Rådet for
Den Europæiske Union

Bruxelles, den 22. marts 2022
(OR. en)

7474/22

Interinstitutionel sag:
2022/0085(COD)

CYBER 93
TELECOM 116
JAI 383
INST 89
INF 32
CSC 119
CSCI 39
DATAPROTECT 81
FIN 353
BUDGET 2
CODEC 349
IA 30

FØLGESKRIVELSE

fra:	Martine DEPREZ, direktør, på vegne af generalsekretæren for Europa-Kommissionen
modtaget:	22. marts 2022
til:	Jeppe TRANHOLM-MIKKELSEN, generalsekretær for Rådet for Den Europæiske Union
Komm. dok. nr.:	COM(2022) 122 final
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

Hermed følger til delegationerne dokument COM(2022) 122 final.

Bilag: COM(2022) 122 final

EUROPA-
KOMMISSIONEN

Bruxelles, den 22.3.2022
COM(2022) 122 final

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

{SWD(2022) 67 final} - {SWD(2022) 68 final}

BEGRUNDELSE

1. BAGGRUND FOR FORSLAGET

• Forslagets begrundelse og formål

Ved dette forslag indføres en ramme til sikring af fælles cybersikkerhedsregler og -foranstaltninger i EU's institutioner, organer og agenturer. Formålet er at forbedre alle enheders modstandsdygtighed og beredskabskapacitet. Forslaget er i overensstemmelse med Kommissionens prioriteter om at gøre Europa klar til den digitale tidsalder og opbygge en fremtidssikret økonomi, der tjener alle. En sikker og modstandsdygtig offentlig forvaltning er en hjørnesten i den digitale omstilling af samfundet som helhed.

Dette forslag bygger på strategien for EU's sikkerhedsunion (COM(2020) 605 final) og EU's strategi for cybersikkerhed for det digitale årti (JOIN(2020) 18 final).

Forslaget moderniserer det eksisterende retsgrundlag for CERT-EU og tager de seneste års ændrede og øgede digitalisering af EU's institutioner, organer og agenturer i betragtning sammen med trusselsbilledet for cybersikkerheden, der udvikler sig løbende. Begge disse tendenser er blevet yderligere forstærket, siden covid-19-krisen satte ind, samtidig med at antallet af hændelser fortsat stiger, og der iværksættes stadig mere sofistikerede angreb fra en bred vifte af kilder.

Forslaget omdøber CERT-EU fra "IT-Beredskabsenheden" til "EU-institutionernes, -organernes og -agenturernes cybersikkerhedscenter" i overensstemmelse med udviklingen i medlemsstaterne og globalt, hvor mange CERT'er nu omdøbes til cybersikkerhedscentre. Dog bibeholdes kortformen "CERT-EU" under henvisning til genkendelsen af navnet.

• Sammenhæng med de gældende regler på samme område

Dette forslag har til formål at øge EU-institutionernes, -organernes og -agenturernes cybermodstandsdygtighed for så vidt angår cybertrusler og strømline med gældende lovgivning:

- Direktiv (EU) 2016/1148 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen. Nærværende forslag stemmer også overens med forslag til direktiv (EU) XXXX/XXXX om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen og om ophævelse af direktiv (EU) 2016/1148 [proposal NIS 2].
- Forordning (EU) 2019/881 om Den Europæiske Unions Agentur for Cybersikkerhed og om cybersikkerhedscertificering af informations- og kommunikationsteknologi (forordningen om cybersikkerhed).
- Forslag til forordning (EU) XXXX/XXXX om informationssikkerhed i EU's institutioner, organer, kontorer og agenturer.
- Kommissionens henstilling (EU) 2021/1086 af 23. juni 2021 om oprettelse af en fælles cyberenhed.
- Kommissionens henstilling (EU) 2017/1584 af 13. september 2017 om en koordineret reaktion på væsentlige cybersikkerhedshændelser og -kriser.

I bilaget til Kommissionens henstilling (EU) 2017/1584 af 13. september 2017 om en koordineret reaktion på væsentlige cybersikkerhedshændelser og -kriser fremlægges en plan

for en koordineret reaktion på væsentlige grænseoverskridende cybersikkerhedshændelser og -kriser.

I sine konklusioner af 9. marts 2021 understreger Rådet for Den Europæiske Union, "at cybersikkerhed (...) er afgørende for en velfungerende offentlig forvaltning (...) på både nationalt plan og EU-plan og for vores samfund og økonomi som helhed" og fremhæver "betydningen af en solid og konsekvent sikkerhedsramme til beskyttelse af al EU's personale, data, kommunikationsnet og informationssystemer samt beslutningsprocesser (...)". Dette bør navnlig ske ved at styrke modstandsdygtigheden og forbedre sikkerhedskulturen i EU's institutioner, organer og agenturer. Der skal stilles tilstrækkelige ressourcer og kapaciteter til rådighed, herunder i forbindelse med styrkelsen af CERT-EU's mandat.

2. RETSGRUNDLAG, NÆRHEDSPRINCIPPET OG PROPORTIONALITETSPRINCIPPET

- **Retsgrundlag**

Retsgrundlaget for denne forordning er artikel 298 i traktaten om Den Europæiske Unions funktionsmåde (TEUF), hvori det fastsættes, at Unionens institutioner, organer, kontorer og agenturer under udførelsen af deres opgaver støtter sig til en åben, effektiv og uafhængig europæisk forvaltning. Under overholdelse af den vedtægt og de ansættelsesvilkår, der er vedtaget på grundlag af artikel 336, fastsætter Europa-Parlamentet og Rådet ved forordning efter den almindelige lovgivningsprocedure bestemmelser med henblik herpå.

Informationsteknologi har gjort det muligt for EU's institutioner, organer og agenturer at arbejde og interagere med borgerne på nye måder samt forbedre den overordnede drift. I takt med at teknologien fortsat udvikles, udvikler trusselsbilledet for cybersikkerheden sig også. EU's institutioner, organer og agenturer er blevet meget attraktive mål for sofistikerede cyberangreb. Etableringen af systemer og krav til sikring af cybersikkerheden lader til at bidrage til den europæiske forvaltnings effektivitet og uafhængighed, således at EU's institutioner, organer, kontorer og agenturer kan fungere på en mere effektiv måde i en digital verden, når de udfører deres missioner.

Derudover udgør de nuværende forskelle i holdning og tilgang til cybersikkerhed i EU's institutioner, organer og agenturer en ekstra forhindring for opnåelsen af en åben, effektiv og uafhængig europæisk forvaltning, jf. afsnit 3 nedenfor. Uden en fælles tilgang vil holdingen til cybersikkerhed i EU's institutioner, organer og agenturer fortsat udvikle sig i forskellige retninger. Det valgte retsgrundlag er derfor det mest hensigtsmæssige, idet forordningen har til formål at oprette en fælles retlig ramme for cybersikkerhed i EU's institutioner, organer, kontorer og agenturer.

- **Nærhedsprincippet**

Forordningen om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i alle EU's institutioner, organer, kontorer og agenturer ligger inden for rammerne af EU's enekompetence.

- **Proportionalitetsprincippet**

Bestemmelserne i denne forordning går ikke videre, end hvad der er nødvendigt for at nå de specifikke mål på tilfredsstillende vis. De påtænkte foranstaltninger vil bidrage til opnåelsen af et højt fælles cybersikkerhedsniveau uden at gå ud over, hvad der er nødvendigt for at nå det tilstræbte mål i lyset af de stadig større risici, som de står over for.

- **Valg af retsakt**

Valget af en forordning, som finder direkte anvendelse, vurderes at være det mest hensigtsmæssige retlige instrument til at fastlægge og strømline de forpligtelser, som EU's institutioner, organer og agenturer pålægges. Med henblik på at give mulighed for målrettede forbedringer er en forordning også det mest hensigtsmæssige retlige instrument.

