Rådet for
Den Europæiske Union

Bruxelles, den 31. oktober 2022
(OR. en)

14128/22

Interinstitutionel sag:
2022/0085(COD)

CYBER 343
TELECOM 428
INST 396
CSC 472
CSCI 157
INF 176
FIN 1158
BUDGET 22
DATAPROTECT 294
CODEC 1617

I/A-PUNKTSNOTE

fra:	Generalsekretariatet for Rådet
til:	De Faste Repræsentanters Komité (2. afdeling)/Rådet
Tidl. dok. nr.:	10097/5/22 REV 5
Komm. dok. nr.:	7474/22 + ADD 1
Vedr.:	Forslag til Europa-Parlamentets og Rådets forordning om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i EU's institutioner, organer, kontorer og agenturer - Generel indstilling

INDLEDNING

1. Den 22. marts 2022 vedtog Kommissionen forslaget til forordning om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i EU's institutioner, organer, kontorer og agenturer. Forslaget var en af de påtænkte foranstaltninger i EU's strategi for cybersikkerhed for det digitale årti[1], som har til formål at styrke Unionens kollektive modstandsdygtighed over for cybertrusler.

[1] 14133/20.

I sine konklusioner af 22. marts 2021 om denne strategi[2] understregede Rådet, at cybersikkerhed er "afgørende for en velfungerende offentlig forvaltning og velfungerende offentlige institutioner på både nationalt plan og EU-plan og for vores samfund og økonomi som helhed".

2. Kommissionens forslag, der er baseret på artikel 298 i traktaten om Den Europæiske Unions funktionsmåde, har til formål at forbedre cybersikkerhedsniveauet i EU's institutioner, organer, kontorer og agenturer ved at fastlægge en fælles ramme under behørig hensyntagen til de enkelte EU-enheders autonomi. Formålet med forslaget er navnlig:

   – at styrke CERT-EU's mandat og finansieringen af det (en uafhængig interinstitutionel IT-beredskabsenhed for EU-enheder)

   – at oprette en interinstitutionel struktur (Det Interinstitutionelle Råd for Cybersikkerhed – IICB), der samler repræsentanter for alle EU-enheder, for at sikre en korrekt gennemførelse af forordningen

   – at indføre en forpligtelse for EU-enhederne til at dele (ikkeklassificerede) oplysninger vedrørende hændelser med CERT-EU og til at rapportere om væsentlige trusler, sårbarheder og hændelser og

   – at fremme koordinering og samarbejde som reaktion på væsentlige hændelser.

3. Europa-Parlamentet udpegede Henna Virkkunen (EPP) til ordfører i det kompetente udvalg, ITRE. Udkastet til betænkning blev offentliggjort den 7. oktober 2022.

4. Den Europæiske Tilsynsførende for Databeskyttelse afgav udtalelse den 17. maj 2022[3].

---

[2] 6722/21.
[3] 9252/22.

5. I Rådet blev behandlingen af forslaget i Den Horisontale Gruppe vedrørende Cyberspørgsmål (Cybergruppen) indledt under det franske formandskab den 29. marts 2022. Det franske formandskab udarbejdede den første kompromistekst, der blev drøftet i Cybergruppen i juni 2022, og forelagde en situationsrapport[4] for Rådet den 21. juni 2022.

6. Under det tjekkiske formandskab afsatte Cybergruppen otte møder[5] til drøftelser om forslaget og om flere på hinanden følgende kompromistekster.

7. Den 23. maj 2022 anmodede formandskabet Rådets Sikkerhedsudvalgt om en udtalelse om de aspekter af forslaget, der vedrører informationssikkerhed og navnlig klassificerede informationer. Sikkerhedsudvalget afgav sin udtalelse den 19. september 2022[6]. Som foreslået af Sikkerhedsudvalget er EU's klassificerede informationer udtrykkeligt blevet udelukket fra forordningens anvendelsesområde. Bestemmelserne vedrørende undtagelser fra forpligtelsen til at dele og rapportere om oplysninger, der modtages fra andre enheder end EU-enheder, er blevet ændret i overensstemmelse hermed.

8. Den 28. oktober 2022 nåede Cybergruppen til enighed om formandskabets kompromistekst, jf. bilaget.

---

4 9719/22.

5 Den 6. og 20. juli, den 13., 21. og 28. september samt den 5., 19. og 28. oktober 2022.

6 12603/22 + COR 1.

DE VIGTIGSTE SPØRGSMÅL

9. Medlemsstaterne hilste forslaget velkommen som værende rettidigt og et supplement til det kommende direktiv om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen ("NIS 2"-direktivet) og støttede dets generelle mål. Medlemsstaterne opfordrede imidlertid til yderligere tilpasning til "NIS 2"-direktivet samt til mere gensidighed i udvekslingen af oplysninger mellem EU-enhederne og medlemsstaterne og påpegede den alt for frivillige karakter af nogle af de foreslåede foranstaltninger. Medlemsstaterne tilkendegav også, at de foretrak at fjerne henvisningerne til den fælles cyberenhed, hvis mandat og sammensætning endnu ikke er fastlagt.

10. På grundlag af drøftelserne i Cybergruppen er følgende punkter blevet udpeget som de vigtigste politiske spørgsmål:

a) Tilpasning til det kommende "NIS 2"-direktiv

Som medlemsstaterne har anmodet om, er der foretaget yderligere tilpasninger til det kommende "NIS 2"-direktiv, bl.a.:

- en række definitioner (artikel 3) er blevet tilpasset definitionerne i "NIS 2"
- der er indsat en ny artikel 7a om frivillige peerevalueringer i overensstemmelse med "NIS 2", som er tilpasset EU-enhedernes behov
- rapporteringsforpligtelserne i artikel 20 er blevet tilpasset rapporteringsforpligtelserne i "NIS 2".

b) Sammensætning af Det Interinstitutionelle Råd for Cybersikkerhed (IICB) (artikel 9)

Efter drøftelser om passende inddragelse af medlemsstaternes repræsentanter i IICB's arbejde blev der fundet et kompromis i form af en erklæring fra Rådet til optagelse i protokollen.

c) Institutionel autonomi

Der blev fundet en afbalanceret tilgang mellem medlemsstaternes ønske om at styrke overholdelsesmekanismerne og nødvendigheden af at respektere princippet om institutionel autonomi, navnlig med hensyn til revisioner og disciplinære foranstaltninger (artikel 11).

Endelig blev henvisningen til en bestemt procentdel af IT-budgettet til cybersikkerhed fjernet fra betragtning 8.

KONKLUSION

11. De Faste Repræsentanters Komité opfordres til

a) at godkende kompromisteksten i bilaget, som derefter vil udgøre mandatet for forhandlingerne med Europa-Parlamentet og

b) at henstille til Rådet, at det godkender kompromisteksten i bilaget på samlingen den 18. november 2022 og optager Rådets erklæring i addendummet til dette dokument i protokollen.

BILAG

2022/0085(COD)

Forslag til

EUROPA-PARLAMENTETS OG RÅDETS FORORDNING

om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i EU's institutioner, organer, kontorer og agenturer

EUROPA-PARLAMENTET OG RÅDET FOR DEN EUROPÆISKE UNION HAR –

under henvisning til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel 298,

under henvisning til traktaten om oprettelse af Det Europæiske Atomenergifællesskab, særlig artikel 106A,

under henvisning til forslag fra Europa-Kommissionen,

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

efter den almindelige lovgivningsprocedure, og

ud fra følgende betragtninger:

(1) I den digitale tidsalder er informations- og kommunikationsteknologi en hjørnesten i en åben, effektiv og uafhængig EU-forvaltning. Ny teknologi, øget kompleksitet og digitale systemers indbyrdes forbundethed øger cybersikkerhedsrisiciene og gør EU-forvaltningen mere sårbar over for cybertrusler og hændelser, hvilket i sidste ende udgør en trussel mod forvaltningens driftskontinuitet og evne til at sikre sine data. Selv om øget brug af cloudtjenester, allestedsnærværende brug af IT, en høj grad af digitalisering, fjernarbejde, ny teknologi og konnektivitet i dag er centrale elementer i alle aktiviteter i EU's forvaltningsenheder, er digital modstandsdygtighed endnu ikke tilstrækkelig indarbejdet.

(2) Det trusselsbillede for cybersikkerheden, som EU-[...]**enheder** står over for, udvikler sig konstant. De taktikker, teknikker og fremgangsmåder, som trusselsaktørerne benytter sig af udvikler sig konstant, men de fremtrædende bevæggrunde for sådanne angreb, dvs. fra at stjæle værdifulde fortrolige oplysninger til at tjene penge, manipulere den offentlige mening eller underminere digital infrastruktur, ændrer sig kun lidt. Den hastighed, med hvilken trusselsaktørerne gennemfører deres cyberangreb, øges hele tiden, og deres kampagner bliver mere og mere avancerede og automatiserede med angreb på eksponerede angrebsflader, der hele tiden udvides, og sårbarheder udnyttes hurtigt.

(3) EU-**enhedernes** [...] IT-miljøer har indbyrdes afhængige elementer og integrerede datastrømme, og brugerne arbejder tæt sammen. Denne sammenkobling betyder, at enhver afbrydelse, selv en, der oprindeligt var begrænset til én EU-[...]**enhed**, kan have kaskadevirkninger mere generelt, hvilket potentielt kan føre til vidtrækkende og langvarige negative virkninger for de andre. Derudover er visse [...]**EU-enheders** IT-miljøer sammenkoblet med medlemsstaternes IT-miljøer, hvilket betyder, at en hændelse i én EU-enhed udgør en risiko for cybersikkerheden i medlemsstaternes IT-miljøer og omvendt. **Desuden håndterer EU-enheder store mængder af ofte følsomme oplysninger fra medlemsstaterne, og hændelser kan derfor også påvirke medlemsstaterne negativt. Derfor er EU-enhedernes cybersikkerhed også af stor betydning for medlemsstaterne. Hændelsesspecifikke oplysninger kan også fremme detektionen af lignende cybertrusler eller hændelser, som påvirker medlemsstaterne.**

(4) EU[...]**-enhederne** er attraktive mål, der står over for højt kvalificerede trusselsaktører med adgang til mange ressourcer samt andre trusler. Men graden og modenheden af cyberrobusthed samt evnen til at reagere på ondsindede cyberaktiviteter varierer betydeligt fra den ene enhed til den anden. Det er derfor nødvendigt for en velfungerende europæisk forvaltning, at EU[...]**-enhederne** opnår et højt fælles cybersikkerhedsniveau ved at **gennemføre cybersikkerhedsforanstaltninger og gennem**[...] udveksling af oplysninger og samarbejde.

(5) Direktivet [forslag til NIS 2] om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen har til formål at forbedre offentlige og private enheders, nationale kompetente myndigheders og organers samt EU's samlede modstandsdygtighed og beredskabskapacitet inden for cybersikkerhed. Det er derfor nødvendigt, at EU[...]**-enhederne** følger trop ved at sikre regler, der er strømlinet med direktiv [forslag til NIS 2] og afspejler dets ambitionsniveau.

