrkelse af produkters sikkerhed fra udformning til kommercialisering af dem.

4. Støtte til at slå bro over færdighedskløften inden for cybersikkerhed under hensyntagen til kønsbalancen ved f.eks. at ensrette programmerne for cybersikkerhedsfærdigheder, tilpasse dem til specifikke sektorbehov og lette adgangen til målrettet specialiseret uddannelse.

5. Fremme af solidaritet mellem medlemsstaterne i forbindelse med beredskab og indsats ved væsentlige cybersikkerhedshændelser gennem udrulning af cybersikkerhedstjenester på tværs af grænserne, herunder støtte til gensidig bistand mellem offentlige myndigheder og etablering af en reserve af betroede udbydere af administrerede sikkerhedstjenester på EU-plan."

2) I bilag II affattes afsnittet "Specifikt mål nr. 3 – Cybersikkerhed og tillid" således:

"Specifikt mål nr. 3 – Cybersikkerhed og tillid

3.1. Antallet af cybersikkerhedsinfrastrukturer eller værktøjer eller begge dele, som er indkøbt i fællesskab, herunder inden for rammerne af det europæiske cybersikkerhedsvarslingssystem

3.2. Antal brugere og brugersamfund, som får adgang til europæiske cybersikkerhedsfaciliteter

3.3. Antal foranstaltninger til støtte for beredskab og reaktion på cybersikkerhedshændelser inden for rammerne af cyberberedskabsmekanismen".

Der er fremsat en erklæring vedrørende denne retsakt, og den kan findes i [EUT indsæt venligst: EUT C XXX, XX.XX.2024, s. XX] og via følgende link: [EUT: indsæt venligst link til erklæringen].