3. RESULTATER AF FORUDGÅENDE EVALUERINGER, HØRINGER AF INTERESSEREDE PARTER OG KONSEKVENSANALYSER

- **Forudgående evalueringer**

CERT-EU har foretaget en vurdering af de vigtigste cybertrusler, som EU's institutioner, organer og agenturer i øjeblikket udsættes for, eller som det er sandsynligt, at de vil blive udsat for i nær fremtid.

Analysen omhandler tre kategorier af observationer:

- Forsøg på brud på EU-institutionernes, -organernes og -agenturernes IT-infrastruktur (når det lykkes, behandles de som hændelser, i modsat fald registreres de som opdagede forsøg).
- Opdagede trusler i EU-institutionernes, -organernes og -agenturernes nærmiljø (f.eks. i relaterede sektorer, interessentgrupper eller i Europa).
- Større trusselstendenser observeret på globalt plan.

Derudover kiggede analysen på, hvordan igangværende større skift påvirker de måder, som EU's institutioner forvalter og anvender deres IT-infrastruktur og -tjenester på. Disse skift omfatter:

- øget telearbejde
- migrering af systemer til dataskyen
- øget udlicitering af IT-tjenester.

Fra 2019 til 2021 er antallet af væsentlige hændelser[1] i EU's institutioner, organer og agenturer, som er orkestreret af avancerede og vedholdende trusselsaktører, steget dramatisk. I første halvdel af 2021 var der således lige så mange væsentlige hændelser som i hele 2020. Dette afspejles også i det antal kriminaltekniske kopier (snapshots af indholdet af de berørte systemer eller anordninger), som CERT-EU analyserede i 2020, idet tallet er tredoblet sammenlignet med 2019 og tidoblet siden 2018.

I 2020 fastlagde CERT-EU's styrelsesråd et nyt strategisk mål for CERT-EU for at garantere et vidtfavnende cybersikkerhedsforsvar for alle EU's institutioner, organer og agenturer med en passende bredde og dybde og fortløbende tilpasning til eller hindring af nært forestående trusler, inkl. angreb på bærbare enheder, dataskymiljøer og IoT-enheder (Internet of Things).

Som supplement til CERT-EU's trusselanalyse har Kommissionen gennemført en evaluering af cybersikkerheden i 20 EU-institutioner, -organer og -agenturer. Evalueringen gav nyttig indsigt i etablerede cybersikkerhedspraksisser og kapacitetsforvaltning inden for cybersikkerhed, inkl. ekstern benchmarking af visse tekniske sikkerhedskontroller.

[1] "Væsentlig hændelse": enhver hændelse, medmindre den har en begrænset indvirkning og sandsynligvis allerede er velforstået med hensyn til metode eller teknologi.

Evalueringen var baseret på spørgeskemaer, som EU-institutioner, organer og agenturer svarede på, offentligt tilgængelige data og data leveret direkte af EU-institutionerne, -organerne og -agenturerne selv. Den giver tilstrækkelig indsigt i den nuværende situation til at konkludere følgende:

- Cybersikkerhedsmodenheden, størrelsen af IT-infrastrukturen og kapaciteten varierer betydeligt fra den ene evaluerede EU-institution, -organ eller -agentur til den anden.
- Selv om der generelt findes moden detektions- og reaktionskapacitet i mange af EU's institutioner, organer og agenturer, er der tale om varierende niveauer af integreret risikostyring i deres cybersikkerhedsforvaltningskapacitet.
- Selv om rammerne for cybersikkerheden (strategier, politikker og en regelbase) i de evaluerede EU-institutioner, -organer og -agenturer er veletablerede for så vidt angår de vigtigste cybersikkerhedsområder, jf. listen i bilag I i denne forordning, mangler visse EU-institutioner, -organer og -agenturer moden kapacitet til styring af driftskontinuitet, overholdelse, audit og fortsatte forbedringer.
- Tekniske foranstaltninger, der kan betegnes som god praksis, blev ikke fundet anvendt konsekvent af de evaluerede EU-institutioner, -organer og -agenturer.

Kort sagt viser analysen af de 20 EU-institutioner, -organer og -agenturer, at deres forvaltning, cyberhygiejne, overordnede kapacitet og modenhed varierer på tværs af et bredt spektrum, og at et krav om, at alle EU-institutioner, -organer og -agenturer gennemfører et minimum af cybersikkerhedsforanstaltninger vil bidrage til at reducere forskellene i modenhed og bringe alle EU-institutioner, -organer og -agenturer op på et højt fælles cybersikkerhedsniveau.

Til dato har ingen EU-lovgivning haft fokus på cybersikkerhed i EU's institutioner, organer og agenturer eller alsidigt beskæftiget sig med trusselsbilledet for cybersikkerheden og de nye IT-risici, der opstår som følge af digitaliseringen.

- **Høringer af interesserede parter**

Kommissionen har hørt interessenter på tværs af EU's institutioner, organer og agenturer samt repræsentanter for medlemsstaterne i Rådet og interessenterne i Europa-Parlamentet. Den 25. juni 2021 deltog repræsentanter for medlemsstaterne og berørte interessenter fra EU's institutioner, organer og agenturer i en workshop arrangeret af Kommissionen med henblik på at drøfte indholdet af det fremtidige forslag til forordning.

- **Konsekvensanalyse**

Dette forslag får konsekvenser for EU's institutioner, organer og agenturer. Det er derfor ikke nødvendigt at udarbejde en specifik konsekvensanalyse, eftersom det ikke finder anvender på medlemsstaterne.

- **Grundlæggende rettigheder**

EU har forpligtet sig at sikre et højt niveau af beskyttelse af de grundlæggende rettigheder. Al deling af oplysninger inden for rammerne af denne forordning vil blive gennemført i sikre miljøer under fuld overholdelse af retten til beskyttelse af personoplysninger, jf. artikel 8 i Den Europæiske Unions charter om grundlæggende rettigheder, og den relevante databeskyttelseslovgivning, især Europa-Parlamentets og Rådets forordning (EU) 2018/1725.

4. VIRKNINGER FOR BUDGETTET

Markedsbenchmark og undersøgelser[2] viser, at andelen af direkte udgifter til cybersikkerhed indtil nu har ligget på mellem 4 og 7 % af de samlede IT-udgifter i en organisation. Den trusselsanalyse, som CERT-EU har udarbejdet til støtte for dette lovgivningsforslag, indikerer imidlertid, at internationale organer og politiske organisationer står over for øgede risici, og at en andel på 10 % til IT-udgifter til cybersikkerhed lader til at være et mere passende mål. De præcise omkostninger ved en sådan indsats kan ikke fastslås som følge af manglen på detaljerede oplysninger om IT-udgifterne i EU's institutioner, organer og agenturer og den relevante andel af udgifterne til cybersikkerhed.

Selv om det således er sandsynligt, at mange af EU's institutioner, organer og agenturer bruger mindre på cybersikkerhed, end de burde, vil denne forordning ikke som sådan føre til en stigning i de nuværende udgifter. Selv uden denne forordning ville hver enhed skulle sikre et passende cybersikkerhedsniveau. Forordningen viderefører det tidligere samarbejde i CERT-EU's styrelsesråd og formaliserer et lag udveksling af oplysninger, der allerede delvist eksisterer i dag. Som det fremgår af finansieringsoversigten, vil CERT-EU få brug for yderligere ressourcer til at kunne udfylde sin udvidede rolle, og disse ressourcer bør omfordeles fra de EU-institutioner, -organer og -agenturer, der nyder gavn af CERT-EU's tjenester.

5. ANDRE FORHOLD

- **Gennemførelse og foranstaltninger til overvågning, evaluering og rapportering**

Det Interinstitutionelle Råd for Cybersikkerhed (IICB) bør med bistand fra CERT-EU gennemgå denne forordnings funktion, udarbejde evalueringer og fremlægge en rapport til Kommissionen herom. Kommissionen bør sikre regelmæssig rapportering til Europa-Parlamentet, Rådet, Det Europæiske Økonomiske og Sociale Udvalg og Regionsudvalget.