(6) For at opnå et højt fælles cybersikkerhedsniveau er det nødvendigt, at hver EU[...]**-enhed** etablerer en intern ramme for styring, forvaltning og kontrol af cybersikkerhedsrisici, som sikrer en effektiv og fornuftig styring af alle cybersikkerhedsrisici [...]. **Rammen bør fastlægge cybersikkerhedspolitikker, herunder procedurer til vurdering af effektiviteten af gennemførte cybersikkerhedsforanstaltninger. Rammen bør være baseret på en tilgang, der omfatter alle farer, og som har til formål at beskytte net- og informationssystemer og deres fysiske miljø mod hændelser som f.eks. tyveri, brand, oversvømmelse, telekommunikations- eller strømsvigt eller mod uautoriseret fysisk adgang til, skade på og indgreb i EU-enhedens oplysninger og faciliteter til behandling af oplysninger, som kan bringe tilgængeligheden, autenticiteten, integriteten og fortroligheden i forbindelse med data, der lagres, overføres, behandles eller er tilgængelige via net- og informationssystemer, i fare. Rammen bør afspejle resultaterne af risikoanalysen og tage hensyn til alle relevante tekniske, operationelle og organisatoriske risici for den pågældende EU-enheds cybersikkerhed.**

(6a) Med henblik på styring af de risici, der er påpeget inden for rammen, bør hver EU-enhed sikre, at der træffes passende og forholdsmæssige tekniske, operationelle og organisatoriske foranstaltninger. De bør omfatte de områder, herunder cybersikkerhedsforanstaltninger, der er fastsat i denne forordning med henblik på at styrke cybersikkerheden i hver EU-enhed.

(6b) De aktiver og risici, der er påpeget inden for rammen, samt de konklusioner, der drages af regelmæssige modenhedsvurderinger, bør afspejles i den cybersikkerhedsplan, der udarbejdes af hver EU-enhed. Cybersikkerhedsplanen bør omfatte de vedtagne cybersikkerhedsforanstaltninger med det formål at øge den samlede cybersikkerhed for den pågældende EU-enhed.

(6c) Da sikring af cybersikkerhed er en kontinuerlig proces, bør egnetheden og effektiviteten af alle foranstaltninger revideres regelmæssigt i lyset af EU-enhedernes skiftende risici, aktiver og modenhed. Rammen bør revideres med jævne mellemrum og mindst hvert tredje år, mens cybersikkerhedsplanen bør revideres mindst hvert andet år eller efter hver modenhedsvurdering eller hver revision af rammen.

(6d) EU-enheder bør regelmæssigt udveksle relevante oplysninger, bl.a. med hensyn til relevante hændelser og cybertrusler, samtidig med at der sikres fortrolighed og passende beskyttelse af de oplysninger, der leveres af den rapporterende EU-enhed.

(6e) Der bør indføres en mekanisme til at sikre effektiv udveksling af oplysninger, koordinering og samarbejde mellem EU-enhederne i tilfælde af større hændelser, herunder en klar fastlæggelse af de involverede EU-enheders roller og ansvarsområder. Det udpegede kontaktpunkt for EU-CyCLONe bør tage de udvekslede oplysninger i betragtning, når det deler relevante oplysninger med EU-CyCLONe som bidrag til den fælles situationsbevidsthed.

(7) Forskellene mellem EU[...]**-enhederne** kræver fleksibilitet i gennemførelsen, fordi den samme model ikke vil være passende for alle. Foranstaltningerne til sikring af et højt fælles cybersikkerhedsniveau bør ikke omfatte forpligtelser, der direkte griber ind i gennemførelsen af EU-[...]**enhedernes** missioner eller deres institutionelle autonomi. [...] **EU-enhederne** bør derfor etablere deres egne rammer for styring, forvaltning og kontrol af cybersikkerhedsrisici **og deres egne cybersikkerhedsplaner** samt vedtage [...]cybersikkerheds[...]**foranstaltninger**. **Ved gennemførelsen af sådanne foranstaltninger bør der tages behørigt hensyn til eksisterende synergier mellem EU-enheder med henblik på korrekt forvaltning af ressourcer og omkostningsoptimering. Der bør også tages behørigt hensyn til, at foranstaltningerne ikke har en negativ indvirkning på EU-enhedernes effektive udveksling af oplysninger og operationer med andre EU-enheder og nationale kompetente myndigheder.**

(8) Med henblik på at undgå at EU[...]**-enhederne** pålægges en uforholdsmæssig stor økonomisk og administrativ byrde, bør kravene til styring af cybersikkerhedsrisici stå i et rimeligt forhold til risikoen fra det pågældende net- og informationssystem under hensyntagen til sådanne foranstaltningers aktuelle tekniske niveau. Hver EU[...]**-enhed** bør sigte på at tildele en passende procentdel af sit IT-budget til forbedring af cybersikkerhedsniveauet [...]. **Modenhedsvurderingen bør også vurdere, om EU-enhedens udgifter til cybersikkerhed står i et rimeligt forhold til de risici, den står over for.**

(9) Et højt fælles cybersikkerhedsniveau kræver, at cybersikkerhed bliver lagt ind under hver EU-[...]**enheds** øverste ledelses tilsyn**.** [...] **Den øverste ledelse bør føre tilsyn med gennemførelsen af denne forordning, herunder etableringen af rammen for styring, forvaltning og kontrol af risici samt cybersikkerhedsplaner, der omfatter cybersikkerhedsforanstaltninger.** Adressering af cybersikkerhedskulturen, dvs. den daglige praksis for cybersikkerhed, er en integreret del af **en ramme** for cybersikkerhed i alle EU-**enheder** [...].

(10) [...] [...] **Cybersikkerheds**foranstaltningerne bør være en del af [...] cybersikkerhed**splanen** og bør specificeres nærmere i vejledende dokumenter eller henstillinger udstedt af CERT-EU. Når der udarbejdes foranstaltninger og vejledninger, bør der tages behørigt hensyn til **det aktuelle tekniske niveau og i givet fald de relevante EU-standarder og internationale standarder samt** den relevante EU-lovgivning og de relevante EU-politikker, herunder risikovurderinger og henstillinger udstedt af NIS-samarbejdsgruppen, såsom EU's koordinerede risikovurdering og EU-værktøjskassen til 5G-cybersikkerhed. Derudover kræves der muligvis certificering af IKT-produkter, -tjenester og -processer i overensstemmelse med specifikke europæiske cybersikkerhedscertificeringsordninger vedtaget i henhold til artikel 49 i forordning (EU) 2019/881. **Hvor det er relevant, bør CERT-EU samarbejde med ENISA.**

(11) I maj 2011 besluttede generalsekretærerne for EU's institutioner, organer og agenturer at etablere et første hold til en IT-beredskabsenhed for EU's institutioner, organer og agenturer (CERT-EU) under tilsyn af et interinstitutionelt styrelsesråd. Generalsekretærerne bekræftede i juli 2012 de praktiske ordninger og nåede til enighed om at bevare CERT-EU som en permanent enhed for fortsat at hjælpe med at øge det generelle IT-sikkerhedsniveau i EU's institutioner, organer og agenturer som et eksempel på synligt interinstitutionelt samarbejde inden for cybersikkerhed. I september 2012 blev CERT-EU etableret som en taskforce under Europa-Kommissionen med et interinstitutionelt mandat. I december 2017 indgik EU's institutioner og organer en interinstitutionel aftale om CERT-EU's organisation og drift[7]. Denne [...]**forordning** bør [...] **fastlægge et omfattende regelsæt for CERT-EU's organisation, funktion og drift. Bestemmelserne i denne forordning har forrang for bestemmelserne i den interinstitutionelle aftale om CERT-EU's organisation og drift, der blev indgået i december 2017.**

[...]

[7] EUT C 12 af 13.1.2018, s. 1.

(13) Mange cyberangreb er en del af bredere kampagner målrettet grupper af EU-[...]**enheder** eller interessefællesskaber, der omfatter EU[...]**-enheder**. Med henblik på at muliggøre proaktiv detektion, reaktion på hændelser eller afhjælpende foranstaltninger bør EU[...]**-enheder** underrette CERT-EU om [...] cybertrusler, [...] sårbarheder**, nærvedhændelser og** [...] hændelser og dele relevante tekniske detaljer, der muliggør detektion eller afhjælpning af samt reaktion på lignende cybertrusler, **sårbarheder, nærvedhændelser og** hændelser i andre EU-[...]**enheder**. I overensstemmelse med den planlagte tilgang i direktiv [forslag til NIS 2] bør **EU-**enheder, når de bliver opmærksomme på en væsentlig hændelse, være forpligtet til at indsende en [...] **tidlig varsling** til CERT-EU inden for 24 timer. En sådan udveksling af oplysninger vil gøre det muligt for CERT-EU at formidle oplysningerne til andre EU-[...]**enheder** samt relevante modparter med henblik på at beskytte EU's og dets modparters IT-miljøer mod lignende hændelser [...].

(13a) **I denne forordning fastlægges en flertrinstilgang for rapportering om væsentlige hændelser med henblik på at finde den rette balance mellem på den ene side hurtig rapportering, der bidrager til at afbøde potentiel spredning af væsentlige hændelser og giver EU-enhederne mulighed for at søge bistand, og på den anden side grundig rapportering, der udleder værdifulde erfaringer af de individuelle hændelser og med tiden forbedrer de enkelte EU-enheders cyberrobusthed. I den forbindelse bør denne forordning omfatte rapportering om hændelser, der på grundlag af en indledende vurdering foretaget af EU-enheden kan forårsage alvorlige operationelle forstyrrelser i EU-enhedens funktion eller finansielle tab for den pågældende EU-enhed, eller som kan påvirke andre fysiske eller juridiske personer ved at forårsage betydelig materiel eller immateriel skade. En sådan indledende vurdering bør bl.a. inddrage de berørte net- og informationssystemer, navnlig deres betydning for EU-enhedens funktion, cybertruslens alvor og tekniske karakteristika samt eventuelle underliggende sårbarheder, der udnyttes, og EU-enhedens erfaringer med lignende hændelser. Indikatorer såsom, i hvilket omfang EU-enhedens funktion påvirkes, varigheden af en hændelse eller antallet af berørte fysiske eller juridiske personer kan spille en vigtig rolle med hensyn til at fastslå, om den operationelle forstyrrelse er alvorlig.**

(13b) **Da infrastrukturen og nettene i den relevante EU-enhed og den medlemsstat, hvor den pågældende EU-enhed er beliggende, er indbyrdes forbundne, er det afgørende, at den pågældende medlemsstat uden unødig forsinkelse underrettes om en væsentlig hændelse i den pågældende EU-enhed. Med henblik herpå bør den berørte EU-enhed underrette CERT-EU's nationale modpart, der er udpeget af medlemsstaten i overensstemmelse med direktiv [forslag til NIS 2], inden for samme tidsfrist, som den bør rapportere om en væsentlig hændelse til CERT-EU. CERT-EU bør også underrette denne nationale modpart, når det bliver opmærksom på en væsentlig hændelse i medlemsstaten, medmindre den berørte EU-enhed allerede har rapporteret om den.**