CERT-EU kan udarbejde et forslag til et vejledende dokument eller en henstilling, som IICB kan vælge at vedtage. Et vejledende dokument er en meddelelse rettet til alle eller en delgruppe af EU's institutioner, organer og agenturer, mens en henstilling er rettet til EU-enkeltinstitutioner, -organer eller -agenturer. En opfordring til tiltag er en CERT-EU-meddelelse, der beskriver hastende sikkerhedsforanstaltninger, som EU's institutioner, organer og agenturer kraftigt opfordres til at træffe inden en fastsat frist.

- **Nærmere redegørelse for de enkelte bestemmelser i forslaget**

Generelle bestemmelser

Ved denne forordning fastsættes foranstaltninger med henblik på at sikre et højt fælles cybersikkerhedsniveau, og den finder anvendelse på alle EU's institutioner, organer og agenturer med henblik på at sætte dem i stand til at gennemføre deres respektive missioner på en åben, effektiv og uafhængig måde (artikel 1-3 og 23-25).

Foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau

EU's institutioner, organer og agenturer er forpligtede til at etablere en intern ramme for styring, forvaltning og kontrol af cybersikkerhedsrisici, som sikrer en effektiv og fornuftig

[2] Kilde: Gartner, "Identifying the Real Information Security Budget" (2016). Dette er i tillæg til indirekte udgifter til IT-sikkerhed såsom til netværkssikkerhed som f.eks. firewalls, antivirus og systemejeransvar, risikovurdering og gennemførelse af sikkerhedskontroller. I et papir fra 2020 vurderes det, at udgifterne til cybersikkerhed i finansielle institutioner ligger på 10-11 % af IT-udgifterne (kilde: DI_2020-FS-ISAC-Cybersecurity.pdf (deloitte.com)).

styring af alle cybersikkerhedsrisici. EU's institutioner, organer og agenturer skal desuden vedtage et referencescenarie for cybersikkerhed med henblik på at håndtere de risici, der konstateres i medfør af denne ramme, gennemføre regelmæssige vurderinger af cybersikkerhedsmodenheden og vedtage en cybersikkerhedsplan (artikel 4-8).

Det Interinstitutionelle Råd for Cybersikkerhed

Det Interinstitutionelle Råd for Cybersikkerhed etableres og skal være ansvarlig for overvågningen af EU-institutionernes, -organernes og agenturernes gennemførelse af denne forordning samt overvågningen af CERT-EU's gennemførelse af de generelle prioriteter og mål samt udstikke den strategiske retning for CERT-EU (artikel 9-11).

CERT-EU

CERT-EU skal bidrage til IT-miljøets sikkerhed i alle EU's institutioner, organer og agenturer ved at rådgive dem, hjælpe dem med at forebygge, detektere, afbøde og reagere på hændelser og ved at fungere som deres knudepunkt for udveksling af oplysninger vedrørende cybersikkerhed og koordinering af beredskabet i forbindelse med hændelser (artikel 12-17).

Samarbejde og rapporteringsforpligtelser

Forordningen sikrer samarbejde og udveksling af oplysninger i CERT-EU og EU's institutioner, organer og agenturer med henblik på at skabe tillid. Med henblik herpå kan CERT-EU anmode EU's institutioner, organer og agenturer om at forsyne det med relevante oplysninger, og CERT-EU må, uden den berørte deltagers samtykke, udveksle hændelsesspecifikke oplysninger med EU's institutioner, organer og agenturer for at fremme detektionen af lignende cybertrusler eller hændelser. CERT-EU må dog kun udveksle hændelsesspecifikke oplysninger, der afslører identiteten på målet for en cybersikkerhedshændelse med den berørte deltagers samtykke.

Alle EU's institutioner, organer og agenturer skal navnlig underrette CERT-EU om væsentlige cybertrusler, væsentlige sårbarheder og væsentlige hændelser uden unødig forsinkelse og senest 24 timer efter, at de er blevet opmærksom på dem (artikel 18-22).

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, 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's institutioner, organer og agenturer 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-institutionernes, -organernes og -agenturernes 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-institution, ét EU-organ eller ét EU-agentur, kan have kaskadevirkninger mere generelt, hvilket potentielt kan føre til vidtrækkende og langvarige negative virkninger for de andre. Derudover er visse institutioners, organers og agenturers 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.

(4) EU's institutioner, organer og agenturer er attraktive mål, der står over for højt kvalificerede trusselsaktører med adgang til mange ressourcer samt andre trusler. Men cybermodstandsdygtighedsgraden og -modenheden 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's institutioner, organer og agenturer opnår et højt fælles cybersikkerhedsniveau ved hjælp af referencescenarie for cybersikkerhed (et sæt minimumsregler, som net- og informationssystemer samt operatører og brugere heraf skal overholde med henblik på at minimere cybersikkerhedsrisiciene), udveksling af oplysninger og samarbejde.

(5) Direktivet [proposal 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's institutioner, organer og agenturer følger trop ved at sikre regler, der er strømlinet med direktiv [proposal NIS 2] og afspejler dets ambitionsniveau.

(6) For at opnå et højt fælles cybersikkerhedsniveau er det nødvendigt, at hver EU-institution, -organ og -agentur etablerer en intern ramme for styring, forvaltning og kontrol af cybersikkerhedsrisici, som sikrer en effektiv og fornuftig styring af alle cybersikkerhedsrisici og tager hensyn til driftskontinuitet og krisestyring.

(7) EU's institutioner, organer og agenturer er forskellige, og det er derfor nødvendigt, at gennemførelsen er fleksibel, 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-institutionernes, -organernes og -agenturernes missioner eller deres institutionelle autonomi. EU's institutioner, organer og agenturer bør derfor etablere deres egne rammer for styring, forvaltning og kontrol af cybersikkerhedsrisici og vedtage deres egne referencescenarier og cybersikkerhedsplaner.

(8) Med henblik på at undgå at EU's institutioner, organer og agenturer 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-institution, -organ og -agentur bør sigte på at tildele en passende procentdel af deres IT-budget til forbedring af cybersikkerhedsniveauet. På længere sigt bør de forfølge et mål på omkring 10 %.

(9) Et højt fælles cybersikkerhedsniveau kræver, at cybersikkerhed bliver lagt ind under hver EU-institutions, -organs og -agenturs øverste ledelses tilsyn, idet den øverste ledelse bør vedtage et referencescenarie for cybersikkerhed med henblik på at imødegå de risici, der er konstateret i henhold til den ramme, som etableres af hver EU-institution og hvert EU-organ og -agentur. Cybersikkerhedskulturen, dvs. den daglige praksis for cybersikkerhed, bør være en integreret del af et referencescenarie for cybersikkerhed i alle EU-institutioner, -organer og -agenturer.

(10) EU's institutioner, organer og agenturer bør vurdere risici vedrørende forholdet til leverandører og tjenesteudbydere, herunder leverandører af datalagrings- og databehandlingstjenester eller administrerede sikkerhedstjenester, og træffe foranstaltninger til at håndtere dem. Disse foranstaltninger bør være en del af referencescenariet for cybersikkerhed og specificeres nærmere i vejledende dokumenter eller henstillinger udstedt af CERT-EU. Når der udarbejdes foranstaltninger og vejledninger, bør der tages behørigt højde for den relevante EU-

lovgivning og de relevante EU-politikker, herunder risikovurderinger og henstillinger udstedt af NIS-samarbejdsgruppen, såsom de koordinerede EU-risikovurderinger og EU-værktøjskassen om 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.

(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[3]. Denne ordning bør fortsat udvikles med henblik på at understøtte gennemførelsen af denne forordning.

(12) CERT-EU bør omdøbes fra "IT-Beredskabsenheden" til "EU-institutionernes, -organernes og -agenturernes cybersikkerhedscenter" i overensstemmelse med udviklingen i medlemsstaterne og globalt, hvor mange CERT'er omdøbes til cybersikkerhedscentre, men kortformen "CERT-EU" bør bibeholdes under henvisning til genkendelsen af navnet.

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

(14) Udover at give CERT-EU flere opgaver og udvide dets rolle bør der oprettes et interinstitutionelt råd for cybersikkerhed (IICB), der skal fremme et højt fælles cybersikkerhedsniveau i alle EU's institutioner, organer og agenturer ved at overvåge EU-institutionernes, -organernes og -agenturernes gennemførelse af denne forordning og CERT-EU's gennemførelse af de generelle prioriteter og mål samt udstikke den strategiske retning for CERT-EU. IICB bør sikre, at EU's institutioner er repræsenteret og inddrage EU's agenturer og organer gennem EU-agenturernes netværk.

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

(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's institutioner, organer og agenturer kraftigt opfordres til at træffe inden en fastsat frist.

(16) IICB bør overvåge overholdelsen af denne forordning og opfølgningen på vejledende dokumenter, henstillinger og opfordringer til tiltag udstedt af CERT-EU. 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's institutioner, organer og agenturer og andre interessenter efter behov. Når det er nødvendigt, bør IICB udstede ikkebindende advarsler og anbefale revisioner.

(17) CERT-EU bør have som mission at bidrage til IT-miljøets sikkerhed i alle EU's institutioner, organer og agenturer. CERT-EU bør agere som ækvivalent til EU's institutioner, organer og agenturer med henblik på koordineret offentliggørelse af sårbarheder for så vidt angår det europæiske sårbarhedsregister, jf. artikel 6 i direktiv [proposal NIS 2].

(18) I 2020 fastlagde CERT-EU's styrelsesråd et nyt strategisk mål for CERT-EU med henblik på at garantere et vidtfavnende cybersikkerhedsforsvar for alle EU's institutioner, organer og agenturer med en passende bredde og dybde og fortløbende tilpasning til eller hindring af overhængende trusler, inkl. angreb på bærbare enheder, dataskymiljøer og IoT-enheder (Internet of Things). Strategien omfatter også bredspektrede sikkerhedsoperationscentre (SOC'er), der overvåger netværk, samt 24/7-overvågning af meget alvorlige trusler. Hvad angår de større EU-institutioner, -organer og -agenturer bør CERT-EU støtte deres IT-sikkerhedsenheder, herunder med 24/7-frontlinjeovervågning. Hvad angår mindre og visse mellemstore EU-institutioner, -organer og -agenturer bør CERT-EU yde alle tjenester.

(19) CERT-EU bør også udfylde den rolle, der er fastsat i direktiv [proposal 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[4] bør CERT-EU samarbejde og koordinere om 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.

(20) I forbindelse med støtte til den operationelle cybersikkerhed bør CERT-EU gøre brug af Den Europæiske Unions Agentur for Cybersikkerheds tilgængelige ekspertise i form af et struktureret samarbejde, jf. Europa-Parlamentets og Rådets forordning (EU) 2019/881[5]. 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 Den

[4] 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] 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).

Europæiske Unions Agentur for Cybersikkerhed om trusselsanalyser og regelmæssigt dele sin rapport om trusselsbilledet med agenturet.

(21) Som støtte for den fælles cyberenhed, der er oprettet i medfør af Kommissionens henstilling af 23. juni 2021[6], bør CERT-EU samarbejde og udveksle oplysninger med interessenterne med henblik på at fremme operationelt samarbejde og for at gøre det muligt for de eksisterende netværk at realisere deres fulde potentiale i forbindelse med beskyttelsen af EU.

(22) Alle personoplysninger, der behandles i henhold til denne forordning, bør behandles i overensstemmelse med databeskyttelseslovgivningen, herunder Europa-Parlamentets og Rådets forordning (EU) 2018/1725[7].

(23) CERT-EU's og EU-institutionernes, -organernes og -agenturernes håndtering af data bør ske i overensstemmelse med bestemmelserne i forordning [proposed Regulation on information security]. For at sikre koordinering af sikkerhedsspørgsmål bør alle kontakter med CERT-EU, som indledes eller efterspørges af nationale sikkerheds- og efterretningstjenester, uden unødig forsinkelse kommunikeres til Kommissionens Direktorat for Sikkerhed og formanden for IICB.

(24) Eftersom CERT-EU's tjenester og opgaver er i alle EU-institutioners, -organers og -agenturers interesse, bør hver EU-institution, -organ og -agentur, der afholder udgifter til IT, bidrage med en retfærdig andel til CERT-EU's tjenester og opgaver. Disse bidrag berører ikke EU-institutionernes, -organernes og -agenturernes budgetautonomi.

(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 —

VEDTAGET DENNE FORORDNING:

Kapitel I
ALMINDELIGE BESTEMMELSER

Artikel 1
Genstand

Ved denne forordning fastsættes:

(a) forpligtelser for EU's institutioner, organer og agenturer om indførelse af en intern ramme for styring, forvaltning og kontrol af cybersikkerhedsrisici

(b) forpligtelser for EU's institutioner, organer og agenturer med hensyn til risikostyring og rapportering i forbindelse med cybersikkerhed

---

6 Kommissionens henstilling (EU) 2021/1086 af 23. juni 2021 om oprettelse af en fælles cyberenhed (EUT L 237 af 5.7.2021, s. 1).

7 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).

(c) bestemmelser om organiseringen og driften af EU-institutionernes, -organernes og -agenturernes Cybersikkerhedscenter (CERT-EU) og om organiseringen og driften af Det Interinstitutionelle Råd for Cybersikkerhed.

Artikel 2
Anvendelsesområde

Denne forordning finder anvendelse på alle EU's institutioners, organers og agenturers ramme for styring, forvaltning og kontrol af cybersikkerhedsrisici og på organiseringen og driften af CERT-EU og Det Interinstitutionelle Råd for Cybersikkerhed.

Artikel 3
Definitioner

I denne forordning forstås ved:

(1) "EU's institutioner, organer og agenturer": EU-institutioner, -organer 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 omhandlet i artikel 4, nr. 1), i direktiv [proposal NIS 2]

(3) "sikkerhed i net- og informationssystemer": sikkerhed i net- og informationssystemer som omhandlet i artikel 4, nr. 2), i direktiv [proposal NIS 2]

(4) "cybersikkerhed": cybersikkerhed som omhandlet i artikel 4, nr. 3), i direktiv [proposal NIS 2]

(5) "øverste ledelse": leder, ledelse eller koordinerings- eller tilsynsorgan på højeste administrative niveau under hensyntagen til ledelsesordningerne på højt niveau i hver EU-institution, -organ eller -agentur

(6) "hændelse": en hændelse som omhandlet i artikel 4, nr. 5), i direktiv [proposal NIS 2]

(7) "væsentlig hændelse": enhver hændelse, medmindre den har en begrænset indvirkning og sandsynligvis allerede er velforstået med hensyn til metode eller teknologi

(8) "større angreb": enhver hændelse, der kræver flere ressourcer end de, der er tilgængelige i de berørte EU-institutioner, -organer eller -agenturer og i CERT-EU

(9) "håndtering af hændelser": håndtering af hændelser som omhandlet i artikel 4, nr. 6), i direktiv [proposal NIS 2]

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

(11) "væsentlig cybertrussel": en cybertrussel, der har til hensigt, mulighed og evne til at forårsage en væsentlig hændelse

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

(13) "væsentlig sårbarhed": en sårbarhed, der sandsynligvis vil føre til en væsentlig hændelse, hvis den udnyttes

(14) "cybersikkerhedsrisiko": enhver rimeligt identificerbar omstændighed eller begivenhed, der har en potentiel negativ indvirkning på sikkerheden i net- og informationssystemer

(15) "fælles cyberenhed": en virtuel og fysisk samarbejdsplatform for de forskellige cybersikkerhedsfællesskaber i EU med fokus på operationel og teknisk koordinering til imødegåelse af større grænseoverskridende cybertrusler og hændelser som omhandlet i Kommissionens henstilling af 23. juni 2021

(16) "referencescenarie for cybersikkerhed": et sæt minimumsregler i forbindelse med cybersikkerhed, som net- og informationssystemer samt operatører og brugere heraf skal overholde med henblik på at minimere cybersikkerhedsrisiciene.