(14) Udover at give CERT-EU flere opgaver og udvide dets rolle bør der oprettes et interinstitutionelt råd for cybersikkerhed (IICB), der **med henblik på at fremme et højt fælles cybersikkerhedsniveau i EU-enhederne** bør **have enekompetence** [...] [...] **til** at overvåge EU-[...]**enhedernes** gennemførelse af denne forordning og **til** at føre tilsyn med CERT-EU's gennemførelse af de generelle prioriteter og mål samt udstikke den strategiske retning for CERT-EU. IICB bør **derfor** sikre, at EU's institutioner er repræsenteret og inddrage EU's agenturer og organer gennem EU-agenturernes netværk. **IICB's organisation og funktion bør yderligere reguleres af dets interne forretningsorden, som kan omfatte nærmere præcisering af regelmæssige møder i IICB, herunder årlige forsamlinger på politisk plan, hvor repræsentanter fra den øverste ledelse i hvert medlem af IICB vil give IICB mulighed for at føre strategiske drøftelser og udstikke strategiske retningslinjer for IICB. IICB kan desuden nedsætte et forretningsudvalg til at bistå IICB i dets arbejde og delegere nogle af sine opgaver og beføjelser til samme, navnlig for så vidt angår opgaver, der kræver** [...] **specifik ekspertise hos dets medlemmer, f.eks. godkendelse af tjenestekataloget og eventuelle efterfølgende ajourføringer heraf, nærmere bestemmelser for serviceleveranceaftaler, vurderinger af dokumenter og rapporter, som EU-enhederne forelægger IICB i henhold til denne forordning, eller opgaver vedrørende udarbejdelse af afgørelser om overholdelsesforanstaltninger udstedt af IICB og overvågning af gennemførelsen heraf. IICB bør fastsætte forretningsudvalgets forretningsorden, inkl. dets opgaver og beføjelser.**

(15) CERT-EU bør støtte gennemførelsen af foranstaltningerne til sikring af et højt fælles cybersikkerhedsniveau ved hjælp af forslag til vejledende dokumenter og henstillinger til IICB eller ved at udstede opfordringer til tiltag. Sådanne vejledende dokumenter og henstillinger bør godkendes af IICB. Når det er nødvendigt, bør CERT-EU udstede opfordringer til tiltag, der beskriver hastende sikkerhedsforanstaltninger, som EU[...]**-enhederne** kraftigt opfordres til at træffe inden en fastsat frist**. IICB kan instruere CERT-EU i at udstede, tilbagekalde eller ændre et foreslået vejledende dokument, en henstilling eller en opfordring til tiltag.**

(16) IICB bør overvåge overholdelsen af denne forordning og opfølgningen på vejledende dokumenter, henstillinger og opfordringer til tiltag [...]. IICB bør i tekniske spørgsmål støttes af rådgivende grupper, der sammensættes, som IICB finder det bedst, og som arbejder tæt sammen med CERT-EU, EU[...]**-enhederne** og andre interessenter efter behov. [...]**Hvis IICB finder, at EU-enhederne ikke har anvendt eller gennemført denne forordning, herunder de vejledende dokumenter, henstillinger og opfordringer til tiltag, der er udstedt i medfør af denne forordning, kan IICB, uden at dette berører den pågældende EU-enheds interne procedurer, iværksætte overholdelsesforanstaltninger. Systemet med overholdelsesforanstaltninger bør anvendes med progressiv strenghed, dvs. når IICB vedtager overholdelsesforanstaltningerne, bør det begynde med en advarsel som den mindst alvorlige foranstaltning og om nødvendigt trappe op til den strengeste foranstaltning, der består i at udstede en meddelelse med en henstilling om midlertidig suspension af datastrømme til den pågældende EU-enhed, som vil blive anvendt i ekstraordinære tilfælde, hvis den pågældende enhed langvarigt, forsætligt og/eller i alvorlig grad ikke overholder sin forpligtelse i henhold til denne forordning.**

(16a) Advarslen udgør den mindst strenge overholdelsesforanstaltning til afhjælpning af påviste mangler hos EU-enheden og omfatter henstillinger om, at den ændrer sine cybersikkerhedsdokumenter inden for en nærmere fastsat frist. Advarslen bør være tilgængelig for alle EU-enheder, medmindre den er behørigt begrænset i overensstemmelse med denne forordning.

(16b) IICB kan endvidere opfordre til, at der foretages en revision af en EU-enhed. EU-enheden kan anvende sin interne revisionsfunktion til dette formål. IICB kan også anmode om, at en revision udføres af en tredjepartsrevisionstjeneste, herunder en gensidigt aftalt tjenesteudbyder i den private sektor.

(16c) På grundlag af resultaterne af en revision udført efter henstilling eller anmodning fra IICB kan IICB endvidere anmode EU-enheden om at bringe styring, forvaltning og kontrol af cybersikkerhedsrisici i overensstemmelse med bestemmelserne i denne forordning.

(16d) Da medlemsstaterne deler oplysninger, der kan være af følsom karakter, med relevante EU-enheder, er cybersikkerheden hos modtageren af sådanne oplysninger af afgørende betydning for medlemsstaterne. I ekstraordinære tilfælde af langvarig, forsætlig, gentagen og/eller alvorlig manglende opfyldelse af EU-enhedens forpligtelse kan IICB derfor som en sidste udvej udstede en meddelelse til alle medlemsstater og EU-enheder med en henstilling om midlertidig suspension af datastrømme til EU-enheden, som bør opretholdes, indtil denne enheds cybersikkerhedssituation er udbedret. Denne meddelelse bør fremsendes til alle medlemsstater og EU-enheder gennem passende sikre kommunikationskanaler.

(16e) **For at sikre korrekt gennemførelse af denne forordning bør IICB, hvis det mener, at en EU-enheds vedvarende overtrædelse af denne forordning er direkte forårsaget af en medarbejders handlinger eller undladelser, herunder i den øverste ledelse, anmode den pågældende EU-enhed om at iværksætte passende tiltag over for den pågældende medarbejder i overensstemmelse med personalevedtægten samt andre tilsvarende regler, der finder anvendelse i visse EU-enheder. Disse tiltag kan f.eks. omfatte disciplinærsager og, hvor det er relevant, i det specifikke tilfælde med EU-agenturer, en anmodning til den kompetente myndighed om at tage de nødvendige skridt i forbindelse med en eventuel afskedigelse af den person, der kan være ansvarlig for den vedvarende overtrædelse af denne forordning.**

(17) CERT-EU bør have som mission at bidrage til IT-miljøets sikkerhed i alle EU[...]**-enheder**. **Når CERT-EU overvejer at yde teknisk rådgivning eller input om relevante politiske spørgsmål efter anmodning fra en EU-enhed, bør det sikre, at dette ikke hindrer udførelsen af dets andre opgaver, der er fastsat i denne forordning.**

(17a) CERT-EU bør agere som ækvivalent til EU[...]**-enhederne** med henblik på koordineret offentliggørelse af sårbarheder for så vidt angår det europæiske sårbarhedsregister, jf. artikel 6 i direktiv [forslag til NIS 2] **og bør udarbejde en politik for styring af sårbarheder, der omfatter fremme og lettelse af frivillig koordineret offentliggørelse af sårbarheder.**

[...]

(19) CERT-EU bør også udfylde den rolle, der er fastsat i direktiv [forslag til NIS 2] for så vidt angår samarbejde og udveksling af oplysninger med netværket af enheder, der håndterer IT-sikkerhedshændelser (CSIRT'er). I overensstemmelse med Kommissionens henstilling (EU) 2017/1584[8] bør CERT-EU samarbejde om og koordinere reaktionen med de relevante interessenter. Med henblik på at bidrage til et højt cybersikkerhedsniveau i hele EU bør CERT-EU dele hændelsesspecifikke oplysninger med nationale modparter. CERT-EU bør også samarbejde med andre offentlige såvel som private modparter, herunder NATO, efter IICB's forudgående godkendelse.

[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).

(20) I forbindelse med støtte til den operationelle cybersikkerhed bør CERT-EU gøre brug af Den Europæiske Unions Agentur for Cybersikkerheds **(ENISA)** tilgængelige ekspertise i form af et struktureret samarbejde, jf. Europa-Parlamentets og Rådets forordning (EU) 2019/881[9]. Hvor det er hensigtsmæssigt, bør der indføres specifikke ordninger mellem de to enheder med henblik på at fastlægge den praktiske gennemførelse af et sådant samarbejde og undgå overlap af aktiviteter. CERT-EU bør samarbejde med [...] **ENISA** om trusselsanalyser og regelmæssigt dele sin rapport om trusselsbilledet med agenturet.

[...][10]

(22) **CERT-EU's aktiviteter og håndtering af oplysninger i henhold til denne forordning kan omfatte behandling af personoplysninger.** Alle personoplysninger, der behandles i henhold til denne forordning, bør behandles i overensstemmelse med databeskyttelseslovgivningen, herunder Europa-Parlamentets og Rådets forordning (EU) 2018/1725[11]. **Hvis personoplysninger i henhold til denne forordning fremsendes til andre modtagere, der er etableret i Unionen, end EU-enheder, bør dette ske i overensstemmelse med artikel 9 i forordning (EU) 2018/1725.**

---

9 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).

10 [...]

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

(23) CERT-EU's og EU-[...]**enhedernes** håndtering af oplysninger bør ske i overensstemmelse med de **gældende** bestemmelser [...] om informationssikkerhed [...]. [...]

(23a) Med henblik på deling af oplysninger anvendes synlige markeringer til at angive, at modtagerne af oplysningerne bør anvende delingsbegrænsninger baseret på navnlig hemmeligholdelsesaftaler eller uformelle hemmeligholdelsesaftaler såsom Traffic Light Protocol eller andre tydelige angivelser fra kilden. Traffic Light Protocol skal forstås som et middel til at informere om eventuelle begrænsninger med hensyn til yderligere spredning af oplysninger. Den anvendes i næsten alle enheder, der håndterer IT-sikkerhedshændelser (CSIRT'er), og i visse centre for informationsanalyse og -udveksling.

(24) **Denne forordning og de nye opgaver, der tildeles CERT-EU, får ikke indvirkning på de samlede udgifter under den flerårige finansielle ramme.** Eftersom CERT-EU's tjenester og opgaver er i alle EU-[...]**enheders** interesse, bør hver EU-[...]**enhed**, der afholder udgifter til IT, bidrage med en rimelig andel til CERT-EU's tjenester og opgaver. Disse bidrag berører ikke EU-[...]**enhedernes** budgetautonomi. **Alle EU-enheder og deres forvaltninger bør sikre optimering af deres ressourcer på det nuværende niveau og øge effektivitetsgevinsterne, bl.a. ved at uddybe det interinstitutionelle samarbejde på cybersikkerhedsområdet. Derfor bør en fælles tilgang til sammenlægning af administrationsudgifter være at foretrække frem for individuelle udgifter i EU-enhederne.**

(25) IICB bør med bistand fra CERT-EU gennemgå og evaluere gennemførelsen af denne forordning og fremlægge en rapport for Kommissionen herom. På baggrund af denne rapportering bør Kommissionen rapportere til Europa-Parlamentet, Rådet, Det Europæiske Økonomiske og Sociale Udvalg og Regionsudvalget. **Desuden opfordres Den Europæiske Revisionsret til regelmæssigt at evaluere, hvordan CERT-EU fungerer –**

VEDTAGET DENNE FORORDNING:

Kapitel I
ALMINDELIGE BESTEMMELSER

Artikel 1

Genstand

1. Ved denne forordning fastsættes **foranstaltninger, der har til formål at opnå et højt fælles cybersikkerhedsniveau i EU-enhederne.** [...]

2. Med henblik herpå fastsættes ved denne forordning:

c) forpligtelser for **hver** EU[...]**-enhed** til at indføre **en** [...] ramme for styring, forvaltning og kontrol af cybersikkerhedsrisici

d) forpligtelser for EU[...]**-enheder** med hensyn til styring af cybersikkerhedsrisici [...]**,** rapportering **og deling af oplysninger**

e) bestemmelser om organiseringen**, funktionen** og driften af den **uafhængige interinstitutionelle IT-beredskabsenhed** for EU-[...]**enhederne** (CERT-EU) og om organiseringen**, funktionen** og driften af Det Interinstitutionelle Råd for Cybersikkerhed **(IICB)**

f) bestemmelser vedrørende overvågning af gennemførelsen af denne forordning.