Kapitel II
FORANSTALTNINGER TIL SIKRING AF ET HØJT FÆLLES CYBERSIKKERHEDSNIVEAU

Artikel 4
Styring, forvaltning og kontrol af risici

1. Hver EU-institution, -organ og -agentur etablerer sin egen interne ramme for styring, forvaltning og kontrol af cybersikkerhedsrisici ("rammen") til støtte for enhedens opgaver og udøvelsen af dens institutionelle autonomi. For at sikre en effektiv og fornuftig styring af alle cybersikkerhedsrisici, fører enhedens øverste ledelse tilsyn hermed. Rammen indføres senest .... [15 months after the entry into force of this Regulation].

2. Rammen skal dække hele den berørte institutions, organs eller agenturs IT-miljø, inkl. lokale IT-miljøer, udliciterede aktiver og tjenester i cloud computing-miljøer 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 tager hensyn til driftskontinuitet og krisestyring og tager højde for forsyningssikkerhed og styring af menneskelige risici, der kan have indvirkning på cybersikkerheden i den berørte EU-institution, -organ eller -agentur.

3. Den øverste ledelse i hver EU-institution, -organ og -agentur fører tilsyn med deres organisations overholdelse af de forpligtelser, der vedrører styring, forvaltning og kontrol af cybersikkerhedsrisici uden at dette berører det formelle ansvar for overholdelse og risikostyring, der er pålagt lederne andre steder i organisationen i relation til deres respektive ansvarsområder.

4. Hver EU-institution, -organ og -agentur indfører effektive mekanismer til sikring af, at en passende procentdel af IT-budgettet bruges på cybersikkerhed.

5. Hver EU-institution, -organ og -agentur udpeger en lokal cybersikkerhedsansvarlig eller en ækvivalent funktion, der fungerer som det centrale kontaktpunkt vedrørende alle aspekter af cybersikkerhed.

Artikel 5
Referencescenarie for cybersikkerhed

1. Den øverste ledelse i hver EU-institution, -organ og -agentur godkender sin enheds referencescenarie for cybersikkerhed med henblik på at imødegå de risici, der konstateres inden for den i artikel 4, stk. 1, omhandlede ramme. Dette gøres med det

formål at støtte enhedens opgaver og udøvelsen af dens institutionelle autonomi. Referencescenariet for cybersikkerhed forelægges senest .... [18 months after the entry into force of this Regulation] og dækker de områder, der er opført i bilag I, og de foranstaltninger, der er opført i bilag II.

2. Topledelsen i hver EU-institution, -organ eller -agentur følger regelmæssigt specifikke kurser for at tilegne sig tilstrækkelig viden og færdigheder til at forstå og vurdere cybersikkerhedsrisici og cybersikkerhedsstyringspraksisser samt disses indvirkning på enheden.

Artikel 6
Modenhedsvurderinger

Hver EU-institution, -organ og -agentur udarbejder mindst hvert tredje år en modenhedsvurdering vedrørende cybersikkerhed, der indarbejder alle elementerne af deres IT-miljø som beskrevet i artikel 4 under hensyntagen til de relevante vejledende dokumenter og henstillinger vedtaget i overensstemmelse med artikel 13.

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-institution, -organ og -agentur, uden unødig forsinkelse og efter etableringen af rammen for styring, forvaltning og kontrol af cybersikkerhedsrisici samt referencescenariet for cybersikkerhed, en cybersikkerhedsplan. Planen skal sigte på at øge den pågældende enheds overordnede cybersikkerhed og derved bidrage til opnåelsen eller forbedringen af et højt fælles cybersikkerhedsniveau i alle EU's institutioner, -organer og -agenturer. Med det formål at støtte enhedens opgaver og udøvelsen af dens institutionelle autonomi omfatter planen som minimum de områder, der er opført i bilag I, de foranstaltninger, der er opført i bilag II, samt foranstaltninger vedrørende beredskab, reaktion og genopretning i forbindelse med hændelser såsom sikkerhedsmonitorering og logning. Planen revideres mindst hvert tredje år med baggrund i de modenhedsvurderinger, der udarbejdes i medfør af artikel 6.

2. Cybersikkerhedsplanen omfatter personalets roller og ansvarsfordeling i relation til gennemførelse af den.

3. Cybersikkerhedsplanen tager hensyn til alle relevante vejledende dokumenter og henstillinger som udstedt af CERT-EU.

Artikel 8
Gennemførelse

1. EU's institutioner, organer og agenturer fremsender deres modenhedsvurderinger til Det Interinstitutionelle Råd for Cybersikkerhed, når disse er afsluttet. EU's institutioner, organer og agenturer underretter Det Interinstitutionelle Råd for Cybersikkerhed, når de har udarbejdet en sikkerhedsplan. På Rådets anmodning rapporterer de om specifikke aspekter af gennemførelsen af dette kapitel.

2. Vejledende dokumenter og henstillinger, der er udstedt i overensstemmelse med artikel 13, understøtter gennemførelsen af bestemmelserne i 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's institutioners, organers og agenturers gennemførelse af denne forordning

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

3. IICB sammensættes af tre repræsentanter for 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, samt én repræsentant fra hver af følgende:

   (a) Europa-Parlamentet

   (b) Rådet for Den Europæiske Union

   (c) Europa-Kommissionen

   (d) Den Europæiske Unions Domstol

   (e) Den Europæiske Centralbank

   (f) Den Europæiske Revisionsret

   (g) Tjenesten for EU's Optræden Udadtil

   (h) Det Europæiske Økonomiske og Sociale Udvalg

   (i) Det Europæiske Regionsudvalg

   (j) Den Europæiske Investeringsbank

   (k) Den Europæiske Unions Agentur for Cybersikkerhed.

   Medlemmerne kan bistås af en suppleant. Formanden kan invitere andre repræsentanter for de enheder, der er angivet ovenfor, eller EU's institutioner, organer og agenturer 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 fire år. Dennes suppleant bliver fuldgyldigt medlem af IICB i samme periode.

6. IICB mødes på formandens initiativ, efter anmodning fra CERT-EU 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, eller dennes suppleant, deltager i IICB's møder, medmindre andet besluttes af IICB.

10. Kommissionen varetager IICB's sekretariatsopgaver.

11. Repræsentanterne for EUAN, som udpeget efter forslag fra netværkets rådgivende IKT-udvalg, formidler IICB's afgørelser til EU's agenturer og fællesforetagender. 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. IICB kan anvende forenklet skriftlig procedure, som indledes af formanden, i henhold til hvilken den relevante afgørelse anses for godkendt inden for den tidsfrist, som formanden har fastsat, medmindre et medlem gør indsigelse.

13. IICB kan udpege et forretningsudvalg til at bistå IICB i dets arbejde og delegere nogle af sine opgaver og beføjelser til samme. IICB fastsætter forretningsudvalgets forretningsorden, inkl. dets opgaver og beføjelser, og dets medlemmers mandatperiode.

Artikel 10
IICB's opgaver

Når det udfører sine forpligtelser, skal IICB navnlig:

(a) gennemgå de rapporter om status for EU-institutionernes, -organernes og -agenturernes gennemførelse af denne forordning, der er bestilt hos CERT-EU

(b) på grundlag af et forslag fra 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

(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, serviceleveranceaftaler eller kontrakter mellem CERT-EU og andre enheder, der indgås i medfør af artikel 17

(i) nedsætte så mange tekniske rådgivende grupper til at bistå IICB i dets arbejde, som der er behov for, godkende disses mandat og udpege de respektive formænd.

Artikel 11
Overholdelse

IICB overvåger EU's institutioners, organers og agenturers gennemførelse af denne forordning, de vejledende dokumenter, henstillinger og opfordringer til tiltag. Hvis IICB

finder, at en EU-institution, -organ eller -agentur ikke effektivt har anvendt eller gennemført denne forordning, vejledende dokumenter, henstillinger eller opfordringer til tiltag, der er udstedt i medfør af denne forordning, kan IICB, uden at dette berører den pågældende EU-institutions, -organs eller -agenturs interne procedurer:

(a) udstede en advarsel; om nødvendigt og i lyset af en markant cybersikkerhedsrisiko begrænses gruppen af modtagere af en sådan advarsel på behørig vis

(b) opfordre den relevante revisionstjeneste til at gennemføre en revision.