Artikel 2

Anvendelsesområde

1. Denne forordning finder anvendelse på [...] alle EU[...]**-enheder** og på [...] [...] CERT-EU og **IICB** [...].

2. Denne forordning finder anvendelse, uden at det berører den institutionelle autonomi i henhold til traktaterne.

3. Med undtagelse af artikel 12, stk. 7, finder denne forordning ikke anvendelse på net- og informationssystemer, der håndterer EU's klassificerede informationer (EUCI).

Artikel 3

Definitioner

I denne forordning forstås ved:

1) "EU-[...]**enheder**": EU-institutioner, -organer**, -kontorer** og -agenturer, der er oprettet ved eller på grundlag af traktaten om Den Europæiske Union, traktaten om Den Europæiske Unions funktionsmåde eller traktaten om oprettelse af Det Europæiske Atomenergifællesskab

2) "net- og informationssystem": **et** net- og informationssystem som [...] **defineret i** artikel 4, nr. 1), i direktiv [forslag til NIS 2]

3) "sikkerhed i net- og informationssystemer": sikkerhed i net- og informationssystemer som [...] **defineret i** artikel 4, nr. 2), i direktiv [forslag til NIS 2]

4) "cybersikkerhed": cybersikkerhed [...] **som defineret i artikel 2, nr. 1), i forordning (EU) 2019/881**

5) "øverste ledelse": leder, ledelse eller koordinerings- og tilsynsorgan på højeste administrative niveau **med beslutningskompetencer** under hensyntagen til ledelsesordningerne på højt niveau i hver EU-[...]**enhed**

5a) "nærvedhændelse": en nærvedhændelse som defineret i artikel 4, nr. 4a), i direktiv [forslag til NIS 2]

6) "hændelse": en hændelse [...] **som defineret i** artikel 4, nr. 5), i direktiv [forslag til NIS 2]

[...]

8) "større **hændelse**" [...]: enhver hændelse, **der forårsager en forstyrrelse på et niveau, som overstiger en EU-enheds og CERT-EU's kapacitet til at reagere på den, eller som har en betydelig indvirkning på mindst to EU-enheder** [...]

9) "håndtering af hændelser": håndtering af hændelser som [...] **defineret i** artikel 4, nr. 6), i direktiv [forslag til NIS 2]

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

[...]

12) "sårbarhed": sårbarhed som omhandlet i artikel 4, nr. 8), i direktiv [forslag til NIS 2]

[...]

14) "[...] risiko": **en risiko som omhandlet i artikel 4, nr. 7b), i direktiv [forslag til NIS 2]**
[...]

[...]

[...]

Artikel 3a

Behandling af personoplysninger

1) CERT-EU's, IICB's og EU-enheders behandling af personoplysninger i henhold til denne forordning foretages i overensstemmelse med forordning (EU) 2018/1725.

2) CERT-EU, IICB og EU-enhederne behandler og udveksler personoplysninger i det nødvendige omfang og udelukkende med henblik på at opfylde deres respektive forpligtelser i henhold til denne forordning.

Kapitel II
FORANSTALTNINGER TIL SIKRING AF ET HØJT FÆLLES CYBERSIKKERHEDSNIVEAU

Artikel 4

Ramme for styring, forvaltning og kontrol af risici

1. Hver EU-[...]**enhed** etablerer sin egen [...] ramme for styring, forvaltning og kontrol af cybersikkerhedsrisici ("rammen") til støtte for enhedens mission [...]**.**For at sikre en effektiv og fornuftig styring af alle cybersikkerhedsrisici, fører enhedens øverste ledelse tilsyn med [...] **rammen**. Rammen indføres senest … [15 måneder efter denne forordnings ikrafttræden].

2. Rammen skal dække hele den pågældende **EU-**[...]**enheds** uklassificerede IT-miljø, herunder lokale IT-miljøer, **driftsteknologinet,** udliciterede aktiver og tjenester i cloudcomputingmiljøer eller som hostes af tredjeparter, bærbare enheder, interne netværk, forretningsnetværk, der ikke er forbundet til internettet, og andre enheder, der er forbundet til IT-miljøet. Rammen **baseres på en tilgang, der omfatter alle farer, og på en modenhedsvurdering i henhold til artikel 6, som omfatter alle de relevante tekniske, operationelle og organisatoriske risici, der kan have indvirkning på cybersikkerheden i den pågældende EU-enhed** [...].

2a. **Rammen fastlægger cybersikkerhedspolitikker, herunder mål og prioriteter for sikkerheden i net- og informationssystemer, og politikker og procedurer til vurdering af effektiviteten af gennemførte foranstaltninger til styring af cybersikkerhedsrisici og fastlægger medarbejdernes roller og ansvarsområder.**

2b. Rammen revideres regelmæssigt og mindst hvert tredje år i lyset af EU-enhedens skiftende risici, aktiver og modenhed.

3. Den øverste ledelse i hver EU-[...]**enhed** fører **tilsyn** [...] med [...] **sin** organisations overholdelse af de forpligtelser, der vedrører styring, forvaltning og kontrol af cybersikkerhedsrisici uden at dette berører andre ledelsesniveauers formelle ansvar for overholdelse og risikostyring inden for deres respektive ansvarsområder.

3a. **Hver EU-enheds øverste ledelse kan, hvis det er relevant, og uden at det berører dens ansvar for gennemførelsen af denne forordning, delegere specifikke forpligtelser i henhold til denne forordning til andre seniormanagere i den pågældende enhed. Den øverste ledelse kan uanset en eventuel delegering af dens specifikke forpligtelse holdes ansvarlig for enhedernes manglende overholdelse af forpligtelserne i henhold til denne forordning.**

3b. Hver EU-enheds øverste ledelse sikrer, at EU-enhederne godkender cybersikkerhedsplanen med foranstaltninger til styring af cybersikkerhedsrisici i overensstemmelse med deres risikoanalyse, således at rammen gennemføres i henhold til denne forordning.

[...]

5. Hver EU-[...]**enhed** udpeger en lokal cybersikkerhedsansvarlig eller en ækvivalent funktion, der fungerer som det centrale kontaktpunkt vedrørende alle aspekter af cybersikkerhed.

Den lokale cybersikkerhedsansvarlige letter gennemførelsen af denne forordning og aflægger regelmæssigt rapport direkte til den øverste ledelse om status for gennemførelsen.

Uden at det berører den lokale cybersikkerhedsansvarlige som centralt kontaktpunkt i hver EU-enhed, kan en EU-enhed delegere visse af den lokale cybersikkerhedsansvarliges opgaver vedrørende gennemførelsen af denne forordning til CERT-EU på grundlag af en serviceleveranceaftale indgået mellem den pågældende EU-enhed og CERT-EU. IICB beslutter, om leveringen af denne tjeneste skal være en del af CERT-EU's basistjenester under hensyntagen til den pågældende EU-enheds menneskelige og finansielle ressourcer. Hver EU-enhed underretter uden unødig forsinkelse CERT-EU om de udpegede lokale cybersikkerhedsansvarlige og alle senere ændringer af disse. CERT-EU fører den løbende ajourførte liste over udpegede lokale cybersikkerhedsansvarlige.

6. Seniormanagere som omhandlet i artikel 29, stk. 2, i personalevedtægten[12] eller andre tjenestemænd på tilsvarende niveau i hver EU-enhed følger regelmæssigt specifikke kurser for at tilegne sig tilstrækkelig viden og tilstrækkelige færdigheder til at forstå og vurdere cybersikkerhedsrisici og cybersikkerhedsstyringspraksisser samt disses indvirkning på enhedens operationer.

12 Rådets forordning nr. 259/68 af 29. februar 1968 om vedtægten for tjenestemænd i De Europæiske Fællesskaber og om ansættelsesvilkårene for de øvrige ansatte i disse Fællesskaber (EFT L 56 af 4. marts 1968).

7. Hver EU-enhed indfører effektive mekanismer til sikring af, at en passende procentdel af IT-budgettet bruges på cybersikkerhed. Der skal tages behørigt hensyn til rammen ved fastsættelsen af denne procentsats.

Artikel 5

Foranstaltninger til styring af cybersikkerhedsrisici [...]

1. [...] **Hver EU-enhed sikrer under** sin øverste ledelses **tilsyn** [...] [...], **at der træffes passende og forholdsmæssige tekniske, operationelle og organisatoriske foranstaltninger til at styre de risici, der konstateres inden for den i artikel 4, stk. 1, omhandlede ramme, og til at forebygge og/eller minimere virkningen af hændelser. Under hensyntagen til det aktuelle tekniske niveau og i givet fald relevante EU-standarder og internationale standarder samt gennemførelsesomkostningerne skal disse foranstaltninger garantere et sikkerhedsniveau for net- og informationssystemer, der står i et rimeligt forhold til risiciene. Ved vurderingen af forholdsmæssigheden af disse foranstaltninger tages der behørigt hensyn til omfanget af enhedens eksponering mod risici, dens størrelse, sandsynligheden for, at der indtræffer hændelser, og alvoren af disse, herunder deres samfundsmæssige og økonomiske konsekvenser.**

[...]

3. EU-enhederne skal som minimum arbejde med følgende specifikke områder i forbindelse med gennemførelsen af foranstaltningerne til styring af cybersikkerhedsrisici i deres cybersikkerhedsplaner i overensstemmelse med vejledende dokumenter og henstillinger udstedt af IICB:

a) cybersikkerhedspolitik med hensyn til præcisering af de værktøjer og foranstaltninger, som er nødvendige for at nå de mål og prioriteter, der er omhandlet i artikel 4 og i artikel 5, stk. 4

b) politikker for risikoanalyse og informationssystemsikkerhed

c) organisering af cybersikkerheden, herunder fastlæggelse af roller og ansvarsområder

d) forvaltning af aktiver, herunder en liste over IT-aktiver og en kortlægning af IT-netværket

e) personalesikkerhed og adgangskontrol

f) driftssikkerhed

g) kommunikationssikkerhed

h) erhvervelse, udvikling og vedligeholdelse af systemer, herunder håndtering og offentliggørelse af sårbarheder

i) forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forbindelserne mellem den enkelte EU-enhed og dens direkte leverandører eller tjenesteudbydere. EU-enhederne tager hensyn til de sårbarheder, der er specifikke for hver direkte leverandør og tjenesteudbyder, og den overordnede kvalitet af deres leverandørers og tjenesteudbyderes produkter og cybersikkerhedspraksis, herunder deres sikre udviklingsprocedurer

j) håndtering af hændelser og samarbejde med CERT-EU såsom vedligeholdelse af sikkerhedsovervågning og -logning

k) styring af forretningskontinuitet såsom backupstyring, katastrofeberedskab og krisestyring og

l) fremme og udvikling af uddannelse, færdigheder, bevidstgørelse, øvelses- og uddannelsesprogrammer i forbindelse med cybersikkerhed.

4. EU-enhederne skal som minimum arbejde med følgende specifikke foranstaltninger til styring af cybersikkerhedsrisici i forbindelse med gennemførelsen af foranstaltningerne til styring af cybersikkerhedsrisici i deres cybersikkerhedsplaner i overensstemmelse med vejledende dokumenter og henstillinger udstedt af IICB:

a) mål og prioriteter for brugen af cloudcomputingtjenester som omhandlet i artikel 4, nr. 19), i direktiv [forslag til NIS 2] og tekniske foranstaltninger med henblik på at muliggøre telearbejde

b) konkrete skridt vedrørende fremtidig brug af nultillidsprincipper, herunder en sikkerhedsmodel, og en koordineret cybersikkerheds- og systemforvaltningsstrategi baseret på en anerkendelse af, at trusler findes både inden for og uden for traditionelle netgrænser

c) indførelse af multifaktorautentificering som standard for alle net- og informationssystemer

d) etablering af forsyningskædesikkerhed for så vidt angår software ved hjælp af kriterier for sikker udvikling og evaluering af software

e) forbedring af indkøbsprocedurerne med henblik på at fremme et højt fælles cybersikkerhedsniveau ved hjælp af:

i) fjernelse af kontraktmæssige hindringer, der begrænser IT-tjenesteudbydernes deling af oplysninger om hændelser, sårbarheder og cybertrusler med CERT-EU

ii) indførelse af en kontraktmæssig forpligtelse til at rapportere om hændelser, sårbarheder og cybertrusler samt til at have passende beredskab og overvågning i forbindelse med hændelser

f) brug af kryptografi og kryptering, navnlig end-to-end-kryptering

g) sikrede kommunikationssystemer i organisationen.

Artikel 6

Modenhedsvurderinger

1. Hver EU-[...]**enhed** udarbejder**, hvor det er relevant med bistand fra en specialiseret tredjepart,** mindst hvert tredje år **en** modenhedsvurdering [...], der indarbejder alle elementer af deres IT-miljø som beskrevet i artikel 4 under hensyntagen til de relevante vejledende dokumenter og henstillinger vedtaget i overensstemmelse med artikel 13.

2. IICB vedtager efter henstilling fra CERT-EU og efter høring af Den Europæiske Unions Agentur for Cybersikkerhed (ENISA) senest fire måneder efter denne forordnings ikrafttræden metodologiske retningslinjer for gennemførelse af modenhedsvurderinger.

3. EU-enheden fremsender modenhedsvurderingen [...] **til IICB, når den er afsluttet. Den første modenhedsvurdering foretages senest [12 måneder efter denne forordnings ikrafttræden].**

Artikel 7

Cybersikkerhedsplaner

1. I forlængelse af modenhedsvurderingens konklusioner og under hensyntagen til de aktiver og risici, der er konstateret i henhold til artikel 4, godkender den øverste ledelse i hver EU-[...]**enhed** en cybersikkerhedsplan uden unødig forsinkelse efter etableringen af [...] rammen, [...] **vedtagelsen af foranstaltningerne til styring af** [...] cybersikkerhed**srisici** [...] **og gennemførelsen af modenhedsvurderingen og senest 21 måneder efter denne forordnings ikrafttræden**. **Cybersikkerheds**planen skal sigte på at øge den **pågældende** [...] **EU-**enheds overordnede cybersikkerhed og derved bidrage til [...] forbedringen af et højt fælles cybersikkerhedsniveau i alle EU[...]**-enheder.** [...] **Cybersikkerheds**planen omfatter som minimum **foranstaltningerne til styring af cybersikkerhedsrisiciene i henhold til artikel 5** [...]. **Cybersikkerheds**planen revideres mindst hvert **andet** [...] år eller efter [...] **hver** modenhedsvurdering [...], der udføres i medfør af artikel 6 **eller hver revision af rammen i medfør af artikel 4.**

2. [...]

3. Cybersikkerhedsplanen **tager hensyn til** [...] alle gældende vejledende dokumenter og henstillinger **udstedt i henhold til artikel 13** [...].

4. **EU-enheden fremsender cybersikkerhedsplanen [...] til IICB, når den er færdiggjort.**

Artikel 7a

Peerevaluering

1. IICB fastlægger efter henstilling fra CERT-EU og efter høring af ENISA senest ... [24 måneder efter denne forordnings ikrafttræden] under anvendelse af metoden til peerevaluering og metoden til selvevaluering i overensstemmelse med artikel 16 i direktiv [forslag til NIS 2], om nødvendigt tilpasset EU-enhedernes behov, metoden til og de organisatoriske aspekter af peerevaluering med henblik på at lære af fælles erfaringer, styrke den gensidige tillid, opnå et højt fælles cybersikkerhedsniveau samt styrke de cybersikkerhedskapaciteter og -politikker i EU-enhederne, der er nødvendige for at gennemføre denne forordning. Deltagelse i peerevalueringer er frivillig. Repræsentanter fra medlemsstaterne kan deltage i peerevalueringerne som observatører. Peerevalueringerne gennemføres af cybersikkerhedseksperter udpeget af mindst to EU-enheder, som ikke er de samme som de EU-enheder, der evalueres, og skal dække mindst ét af følgende aspekter:

i) graden af gennemførelse af foranstaltningerne til styring af cybersikkerhedsrisici og rapporteringsforpligtelserne, jf. artikel 5 og 20

ii) kapacitetsniveauet, herunder de disponible finansielle, tekniske og menneskelige ressourcer

iii) graden af gennemførelse af rammen for deling af oplysninger, jf. artikel 19

iv) specifikke spørgsmål af tværsektoriel karakter.

2. EU-enhederne kan udpege specifikke spørgsmål, jf. stk. 1, nr. iv), som skal evalueres. Evalueringens omfang, herunder udpegede spørgsmål, meddeles de deltagende EU-enheder, inden peerevalueringen påbegyndes.

3. Inden peerevalueringen påbegyndes, kan EU-enhederne foretage en selvevaluering af de evaluerede aspekter og stille denne selvevaluering til rådighed for de udpegede eksperter.

4. Peerevalueringer omfatter fysiske eller virtuelle besøg på stedet og udvekslinger uden for stedet. I henhold til princippet om godt samarbejde giver de EU-enheder, der er omfattet af peerevalueringen, de udpegede eksperter de oplysninger, der er nødvendige for vurderingen, med forbehold af national ret eller EU-retten om beskyttelse af følsomme eller klassificerede informationer. Alle oplysninger, der indhentes i forbindelse med peerevalueringsprocessen, må kun anvendes til dette formål. De eksperter, der deltager i peerevalueringen, må ikke videregive følsomme eller klassificerede informationer, som er indhentet i forbindelse med denne evaluering, til tredjemand.

5. De samme aspekter, der været genstand for peerevaluering, og som evalueres i EU-enhederne, må ikke gøres til genstand for yderligere peerevaluering i de pågældende EU-enheder i to år efter afslutningen af peerevalueringen, medmindre EU-enhederne anmoder om andet, eller der aftales andet på forslag af IICB.

6. EU-enhederne sikrer, at enhver risiko for interessekonflikter vedrørende de udpegede eksperter meddeles de øvrige EU-enheder og IICB, inden peerevalueringen påbegyndes. De EU-enheder, der er omfattet af peerevalueringen, kan gøre indsigelse mod udpegelsen af bestemte eksperter af behørigt begrundede årsager, der meddeles de udpegende EU-enheder.

7. Eksperter, der deltager i peerevalueringer, udarbejder rapporter om resultaterne og konklusionerne af evalueringerne. EU-enhederne har mulighed for at fremsætte bemærkninger til deres respektive udkast til rapporterne, som vedlægges rapporterne. Rapporterne skal indeholde henstillinger, der gør det muligt at forbedre de aspekter, der er omfattet af peerevalueringen. Rapporterne forelægges IICB og CSIRT-netværket, når det er relevant. EU-enheder, der evalueres, kan beslutte at gøre deres rapport eller en redigeret udgave af deres rapport offentligt tilgængelig.

Artikel 8

Gennemførelse

1. [...]

2. Vejledende dokumenter og henstillinger, der er udstedt i overensstemmelse med artikel 13, understøtter gennemførelsen af bestemmelserne i dette kapitel.

3. På IICB's anmodning rapporterer EU-enhederne om specifikke aspekter af gennemførelsen af dette kapitel.

Kapitel III
DET INTERINSTITUTIONELLE RÅD FOR CYBERSIKKERHED

Artikel 9

Det Interinstitutionelle Råd for Cybersikkerhed

1. Det Interinstitutionelle Råd for Cybersikkerhed (IICB) oprettes.

2. IICB er ansvarlig for:

   a) overvågningen af **EU-**[...]**enhedernes** gennemførelse af denne forordning

   b) tilsynet med CERT-EU's gennemførelse af de generelle prioriteter og mål samt udstikkelse af den strategiske retning for CERT-EU.

3. IICB sammensættes af**:**

   a) én repræsentant udpeget af hver af følgende:

      i) Europa-Parlamentet

      ii) Det Europæiske Råd

      iii) Rådet for Den Europæiske Union

      iv) Europa-Kommissionen

      v) Den Europæiske Unions Domstol

      vi) Den Europæiske Centralbank

vii) Den Europæiske Revisionsret

viii) Tjenesten for EU's Optræden Udadtil

ix) Det Europæiske Økonomiske og Sociale Udvalg

x) Det Europæiske Regionsudvalg

xi) Den Europæiske Investeringsbank

xii) Det Europæiske Industri-, Teknologi- og Forskningskompetencecenter for Cybersikkerhed og

xiii) Den Europæiske Unions Agentur for Cybersikkerhed

b) tre repræsentanter [...] **udpeget** af EU-agenturernes netværk (EUAN) udpeget efter forslag fra netværkets rådgivende IKT-udvalg med henblik på at repræsentere interesserne i de agenturer og organer, der har deres eget IT-miljø. [...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

3a. Medlemmerne kan bistås af en suppleant. Formanden kan invitere andre repræsentanter for de **enheder**, [...] der er angivet ovenfor, eller andre EU[...]**-enheder** til at deltage i IICB's møder uden stemmeret.

4. IICB vedtager sin egen forretningsorden.

5. IICB udpeger en formand blandt medlemmerne i henhold til sin forretningsorden og for en periode på [...] **to** år. Dennes suppleant bliver fuldgyldigt medlem af IICB i samme periode.

6. IICB mødes **mindst tre gange årligt** på formandens initiativ **og/eller** efter anmodning fra CERT-EU **og/**eller efter anmodning fra et af medlemmerne.

7. Hvert medlem af IICB har én stemme. IICB's afgørelser træffes med simpelt flertal, såfremt intet andet er fastsat i denne forordning. Formanden deltager kun i afstemningen i tilfælde af stemmelighed, idet formanden har den afgørende stemme.

8. IICB kan anvende forenklet skriftlig procedure, som indledes i overensstemmelse med IICB's forretningsorden. I henhold til denne procedure anses den relevante afgørelse for godkendt inden for den tidsfrist, som formanden har fastsat, medmindre et medlem gør indsigelse.

9. CERT-EU's chef**, formanden for NIS-samarbejdsgruppen**, **formanden for EU-CyCLONe og formanden for CSIRT-netværket,** eller **deres** [...] suppleanter, [...] **kan**, medmindre andet besluttes af IICB, deltage i IICB's møder **som observatører**.

10. IICB's sekretariatsopgaver varetages af **ENISA** [...] **og refererer til IICB's formand**.

11. Repræsentanterne for EUAN, som udpeget efter forslag fra netværkets rådgivende IKT-udvalg, formidler IICB's afgørelser til **medlemmerne af EUAN**[…]. Alle EU-agenturer og -organer har ret til over for repræsentanterne eller IICB's formand at rejse ethvert spørgsmål, som de mener, IICB bør gøres opmærksom på.

12. [...]

13. IICB kan **nedsætte** [...] et forretningsudvalg til at bistå IICB i dets arbejde og delegere nogle af sine opgaver og beføjelser til samme**, navnlig de i artikel 10, litra c) og e) anførte**. IICB fastsætter forretningsudvalgets forretningsorden, inkl. dets opgaver og beføjelser, og dets medlemmers mandatperiode.