Kapitel IV
CERT-EU

Artikel 12
CERT-EU's mission og opgaver

1. CERT-EU er det uafhængige interinstitutionelle cybersikkerhedscenter for alle EU's institutioner, organer og agenturer, hvis mission er at bidrage til det uklassificerede IT-miljøs sikkerhed i alle EU's institutioner, organer og agenturer 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 beredskabet i forbindelse med hændelser.

2. CERT-EU udfører følgende opgaver for EU's institutioner, organer og agenturer:

   (a) støtter dem i forbindelse med gennemførelsen af denne forordning og bidrager til koordineringen af anvendelsen af denne forordning ved hjælp af de foranstaltninger, der er opført i artikel 13, stk. 1, eller ved hjælp af ad hoc-rapporter, som IICB har bestilt

   (b) støtter dem ved hjælp af en pakke af cybersikkerhedstjenester beskrevet i dets servicekatalog ("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) rapporterer om de cybertrusler, som EU's institutioner, organer og agenturer står over for, og bidrager til EU-cybersituationsbevidstheden.

3. CERT-EU bidrager til den fælles cyberenhed, der er oprettet i medfør af Kommissionens henstilling af 23. juni 2021, bl.a. på følgende områder:

   (a) beredskab og koordinering i forbindelse med hændelser, udveksling af oplysninger og krisebredskab på teknisk plan i forbindelse med sager, der har tilknytning til EU's institutioner, organer og agenturer

   (b) operationelt samarbejde i forbindelse med netværket af enheder, der håndterer IT-sikkerhedshændelser (CSIRT'er), herunder om gensidig bistand, og det bredere cybersikkerhedsmiljø

   (c) efterretninger om cybertrusler, herunder situationsbevidsthed

(d) eller et hvilket som helst andet område, hvor CERT-EU's tekniske cybersikkerhedsekspertise er påkrævet.

4. CERT-EU indgår i et struktureret samarbejde med Den Europæiske Unions Agentur for Cybersikkerhed 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 relation til EU-institutionernes, -organernes og -agenturernes 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-institutionernes, -organernes og -agenturernes 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-institutionerne, -organerne og -agenturerne, som arbejder tæt sammen med EU's institutioner, organer og agenturer, f.eks. fordi de er tildelt opgaver eller ansvarsområder i henhold til EU-lovgivning, i henhold til skriftlige aftaler og under forudsætning af forudgående godkendelse fra IICB.

6. CERT-EU kan arrangere cybersikkerhedsøvelser eller opfordre til deltagelse i eksisterende øvelser, hvor det er relevant i tæt samarbejde med Den Europæiske Unions Agentur for Cybersikkerhed, med henblik på at teste cybersikkerhedsniveauet i EU's institutioner, organer og agenturer.

7. CERT-EU kan yde bistand til EU's institutioner, organer og agenturer vedrørende hændelser i klassificerede IT-miljøer, hvis den berørte deltager udtrykkeligt anmoder herom.

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's institutioner, organer og agenturer kraftigt opfordres til at træffe inden udløbet af en fastsat frist

(b) forslag til IICB om vejledende dokumenter rettet til alle eller en delgruppe af EU's institutioner, organer og agenturer

(c) forslag til IICB om henstillinger rettet til EU-enkeltinstitutioner, -organer eller -agenturer.

2. Vejledende dokumenter og henstillinger kan omfatte:

(a) metoder til eller forbedring af styringen af cybersikkerhedsrisici og referencescenariet for cybersikkerhed

(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 som omhandlet i artikel 4, nr. 10, i direktiv [proposal NIS 2].

3. IICB kan vedtage vejledende dokumenter og henstillinger på forslag af CERT-EU.

4. IICB kan instruere CERT-EU i at udstede, tilbagekalde eller ændre et foreslået vejledende dokument, en henstilling eller en opfordring til tiltag.

Artikel 14
Chefen for CERT-EU

Chefen for CERT-EU forelægger regelmæssigt rapporter til IICB og IICB's formand 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, stk. 1.

Artikel 15
Finansielle og personalemæssige spørgsmål

1. Kommissionen udpeger efter IICB's enstemmige godkendelse 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. 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, 3, 4 og 6, og artikel 13, stk. 1, til EU's institutioner, organer og agenturer, 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-institutioner, -organer og -agenturer 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[8].

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

[8] 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 oplysninger med de nationale modparter i medlemsstaterne, herunder CERT'er, nationale cybersikkerhedscentre, CSIRT'er og centrale kontaktpunkter, jf. artikel 8 i direktiv [proposal NIS 2], om cybertrusler, sårbarheder og hændelser, om eventuelle modforanstaltninger og om alle områder, der er relevante for at forbedre beskyttelsen af EU-institutionernes, -organernes og -agenturernes IT-miljøer, herunder gennem det CSIRT-netværk, der er omhandlet i artikel 13 i direktiv [proposal NIS 2].

2. CERT-EU må, uden den berørte deltagers samtykke, udveksle hændelsesspecifikke oplysninger med nationale modparter i medlemsstaterne for at fremme detektionen af lignende cybertrusler eller hændelser. CERT-EU må kun udveksle hændelsesspecifikke oplysninger, der afslører identiteten på målet for en cybersikkerhedshændelse med den berørte deltagers samtykke.

Artikel 17

CERT-EU's samarbejde med tredjelandes modparter

1. CERT-EU må samarbejde med modparter i tredjelande, inkl. branchespecifikke modparter, om værktøjer og metoder såsom teknikker, taktikker, procedurer og bedste praksis samt om cybertrusler og sårbarheder. CERT-EU indhenter i forbindelse med alt samarbejde med sådanne modparter, herunder inden for rammer, hvor modparter i tredjelande samarbejder med nationale modparter i medlemsstaterne, forudgående godkendelse fra IICB.

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.

3. CERT-EU må med samtykke fra den deltager, der er berørt af hændelsen, udlevere oplysninger om hændelsen til partnere, der kan bidrage til analysen heraf.

Kapitel V
SAMARBEJDE OG RAPPORTERINGSFORPLIGTELSER

Artikel 18

Datahåndtering

1. CERT-EU og EU's institutioner, organer og agenturer overholder 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[9] finder anvendelse på anmodninger om aktindsigt i dokumenter, som CERT-EU er i besiddelse af, herunder nævnte forordnings forpligtelse om at rådføre sig med andre

[9] 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).

EU-institutioner, -organer og -agenturer, når en anmodning vedrører deres dokumenter.

3. Behandling af personoplysninger, som udføres i henhold til nævnte forordning, er omfattet af Europa-Parlamentets og Rådets forordning (EU) 2018/1725.

4. CERT-EU's og EU-institutionernes, -organernes og -agenturernes håndtering af data sker i overensstemmelse med bestemmelserne i [proposed Regulation on information security].

5. Alle kontakter med CERT-EU, som indledes eller efterspørges af nationale sikkerheds- og efterretningstjenester, kommunikeres uden unødig forsinkelse til Kommissionens Direktorat for Sikkerhed og formanden for IICB.

Artikel 19
Delingsforpligtelser

1. Med henblik på at gøre det muligt for CERT-EU at koordinere styringen af sårbarheder og reaktionen på hændelser kan det anmode EU's institutioner, organer og agenturer om oplysninger fra deres respektive IT-systemfortegnelser, der er relevante for den støtte, som CERT-EU yder. En EU-institution, -organ eller -agentur, der modtager en sådan anmodning, overfører de oplysninger, der anmodes om, samt eventuelle efterfølgende ajourføringer heraf uden unødig forsinkelse.

2. EU's institutioner, organer og agenturer 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, hvilken type digitale oplysninger det har brug for i forbindelse med situationsbevidsthed og reaktion på hændelser.

3. CERT-EU må kun udveksle hændelsesspecifikke oplysninger, der afslører identiteten på den EU-institution, -organ eller -agentur, der er berørt af hændelsen, med denne enheds samtykke. CERT-EU må kun udveksle hændelsesspecifikke oplysninger, der afslører identiteten på målet for en cybersikkerhedshændelse, med samtykke fra den enhed, der er berørt af hændelsen.

4. Delingsforpligtelsen gælder ikke EU-klassificerede informationer (EUCI) eller informationer, som en EU-institution, -organ eller -agentur har modtaget fra medlemsstaternes sikkerhedsmyndigheder, efterretningstjenester eller retshåndhævende myndigheder på eksplicit betingelse af, at de ikke deles med CERT-EU.

Artikel 20
Underretningspligt

1. Alle EU's institutioner, organer og agenturer indsender en første underretning til CERT-EU om væsentlige cybertrusler, væsentlige sårbarheder og væsentlige hændelser uden unødig forsinkelse og senest 24 timer efter, at de er blevet opmærksom på dem.

   I behørigt begrundede tilfælde og efter aftale med CERT-EU kan den berørte EU-institution, -organ eller -agentur overskride den i forrige stykke fastsatte frist.

2. EU's institutioner, organer og agenturer indsender desuden uden unødig forsinkelse relevante tekniske detaljer om cybertrusler, sårbarheder og hændelser, der gør det

muligt at foretage detektion, reagere på hændelser eller træffe afhjælpende foranstaltninger, til CERT-EU. Underretningen skal om muligt omfatte følgende:

(a) relevante kompromitteringsindikatorer

(b) relevante detektionsmekanismer

(c) potentiel virkning

(d) relevante afhjælpende foranstaltninger.

3. CERT-EU forelægger hver måned en sammenfattende rapport for Den Europæiske Unions Agentur for Cybersikkerhed, herunder anonymiserede og aggregerede data om hændelser, væsentlige cybertrusler, væsentlige sårbarheder og væsentlige hændelser, der er underrettet om i overensstemmelse med stk. 1.

4. IICB kan udstede vejledende dokumenter eller henstillinger om metoden for og indholdet af underretningen. CERT-EU formidler de relevante tekniske detaljer om cybertrusler for at gøre det muligt for EU's institutioner, organer og agenturer at foretage proaktiv detektion, reagere på hændelser eller træffe afhjælpende foranstaltninger.

5. Underretningsforpligtelsen gælder ikke EUCI eller informationer, som en EU-institution, -organ eller -agentur har modtaget fra medlemsstaternes sikkerhedsmyndigheder, efterretningstjenester eller retshåndhævende myndigheder på eksplicit betingelse af, at de ikke deles med CERT-EU.

Artikel 21

Koordinering af beredskabet i forbindelse med hændelser og samarbejde om væsentlige hændelser

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

(a) EU's institutioner, organer og agenturer

(b) de i artikel 16 og 17 omhandlede modparter.

2. CERT-EU fremmer koordineringen af reaktioner på hændelser mellem EU's institutioner, organer og agenturer, herunder:

(a) bidrag til konsekvent ekstern kommunikation

(b) gensidig bistand

(c) optimal udnyttelse af operationelle ressourcer

(d) koordineringen med andre krisereaktionsmekanismer på EU-plan.

3. CERT-EU støtter EU-institutionerne, -organerne og -agenturerne i relation til situationsbevidsthed i forbindelse med cybertrusler, sårbarheder og hændelser.

4. IICB udsteder vejledende dokumenter om koordinering af beredskabet i forbindelse med hændelser og samarbejde om væsentlige hændelser. Hvis hændelsen mistænkes for at være af strafferetlig karakter, rådgiver CERT-EU også om, hvordan de retshåndhævende myndigheder underrettes om hændelsen.

Artikel 22

Større angreb

1. CERT-EU koordinerer reaktioner på større angreb mellem EU's institutioner, organer og agenturer. Med henblik på sådanne angreb fører CERT-EU en fortegnelse over den tekniske ekspertise, der vil være brug for i forbindelse med en reaktion på sådanne hændelser.
2. EU's institutioner, organer og agenturer bidrager til denne fortegnelse over teknisk ekspertise i form af en årlig ajourført liste over eksperter, der er til rådighed i deres respektive enheder, inkl. detaljerede beskrivelser af deres specifikke tekniske færdigheder.
3. Hvis de berørte EU-institutioner, -organer og -agenturer godkender det, kan CERT-EU også trække på eksperterne på den liste, der er omhandlet i stk. 2, med henblik på at bidrage til reaktionen på et større angreb i en medlemsstat i overensstemmelse med den fælles cyberenheds standardprocedurer.

Kapitel VI
AFSLUTTENDE BESTEMMELSER

Artikel 23

Oprindelig budgetomfordeling

Kommissionen foreslår en omfordeling af personale og finansielle ressourcer fra de relevante EU-institutioner, -organer og -agenturer 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 foreslå ændringer til denne forordning.
2. Kommissionen rapporterer til Europa-Parlamentet og Rådet om gennemførelsen af denne forordning senest 48 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 tidligst fem år efter datoen for dens ikrafttræden.

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*

FINANSIERINGSOVERSIGT

1. FORSLAGETS/INITIATIVETS RAMME

1.1. Forslagets/initiativets betegnelse

1.2. Berørt(e) politikområde(r)

1.3. Forslaget/initiativet vedrører:

1.4. Mål

1.4.1. Generelt/generelle mål

1.4.2. Specifikt/specifikke mål

1.4.3. Forventet/forventede resultat(er) og virkning(er)

1.4.4. Resultatindikatorer

1.5. Begrundelse for forslaget/initiativet

1.5.1. Behov, der skal opfyldes på kort eller lang sigt, herunder en detaljeret tidsplan for iværksættelsen af initiativet

1.5.2. Merværdien ved et EU-tiltag (f.eks. som følge af koordineringsfordele, retssikkerhed, større effekt eller komplementaritet). Ved "merværdien ved et EU-tiltag" forstås her merværdien af EU's intervention i forhold til den værdi, som medlemsstaterne ville have skabt enkeltvis

1.5.3. Erfaringer fra tidligere foranstaltninger af lignende art

1.5.4. Forenelighed med den flerårige finansielle ramme og mulige synergivirkninger med andre relevante instrumenter

1.5.5. Vurdering af de forskellige finansieringsmuligheder, der er til rådighed, herunder muligheden for omfordeling

1.6. Forslagets/initiativets varighed og finansielle virkninger

1.7. Planlagt(e) forvaltningsmetode(r)

2. FORVALTNINGSFORANSTALTNINGER

2.1. Bestemmelser om overvågning og rapportering

2.2. Forvaltnings- og kontrolsystem(er)

2.2.1. Begrundelse for den/de foreslåede forvaltningsmetode(r), finansieringsmekanisme(r), betalingsvilkår og kontrolstrategi

2.2.2. Oplysninger om de konstaterede risici og det/de interne kontrolsystem(er), der etableres for at afbøde dem

2.2.3. Vurdering af og begrundelse for kontrolforanstaltningernes omkostningseffektivitet (forholdet mellem kontrolomkostningerne og værdien af de forvaltede midler) samt vurdering af den forventede risiko for fejl (ved betaling og ved afslutning)

2.3. Foranstaltninger til forebyggelse af svig og uregelmæssigheder

3. FORSLAGETS/INITIATIVETS ANSLÅEDE FINANSIELLE VIRKNINGER

3.1. Berørt(e) udgiftsområde(r) i den flerårige finansielle ramme og udgiftspost(er) på budgettet

3.2. Forslagets anslåede finansielle virkninger for bevillingerne

3.2.1. Sammenfatning af de anslåede virkninger for aktionsbevillingerne

3.2.2. Anslåede resultater finansieret med aktionsbevillinger

3.2.3. Sammenfatning af de anslåede virkninger for administrationsbevillingerne

3.2.4. Forenelighed med indeværende flerårige finansielle ramme

3.2.5. Bidrag fra tredjemand

3.3. Anslåede virkninger for indtægterne

FINANSIERINGSOVERSIGT

1. FORSLAGETS/INITIATIVETS RAMME

1.1. Forslagets/initiativets betegnelse

Forslag til Europa-Parlamentets og Rådets forordning om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i EU's institutioner, organer, kontorer og agenturer.