14. IICB forelægger hver 12. måned Rådet en rapport om de fremskridt, der er gjort med gennemførelsen af denne forordning, med en præcisering af navnlig omfanget af CERT-EU's samarbejde med dets nationale modparter i hver af medlemsstaterne. Denne rapport udgør et bidrag til rapporten hvert andet år om cybersikkerhedssituationen i Unionen for samme periode i overensstemmelse med artikel 15 i direktiv [forslag til NIS 2].

Artikel 10

IICB's opgaver

Når det udfører sine forpligtelser, skal IICB navnlig:

a) [...] **effektivt overvåge og føre tilsyn med anvendelsen** af denne forordning [...] **og støtte** EU-[...]**enhederne i at styrke deres cybersikkerhed**; **med henblik herpå kan IICB anmode om ad hoc-rapporter fra CERT-EU og EU-enhederne**

aa) **efter en strategisk drøftelse vedtage en flerårig strategi for forøgelse af cybersikkerhedsniveauet i EU-enhederne, vurdere den regelmæssigt og mindst hvert femte år samt ændre den, når det er nødvendigt**

b) på grundlag af et forslag **fremsat af** [...] CERT-EU's chef godkende det årlige arbejdsprogram for CERT-EU og overvåge gennemførelsen heraf

c) på grundlag af et forslag fra CERT-EU's chef godkende CERT-EU's tjenestekatalog **og eventuelle senere ajourføringer heraf**

d) på grundlag af et forslag fra CERT-EU's chef godkende den årlige finansielle planlægning af indtægter og udgifter, herunder personale, i forbindelse med CERT-EU's aktiviteter

e) på grundlag af et forslag fra CERT-EU's chef godkende modaliteterne for serviceleveranceaftaler

f) behandle og godkende den årsrapport, som udarbejdes af CERT-EU's chef, og som omfatter CERT-EU's aktiviteter og forvaltning af midler

g) på grundlag af et forslag fra CERT-EU's chef godkende og overvåge nøgleresultatindikatorer for CERT-EU

h) godkende samarbejdsaftaler, serviceleverance**aftaler** [...] eller kontrakter mellem CERT-EU og andre enheder, der indgås i medfør af artikel 17

i) nedsætte [...] tekniske rådgivende grupper til at bistå IICB i dets arbejde, [...] godkende disses mandat og udpege de respektive formænd

j) **vedtage vejledende dokumenter og henstillinger på grundlag af et forslag fra CERT-EU i henhold til artikel 13 og give CERT-EU instruks om at udstede, tilbagekalde eller ændre et forslag til vejledende dokument eller henstilling eller en opfordring til tiltag**

k) modtage og vurdere dokumenter og rapporter, som EU-enhederne forelægger i henhold til denne forordning

l) støtte oprettelsen af en uformel gruppe bestående af alle enhedernes lokale cybersikkerhedsansvarlige og derved lette udvekslingen af bedste praksis og oplysninger i forbindelse med gennemførelsen af denne forordning

m) udarbejde en cyberkrisestyringsplan for at støtte den koordinerede håndtering af større hændelser på operationelt plan, der berører EU-enheder, og for at bidrage til regelmæssig udveksling af relevante oplysninger, navnlig om virkningerne og alvoren af større hændelser, og hvordan disse kan afbødes.

Artikel 11

Overholdelse

1. IICB overvåger **i henhold til artikel 9, stk. 2, og artikel 10 effektivt** EU[...]**-enhedernes** gennemførelse af denne forordning og de vedtagne vejledende dokumenter, henstillinger og opfordringer til tiltag. **Med henblik herpå kan IICB anmode om oplysninger eller dokumentation, der er nødvendig til vurdering af EU-enhedernes korrekte anvendelse af forordningens bestemmelser. Med henblik på vedtagelse af overholdelsesforanstaltninger i henhold til denne artikel har den pågældende EU-enhed ikke stemmeret.**

2. Hvis IICB finder, at en EU-**enhed** [...] ikke effektivt har anvendt eller gennemført denne forordning eller vejledende dokumenter, henstillinger eller opfordringer til tiltag, der er udstedt i medfør af denne forordning, kan IICB, uden at dette berører den pågældende EU-[...] **enheds interne procedurer, og efter at have givet den pågældende enhed eller person mulighed for at fremsætte sine synspunkter**:

a) udstede en advarsel **om at afhjælpe konstaterede mangler inden for en nærmere fastsat frist, herunder henstillinger om at ændre cybersikkerhedsdokumenter, som EU-enhederne har vedtaget på grundlag af denne forordning**; om nødvendigt og i lyset af en markant cybersikkerhedsrisiko begrænses gruppen af modtagere af en sådan advarsel på behørig vis

aa) udstede en begrundet meddelelse til en EU-enhed, hvis de mangler, der blev konstateret i den tidligere udstedte advarsel, ikke er blevet afhjulpet i tilstrækkelig grad inden for en nærmere fastsat frist, og formelt underrette Rådet, Europa-Parlamentet og Kommissionen om denne udtalelse

b) **udstede, navnlig:** [...]

i. en henstilling om, at der foretages en revision af en EU-enhed.

ii. en anmodning om, at en revision udføres af en tredjepartsrevisionstjeneste

c) anmode EU-enheden om at bringe styring, forvaltning og kontrol af cybersikkerhedsrisici i overensstemmelse med bestemmelserne i denne forordning, hvis det er relevant, på en nærmere præciseret måde og inden for en nærmere fastsat frist.

d) udstede en meddelelse til alle medlemsstater og EU-enheder med en henstilling om midlertidig suspension af datastrømme til EU-enheden.

3. Hvis IICB har vedtaget foranstaltninger i henhold til stk. 2, litra a) -d), giver den pågældende EU-enhed en detaljeret redegørelse for de foranstaltninger og tiltag, der er iværksat for at afhjælpe de påståede mangler, som IICB har konstateret. EU-enheden indsender denne redegørelse inden for en rimelig frist, der aftales med IICB.

4. Hvis IICB finder, at en EU-enhed vedvarende overtræder bestemmelserne i denne forordning som en direkte følge af en EU-tjenestemands eller anden EU-ansats handlinger eller undladelser, herunder i den øverste ledelse, anmoder IICB den pågældende enhed om at iværksætte passende tiltag, herunder af disciplinær karakter, i overensstemmelse med navnlig de regler, der er fastsat i vedtægten for tjenestemænd og ansættelsesvilkårene for Unionens øvrige ansatte. Med henblik herpå videregiver IICB de nødvendige oplysninger til den pågældende enhed.

Kapitel IV
CERT-EU

Artikel 12

CERT-EU's mission og opgaver

1. [...] [...] **CERT-EU's mission** er at bidrage til det uklassificerede IT-miljøs sikkerhed i alle EU[...] **-enheder** ved at rådgive dem om cybersikkerhed, hjælpe dem med at forebygge, detektere, afbøde og reagere på hændelser og fungere som deres knudepunkt for udveksling af oplysninger vedrørende cybersikkerhed og for koordinering af reaktionen på hændelser.

1a. CERT-EU indsamler, forvalter, analyserer og deler oplysninger med EU-enhederne om trusler, sårbarheder og hændelser vedrørende uklassificeret IKT-infrastruktur. Det koordinerer reaktionen i forbindelse med hændelser på interinstitutionelt niveau og på EU-enhedsniveau, herunder ved at yde eller koordinere ydelsen af specialiseret operationel bistand.

2. CERT-EU udfører følgende opgaver for EU[...]**-enhederne**:

a) støtter dem i forbindelse med gennemførelsen af denne forordning og bidrager til koordineringen af anvendelsen af denne forordning ved hjælp af **bestemmelserne** [...] i artikel 13, stk. 1, eller ved hjælp af ad hoc-rapporter, som IICB har bestilt

b) [...] **tilbyder standardiserede CSIRT-tjenester til alle EU-enheder i form** af en pakke af cybersikkerhedstjenester beskrevet i dets tjenestekatalog ("basistjenester")

c) vedligeholder et netværk af ligestillede og partnere til støtte for tjenesterne, jf. artikel 16 og 17

d) gør IICB opmærksom på spørgsmål, der vedrører gennemførelsen af denne forordning samt gennemførelsen af vejledende dokumenter, henstillinger og opfordringer til tiltag

e) [...] bidrager **på grundlag af oplysningerne i stk. 1a** til EU-cybersituationsbevidstheden **i tæt samarbejde med ENISA. Disse oplysninger deles med IICB samt CSIRT-netværket og EU-INTCEN**

f) fungerer som ækvivalent til den udpegede koordinator for EU-enhederne, jf. artikel 6 i direktiv [forslag til NIS 2].

[...]

[...]

[...]

[...]

[...]

4. **Inden for rammerne af sine beføjelser** indgår CERT-EU i et struktureret samarbejde med [...] **ENISA** om kapacitetsopbygning, operationelt samarbejde og langsigtede strategiske analyser af cybertrusler i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) 2019/881.

5. CERT-EU kan levere følgende tjenester, der ikke er beskrevet i dets tjenestekatalog ("betalingspligtige tjenester"):

   a) tjenester til støtte for cybersikkerheden i EU-[...]**enhedernes** IT-miljø ud over dem, der er beskrevet i stk. 2, i henhold til serviceleveranceaftaler og under forudsætning af, at der er ressourcer til rådighed

   b) tjenester til støtte for EU-[...]**enhedernes** cybersikkerhedsoperationer eller -projekter ud over dem, der beskytter deres IT-miljø, i henhold til skriftlige aftaler og under forudsætning af forudgående godkendelse fra IICB

   c) tjenester til støtte for IT-miljøers sikkerhed i andre organisationer end EU-[...] **enhederne**, som arbejder tæt sammen med EU[...]**-enhederne**, f.eks. fordi de er tildelt opgaver eller ansvarsområder i henhold til EU-retten, i henhold til skriftlige aftaler og under forudsætning af forudgående godkendelse fra IICB.

6. CERT-EU kan arrangere **eller deltage i** cybersikkerhedsøvelser eller opfordre til deltagelse i eksisterende øvelser, hvor det er relevant i tæt samarbejde med [...] **ENISA**, med henblik på at teste cybersikkerhedsniveauet i EU[...]**-enhederne**.

7. CERT-EU kan yde bistand til EU[...] **-enhederne** vedrørende hændelser i klassificerede IT-miljøer, hvis **de pågældende EU-enheder**[...] udtrykkeligt anmoder herom **i overensstemmelse med deres respektive procedurer. I så fald finder bestemmelserne i artikel 19-21 i denne forordning ikke anvendelse. Levering af bistand fra CERT-EU i henhold til dette stykke berører ikke gældende medlemsstats- eller EU-regler om beskyttelse af følsomme eller klassificerede informationer.**

8. CERT-EU underretter EU-enhederne om sine procedurer og processer for håndtering af hændelser.

9. CERT-EU kan overvåge EU-enhedernes nettrafik med den relevante EU-enheds samtykke.

10. CERT-EU kan, hvis EU-enhedernes politiske afdelinger udtrykkeligt anmoder herom, bidrage med teknisk rådgivning eller input om relevante politiske spørgsmål.

11. CERT-EU støtter i samarbejde med Den Europæiske Tilsynsførende for Databeskyttelse de pågældende EU-enheder ved håndtering af hændelser, der har ført til brud på persondatasikkerheden.

Artikel 13

Vejledende dokumenter, henstillinger og opfordringer til tiltag

1. CERT-EU støtter gennemførelsen af denne forordning ved at udstede:

   a) opfordringer til tiltag, der beskriver hastende sikkerhedsforanstaltninger, som EU[...]-enhederne kraftigt opfordres til at træffe inden for en fastsat frist. Efter modtagelse af opfordringen til tiltag underretter den pågældende EU-enhed uden unødig forsinkelse CERT-EU om, hvordan disse foranstaltninger blev anvendt

   b) forslag til IICB om vejledende dokumenter rettet til alle eller en delgruppe af EU[...]**-enheder**

   c) forslag til IICB om henstillinger rettet til individuelle EU-[...]**enheder**.

2. Vejledende dokumenter og henstillinger kan omfatte:

   a) metoder til eller forbedring af styringen af cybersikkerhedsrisici og **foranstaltningerne til styring af** cybersikkerhed**srisici**[...]

   b) metoder til brug i forbindelse med modenhedsvurderinger og cybersikkerhedsplaner og

   c) hvor det er passende, brugen af fælles teknologi, arkitektur og dertil knyttet bedste praksis med henblik på at opnå interoperabilitet og fælles standarder**, herunder en koordineret tilgang til forsyningskædesikkerhed** [...]**.**

[...]

[...]

Artikel 14

Chefen for CERT-EU

1. Kommissionen udpeger efter godkendelse fra to tredjedele af medlemmerne af IICB CERT-EU's chef. IICB høres i alle procedurens faser forud for udpegelsen af CERT-EU's chef, navnlig i forbindelse med udarbejdelse af stillingsopslag, behandling af ansøgninger og udpegelse af en udvælgelseskomité i forbindelse med denne stilling.

2. Chefen for CERT-EU er ansvarlig for, at CERT-EU fungerer korrekt og handler inden for rammerne af sit mandat under IICB's ledelse. Han eller hun er ansvarlig for at gennemføre den strategiske retning, de retningslinjer, mål og prioriteter, som IICB har fastsat, og for forvaltning af CERT-EU, herunder af dets finansielle og menneskelige ressourcer. Han eller hun aflægger regelmæssigt rapport til IICB's formand.

3. CERT-EU's chef bistår den ved delegation bemyndigede ansvarlige anvisningsberettigede i forbindelse med udarbejdelsen af den årsberetning, der indeholder oplysninger om finansielle og forvaltningsmæssige forhold, herunder kontrolresultater, og som udarbejdes i overensstemmelse med finansforordningens artikel 66, stk. 9, og aflægger regelmæssigt rapport til ham eller hende om gennemførelsen af foranstaltninger, for hvilke CERT-EU's chef har fået ovedraget beføjelser ved subdelegation.

4. CERT-EU's chef udarbejder årligt en finansiel planlægning af de administrative indtægter og udgifter i forbindelse med CERT-EU's aktiviteter, et forslag til det årlige arbejdsprogram, et forslag til CERT-EU's tjenestekatalog og revisionen heraf, et forslag om nærmere bestemmelser for serviceleveranceaftaler og et forslag om nøgleresultatindikatorer for CERT-EU, som IICB skal godkende i overensstemmelse med artikel 10.

Ved revision af listen over tjenester i CERT-EU's tjenestekatalog tager CERT-EU's chef hensyn til de ressourcer, som CERT-EU har fået tildelt.

5. Chefen for CERT-EU forelægger [...] **årlige** rapporter til IICB [...] om CERT-EU's resultater, finansielle planlægning, indtægter, gennemførelsen af budgettet, serviceleveranceaftaler og skriftlige aftaler, der er indgået, samarbejde med modparter og partnere samt tjenesterejser, som personalet har været på, herunder de rapporter, der er omhandlet i artikel 10, [...]**litra a)**.

Artikel 15

Finansielle og personalemæssige spørgsmål

[...]

1a. Selv om CERT-EU oprettes som en uafhængig interinstitutionel udbyder af tjenester til alle EU-enheder, skal det integreres i den administrative struktur i et af Kommissionens generaldirektorater for at udnytte Kommissionens støttestrukturer for administration, finansiel forvaltning og regnskab. Kommissionen underretter IICB om CERT-EU's administrative placering og alle ændringer heraf. Denne tilgang evalueres regelmæssigt og senest inden udløbet af en flerårig finansiel ramme, der er fastlagt i overensstemmelse med artikel 312 i TEUF, for at gøre det muligt at træffe passende foranstaltninger.

2. Med hensyn til anvendelsen af de administrative og finansielle procedurer handler CERT-EU's chef med referat til Kommissionen.

3. CERT-EU's opgaver og aktiviteter, herunder tjenester, som CERT-EU yder i henhold til artikel 12, stk. 2, [...] 4 og 6, og artikel 13, stk. 1, til EU[...]**-enhederne**, og som finansieres under det udgiftsområde i den flerårige finansielle ramme, der vedrører europæisk offentlig forvaltning, finansieres over en særlig budgetpost på Kommissionens budget. Stillinger, der er øremærket til CERT-EU, skal beskrives nærmere i en fodnote til Kommissionens stillingsfortegnelse.

4. Andre EU-[...]**enheder** end dem, der er omhandlet i stk. 3, yder et årligt finansielt bidrag til CERT-EU til dækning af de tjenester, som CERT-EU yder i henhold til stk. 3. De respektive bidrag baseres på retningslinjer, der er udstedt af IICB og aftalt mellem hver enhed og CERT-EU i en serviceleveranceaftale. Bidragene afspejler en retfærdig og proportionel andel af de samlede omkostninger ved de tjenester, der er ydet. De opføres på den særlige budgetpost, jf. stk. 3, som formålsbestemte indtægter, jf. artikel 21, stk. 3, litra c), i Europa-Parlamentets og Rådets forordning (EU, Euratom) 2018/1046[13].

5. Omkostningerne ved de opgaver, der er defineret i artikel 12, stk. 5, opkræves hos de EU-[...]**enheder**, der har gjort brug af CERT-EU's tjenester. Indtægterne opføres på de budgetposter, der vedrører omkostningerne.

[13] Europa-Parlamentets og Rådets forordning (EU, Euratom) 2018/1046 af 18. juli 2018 om de finansielle regler vedrørende Unionens almindelige budget, om ændring af forordning (EU) nr. 1296/2013, (EU) nr. 1301/2013, (EU) nr. 1303/2013, (EU) nr. 1304/2013, (EU) nr. 1309/2013, (EU) nr. 1316/2013, (EU) nr. 223/2014, (EU) nr. 283/2014 og afgørelse nr. 541/2014/EU og om ophævelse af forordning (EU, Euratom) nr. 966/2012 (EUT L 193 af 30.7.2018, s. 1).

Artikel 16

CERT-EU's samarbejde med medlemsstaternes modparter

1. CERT-EU samarbejder og udveksler **uden unødig forsinkelse** oplysninger med de nationale modparter i medlemsstaterne, **navnlig** [...] [...] [...] CSIRT'er**, jf. artikel 9 i direktiv [forslag til NIS 2]**, **og/eller såfremt relevant de nationale kompetente myndigheder** og centrale kontaktpunkter, jf. artikel 8 i direktiv [forslag til NIS 2], om cybertrusler, sårbarheder og hændelser, om eventuelle modforanstaltninger og om alle områder, der er relevante for at forbedre beskyttelsen af EU-[...]**enhedernes** IT-miljøer, herunder gennem det CSIRT-netværk, der er omhandlet i artikel 13 i direktiv [forslag til NIS 2].

1a. CERT-EU underretter straks alle relevante nationale modparter, jf. stk. 1, i en medlemsstat, når det får kendskab til væsentlige hændelser, der indtræffer på den pågældende medlemsstats område, medmindre CERT-EU har oplysninger om, at den berørte EU-enhed allerede har rapporteret om disse hændelser i overensstemmelse med artikel 20, stk. 2a.

2. CERT-EU **udveksler uden unødig forsinkelse** [...] hændelsesspecifikke oplysninger med nationale modparter i medlemsstaterne for at fremme detektionen af lignende cybertrusler eller hændelser **eller for at bidrage til analysen af en hændelse** uden **at skulle indhente** den berørte **EU-enheds** [...] samtykke. CERT-EU **må ikke** [...] udveksle hændelsesspecifikke oplysninger, der afslører identiteten på målet for cybersikkerhedshændelsen, **medmindre** [...]

a) den berørte EU-enhed har givet sit samtykke

b) den berørte EU-enhed allerede har offentliggjort, at den var berørt

c) offentliggørelsen af den berørte EU-enheds identitet i tilfælde, hvor der ikke foreligger samtykke fra den berørte EU-enhed, vil øge sandsynligheden for at undgå eller afbøde hændelser andre steder. Sådanne afgørelser kræver godkendelse fra chefen for CERT-EU. Den berørte EU-enhed underrettes inden offentliggørelsen.

Artikel 17

CERT-EU's samarbejde med [...] ***andre modparter***

1. CERT-EU må samarbejde med modparter [...] **i Den Europæiske Union undtagen dem, der er anført i artikel 16,** herunder branchespecifikke modparter, om værktøjer og metoder såsom teknikker, taktikker, procedurer og bedste praksis samt om cybertrusler og sårbarheder. CERT-EU indhenter med henblik på at indlede [...] samarbejde med sådanne modparter forudgående godkendelse fra IICB **i hvert enkelt tilfælde**. **Når CERT-EU etablerer et samarbejde med sådanne modparter, underretter CERT-EU alle relevante nationale modparter, jf. artikel 16, stk. 1, i den medlemsstat, hvor modparten befinder sig.**

2. CERT-EU må samarbejde med andre partnere såsom kommercielle enheder, internationale organisationer, nationale ikke-EU-enheder eller individuelle eksperter med henblik på at indsamle oplysninger om generelle og specifikke cybertrusler, sårbarheder og mulige modforanstaltninger. CERT-EU indhenter med henblik på at indlede et bredere samarbejde med sådanne partnere forudgående godkendelse fra IICB **i hvert enkelt tilfælde**.

3. CERT-EU må**, forudsat at der er indgået en hemmeligholdelsesaftale eller -kontrakt med den relevante partner,** med samtykke fra den **EU-enhed** [...], der er berørt af hændelsen, **udelukkende** udlevere oplysninger om den **specifikke** hændelse til **de i stk. 1 og 2 omhandlede partnere med henblik på at** [...] bidrage til analysen heraf. **Sådanne hemmeligholdelsesaftaler eller -kontrakter skal være juridisk bekræftet i overensstemmelse med Kommissionens relevante interne procedurer. Hemmeligholdelsesaftaler eller -kontrakter kræver ikke forudgående godkendelse fra IICB, men IICB's formand skal underrettes.**

4. **CERT-EU kan undtagelsesvis indgå serviceleveranceaftaler med andre enheder end EU-enhederne med forudgående godkendelse fra IICB.**

Kapitel V
SAMARBEJDE OG RAPPORTERINGSFORPLIGTELSER

Artikel 18

Håndtering af oplysninger

1. CERT-EU og EU[...]**-enhederne** skal overholde tavshedspligten i overensstemmelse med artikel 339 i traktaten om Den Europæiske Unions funktionsmåde eller tilsvarende gældende rammer.

2. Bestemmelserne i Europa-Parlamentets og Rådets forordning (EF) nr. 1049/2001[14] finder anvendelse på anmodninger om aktindsigt i dokumenter, som CERT-EU er i besiddelse af, herunder nævnte forordnings forpligtelse til at rådføre sig med andre EU-[...]**enheder, og såfremt relevant med medlemsstaterne,** når en anmodning vedrører deres dokumenter.

[...]

4. CERT-EU's og EU-[...]**enhedernes** håndtering af oplysninger sker i overensstemmelse med de **gældende** bestemmelser [...] om informationssikkerhed [...].

[...]

Artikel 19

[...] ***Deling af oplysninger vedrørende cybersikkerhed***

-1. EU-enhederne kan frivilligt give CERT-EU oplysninger om cybertrusler, hændelser, nærvedhændelser og sårbarheder, der berører dem. For at fremme delingen af oplysninger med EU-enhederne sikrer CERT-EU, at der er adgang til effektive kommunikationsmidler. CERT-EU kan prioritere behandling af obligatoriske underretninger frem for frivillige underretninger.

[14] Europa-Parlamentets og Rådets forordning (EF) nr. 1049/2001 af 30. maj 2001 om aktindsigt i Europa-Parlamentets, Rådets og Kommissionens dokumenter (EFT L 145 af 31.5.2001, s. 43).

1. CERT-EU kan **med henblik på at udføre sin mission og sine opgaver som omhandlet i artikel 12** [...] anmode EU[...]**-enhederne** om oplysninger fra deres respektive IT-systemfortegnelser**, herunder oplysninger vedrørende cybertrusler, nærvedhændelser, sårbarheder, kompromitteringsindikatorer, cybersikkerhedsadvarsler og henstillinger vedrørende konfiguration af cybersikkerhedsværktøjer til detektion af cyberhændelser** [...]. En EU-[...]**enhed**, der modtager en sådan anmodning, overfører de oplysninger, der anmodes om, samt eventuelle efterfølgende ajourføringer heraf uden unødig forsinkelse.

2. EU[...]**-enhederne** deler på CERT-EU's anmodning og uden unødig forsinkelse digitale oplysninger skabt ved brug af en elektronisk enhed, der har været involveret i deres respektive hændelser, med CERT-EU. CERT-EU kan præcisere yderligere, hvilke typer digitale oplysninger det har brug for i forbindelse med situationsbevidsthed og reaktion på hændelser.

3. CERT-EU må kun udveksle hændelsesspecifikke oplysninger **med EU-enhederne**, der afslører identiteten på den EU-[...]**enhed**, der er berørt af hændelsen, med denne enheds samtykke. **Hvis samtykke nægtes, skal den pågældende enhed forelægge CERT-EU behørigt begrundede årsager.** [...]

4. Delingsforpligtelsen gælder ikke EU's klassificerede informationer (EUCI) eller oplysninger**, hvis distribution til andre end den modtagende EU-enhed kilden har udelukket ved hjælp af en synlig markering, medmindre kilden til oplysningerne** [...] **udtrykkeligt tillader, at disse oplysninger deles med CERT-EU.** [...]

Artikel 20

[...] ***Rapporteringsforpligtelser***

-1. En hændelse anses for at være væsentlig, hvis:

a) den har forårsaget eller kan forårsage alvorlige operationelle forstyrrelser i EU-enhedens funktion eller økonomiske tab for den pågældende EU-enhed

b) den har påvirket eller kan påvirke andre fysiske eller juridiske personer ved at forårsage betydelig materiel eller immateriel skade.

1. Alle EU[...] **-enheder indsender**[...] **til CERT-EU:** [...]

[...].

a) uden unødig forsinkelse og under alle omstændigheder senest 24 timer efter at have fået kendskab til den væsentlige hændelse en tidlig varsling, som, hvor det er relevant, skal angive, om den væsentlige hændelse formodes at være forårsaget af ulovlige eller ondsindede handlinger og har eller kan få grænseoverskridende indvirkning

b) uden unødig forsinkelse og under alle omstændigheder senest 72 timer efter at have fået kendskab til den væsentlige hændelse en hændelsesunderretning, som, hvor det er relevant, ajourfører de oplysninger, der er omhandlet i litra a), og angiver en indledende vurdering af den væsentlige hændelse, dens alvor og indvirkning samt, hvis det er muligt, kompromitterings**indikatorerne**

c) efter anmodning fra CERT-EU en foreløbig rapport om relevante statusopdateringer

d) en endelig rapport senest en måned efter forelæggelsen af den i litra b) omhandlede underretning om den væsentlige hændelse, der som minimum omfatter følgende:

i) en detaljeret beskrivelse af den væsentlige hændelse, dens alvor og indvirkning

ii) den type trussel eller grundlæggende årsag, der sandsynligvis udløste den væsentlige hændelse

iii) anvendte og igangværende afbødende foranstaltninger

iv) hvor det er relevant, den grænseoverskridende indvirkning af den væsentlige hændelse

e) i tilfælde af igangværende væsentlige hændelser på tidspunktet for forelæggelsen af den i litra d) omhandlede endelige rapport en statusrapport på det pågældende tidspunkt og en endelig rapport senest en måned efter, at hændelsen er blevet håndteret.

[...]

g) [...]

h) [...]

i) [...]

j) [...]

2a. Alle EU-enheder deler inden for samme frist de oplysninger, der rapporteres i henhold til stk. 1, med alle relevante nationale modparter, jf. artikel 16, stk. 1, hvor den forefindes.

3. CERT-EU forelægger **hver tredje måned** en sammenfattende rapport for [...] **IICB, EU INTCEN og CSIRT-netværket,** der indeholder anonymiserede og aggregerede data om [...] cybertrusler, [...] sårbarheder **i henhold til artikel 19, EU-enhedernes svar på opfordringer til tiltag i henhold til artikel 13, stk. 1, litra (a),** og væsentlige hændelser, der er underrettet om i henhold til stk. 1. **Denne rapport udgør et bidrag til rapporten hvert andet år om cybersikkerhedssituationen i Unionen i henhold til artikel 15 i direktiv [forslag til NIS 2].**

4. IICB [...] udsteder **senest [6 måneder efter denne forordnings ikrafttræden]** vejledende dokumenter eller henstillinger **med nærmere præcisering af** [...] metoden **og formatet for** samt indholdet af **rapporteringen** [...]. **De vejledende dokumenter eller henstillingerne skal tage behørigt hensyn til de bestemmelser, der gennemføres ved gennemførelsesretsakter i henhold til artikel 20, stk. 11, i direktiv [forslag til NIS 2].** CERT-EU formidler de relevante tekniske detaljer for at gøre det muligt for EU[...]**-enhederne** at foretage proaktiv detektion, reagere på hændelser eller træffe afhjælpende foranstaltninger.

5. **Rapporterings**[...]forpligtelserne gælder ikke EUCI eller oplysninger**, hvis distribution til andre end den modtagende EU-enhed kilden har udelukket ved hjælp af en synlig markering, medmindre kilden til oplysningerne** [...] **udtrykkeligt tillader, at disse oplysninger deles med CERT-EU.** [...]

Artikel 21

Koordinering af og samarbejde om reaktionen på hændelser [...]

1. I sin funktion som knudepunkt for udveksling af oplysninger vedrørende cybersikkerhed og for koordinering af reaktionen på hændelser muliggør CERT-EU udvekslingen af oplysninger om cybertrusler, sårbarheder og hændelser mellem:

   a) EU[...]**enhederne**

   b) de i artikel 16 og 17 omhandlede modparter.

2. CERT-EU fremmer**,** [...] **hvor det er relevant i tæt samarbejde med ENISA i henhold til artikel 7, stk. 7, litra d) i forordningen om cybersikkerhed**[15]**,** koordineringen af reaktioner på hændelser mellem EU[...]**-enhederne**, herunder:

   a) bidrag til konsekvent ekstern kommunikation

   [...]

   c) optimal udnyttelse af operationelle ressourcer

   d) koordineringen med andre krisereaktionsmekanismer på EU-plan.

3. CERT-EU støtter **i tæt samarbejde med ENISA** EU-[...]**enhederne** i relation til situationsbevidsthed i forbindelse med cybertrusler, sårbarheder og hændelser.

---

15 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).

4. IICB **vedtager senest [12 måneder efter datoen for denne forordnings ikrafttræden] på grundlag af et forslag fra CERT-EU** [...] vejledende **dokumenter eller henstillinger** om koordinering af reaktionen på hændelser og samarbejde om væsentlige hændelser. Hvis der er mistanke om, at hændelsen er af strafferetlig karakter, rådgiver CERT-EU også om, hvordan de retshåndhævende myndigheder underrettes om hændelsen.

Artikel 22

Håndtering af større hændelser [...]

-1. For at støtte den koordinerede håndtering af større hændelser på operationelt plan, der berører EU-enheder, og for at bidrage til regelmæssig udveksling af relevante oplysninger mellem EU-enhederne og med medlemsstaterne udarbejder IICB, i tæt samarbejde med CERT-EU og ENISA, en cyberkrisestyringsplan baseret på de aktiviteter, der er beskrevet i artikel 21, stk. 2, og medtager som minimum følgende elementer:

a) metoder til koordinering og informationsstrøm mellem EU-enhederne med henblik på håndtering af større hændelser på operationelt plan

b) fælles operative standardprocedurer (SOP)

c) en fælles taksonomi for alvorsgraden af større hændelser og kriseudløsende faktorer

d) regelmæssige øvelser

e) sikre kommunikationskanaler, der skal anvendes

f) et kontaktpunkt for EU-CyCLONe, som deler relevante oplysninger med EU-CyCLONe som bidrag til fælles situationsbevidsthed.

1. CERT-EU koordinerer reaktioner på større **hændelser** [...] mellem EU[...]**-enhederne**. Det fører en fortegnelse over den tekniske ekspertise, der vil være brug for i forbindelse med en reaktion på **større hændelser**[...].

2. EU[...]**-enhederne** bidrager til denne fortegnelse over teknisk ekspertise i form af en årlig ajourført liste over eksperter, der er til rådighed i deres respektive organisationer, med nærmere oplysninger om deres specifikke tekniske færdigheder.

3. Efter specifik anmodning fra en medlemsstat, hvor den berørte EU-enhed er beliggende, og med [...] den **berørte** EU**-enheds** godkendelse [...], kan CERT-EU også trække på eksperterne på den liste, der er omhandlet i stk. 2, med henblik på at bidrage til reaktionen på en større **hændelse** [...] i [...] **den pågældende EU-enhed** [...]**.**

KAPITEL VI
AFSLUTTENDE BESTEMMELSER

Artikel 23

Oprindelig budgetomfordeling

Kommissionen foreslår en omfordeling af personale og finansielle ressourcer fra de relevante EU-[...]**enheder** til Kommissionens budget. Omfordelingen træder i kraft samtidig med det første budget, der vedtages efter denne forordnings ikrafttræden.

Artikel 24

Gennemgang

1. IICB bør med bistand fra CERT-EU regelmæssigt rapportere til Kommissionen om gennemførelsen af denne forordning. IICB kan også henstille til Kommissionen at **gennemgå** [...] denne forordning.

2. Kommissionen rapporterer til Europa-Parlamentet og Rådet om gennemførelsen af denne forordning senest **36** [...] måneder efter denne forordnings ikrafttræden og derefter hvert tredje år.

3. Kommissionen evaluerer denne forordnings funktion og rapporterer til Europa-Parlamentet, Rådet, Det Europæiske Økonomiske og Sociale Udvalg og Regionsudvalget herom **senest** [...] fem år efter datoen for dens ikrafttræden. **Rapporten ledsages om nødvendigt af et lovgivningsforslag.**

Artikel 25

Ikrafttræden

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

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

Udfærdiget i Bruxelles, den […].

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

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

BILAG II

[...]

[...]

[...]

[...]

[...]

[...]

[...]