1.2. Berørt(e) politikområde(r)

Europæisk offentlig forvaltning

Forslaget vedrører foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i EU's institutioner, organer og agenturer.

1.3. Forslaget/initiativet vedrører:

☑ en ny foranstaltning

☐ en ny foranstaltning som opfølgning på et pilotprojekt/en forberedende foranstaltning[10]

☐ en forlængelse af en eksisterende foranstaltning

☑ en sammenlægning eller en omlægning af en eller flere foranstaltninger til en anden/en ny foranstaltning

1.4. Mål

1.4.1. Generelt/generelle mål

– Skabe rammerne for sikring af et højt fælles cybersikkerhedsniveau i EU's institutioner, organer og agenturer.

– Indføre et nyt retsgrundlag for CERT-EU med henblik på at styrke enhedens mandat og finansieringen af det.

1.4.2. Specifikt/specifikke mål

(1) Fastsætte forpligtelser for EU's institutioner, organer og agenturer om indførelsen af en intern ramme for styring, forvaltning og kontrol af cybersikkerhedsrisici.

(2) Fastsætte forpligtelser for EU's institutioner, organer og agenturer om rapportering om deres ramme for styring, forvaltning og kontrol af cybersikkerhedsrisici samt cybersikkerhedshændelser.

(3) Fastsætte bestemmelser om organiseringen og driften af EU-institutionernes, -organernes og -agenturernes cybersikkerhedscenter (CERT-EU) og om organiseringen og driften af Det Interinstitutionelle Råd for Cybersikkerhed (IICB).

(4) Bidrage til den fælles cyberenhed.

[10] Jf. finansforordningens artikel 58, stk. 2, litra a) hhv. b).

1.4.3. Forventet/forventede resultat(er) og virkning(er)

Angiv, hvilke virkninger forslaget/initiativet forventes at få for modtagerne/målgrupperne.

- Intern ramme for styring, forvaltning og kontrol af cybersikkerhedsrisici, referencescenarier for cybersikkerhed, regelmæssige modenhedsvurderinger og cybersikkerhedsplaner i EU's institutioner, organer og agenturer.
- Forbedring af cybermodstandsdygtigheden og beredskabskapaciteten i EU's institutioner, organer og agenturer.
- Modernisering af CERT-EU.
- Bidrag til den fælles cyberenhed.

1.4.4. Resultatindikatorer

Angiv indikatorerne til overvågning af fremskridt og resultater.

- Fastsatte rammer og referencescenarier, gennemførelse af regelmæssige modenhedsvurderinger og cybersikkerhedsplaner i EU's institutioner, organer og agenturer.
- Bedre håndtering af hændelser.
- Øget kendskab til cybersikkerhedsrisici i topledelsen i EU's institutioner, organer og agenturer.
- Tilpasning af de gennemsnitlige udgifter til IKT-sikkerhed som en procentdel af de samlede IKT-udgifter.
- Stærkt lederskab i IICB og CERT-EU.
- Øget deling af oplysninger mellem EU's institutioner, organer og agenturer og med relevante organer og interessenter i EU.
- Øget cybersikkerhedssamarbejde med relevante organer og interessenter i EU via CERT-EU og ENISA.

1.5. Begrundelse for forslaget/initiativet

1.5.1. Behov, der skal opfyldes på kort eller lang sigt, herunder en detaljeret tidsplan for iværksættelsen af initiativet.

Formålet med forslaget er at øge cybermodstandsdygtigheden i EU's institutioner, organer og agenturer, mindske uoverensstemmelser i modstandsdygtigheden på tværs af disse og forbedre niveauet af fælles situationsbevidsthed og den kollektive kapacitet til at forberede sig og reagere.

Forslaget er fuldt ud i overensstemmelse med og konsekvent i forhold til andre relaterede initiativer, herunder navnlig forslaget til direktiv om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen og om ophævelse af direktiv (EU) 2016/1148 [proposal NIS 2].

Forslaget er en væsentlig del af strategien for EU's sikkerhedsunion og EU's strategi for cybersikkerhed for det digitale årti.

Forslaget forventes fremlagt af Europa-Kommissionen i oktober 2021, vedtaget af Europa-Parlamentet og Rådet i 2022, og bestemmelserne vil gælde fra forordningens ikrafttræden. Det forventes, at indvirkningen på de finansielle og menneskelige ressourcer som præsenteret i denne finansieringsoversigt begynder at slå igennem i 2023. Forberedelsesperioden begyndte allerede i 2021, men de forberedende

aktiviteter, der gennemføres i 2021 og 2022, er ikke omfattet af de virkninger, der beskrives i denne finansieringsoversigt.

1.5.2. Merværdien ved et EU-tiltag (f.eks. som følge af koordineringsfordele, retssikkerhed, større effekt eller komplementaritet). Ved "merværdien ved et EU-tiltag" forstås her merværdien af EU's intervention i forhold til den værdi, som medlemsstaterne ville have skabt enkeltvis

Begrundelse for en indsats på EU-plan (forudgående)

Fra 2019 til 2021 er antallet af væsentlige hændelser orkestreret af avancerede og vedholdende trusselsaktører i EU's institutioner, organer og agenturer steget voldsomt. I første halvdel af 2021 var der således lige så mange væsentlige hændelser som i hele 2020. Dette afspejles også i det antal kriminaltekniske kopier (snapshots af indholdet af de berørte systemer eller anordninger), som CERT-EU analyserede i 2020, idet tallet er tredoblet sammenlignet med 2019 og tidoblet siden 2018.

Cybersikkerhedsmodenheden varierer betydeligt fra den ene enhed til den anden[11]. Denne forordning sikrer, at alle EU's institutioner, organer og agenturer implementerer et minimum af sikkerhedsforanstaltninger og samarbejder med hinanden med det formål at skabe en åben og effektiv velfungerede EU-forvaltning.

De systemer, der skal beskyttes, hører under EU-institutionernes, -organernes og -agenturernes autonomi, og det er EU-institutionerne, -organerne og -agenturerne, der står for driften af dem. De foreslåede tiltag ville ikke kunne gennemføres af medlemsstaterne.

1.5.3. Erfaringer fra tidligere foranstaltninger af lignende art

NIS-direktivet var det første horisontale instrument for det indre marked, der havde til formål at forbedre nettenes og systemernes modstandsdygtighed over for cybersikkerhedsrisici i EU. Siden det trådte i kraft i 2016, har det i høj grad bidraget til at øge det fælles cybersikkerhedsniveau i medlemsstaterne. Forslaget til NIS 2-direktivet har til formål at forbedre disse foranstaltninger yderligere.

Denne forordning har til formål at indføre tilsvarende foranstaltninger i EU's institutioner, organer og agenturer.

1.5.4. Forenelighed med den flerårige finansielle ramme og mulige synergivirkninger med andre relevante instrumenter

Forslaget er i overensstemmelse med den flerårige finansielle ramme og udgør en væsentlig del af strategien for EU's sikkerhedsunion og EU's strategi for cybersikkerhed for det digitale årti.

Forslaget indfører foranstaltninger med henblik på et højt fælles cybersikkerhedsniveau i EU's institutioner, organer og agenturer. Forslaget er i overensstemmelse med forslaget til direktiv om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen og om ophævelse af direktiv (EU) 2016/1148 [proposal NIS 2].

[11] Reference: [ECA Special Report on cybersecurity at the Union institutions, bodies and agencies].

1.5.5. Vurdering af de forskellige finansieringsmuligheder, der er til rådighed, herunder muligheden for omfordeling

CERT-EU's forvaltning af disse opgaver kræver særlige profiler og en ekstra arbejdsbyrde, som ikke kan absorberes uden en styrkelse af de menneskelige og finansielle ressourcer.

1.6. Forslagets/initiativets varighed og finansielle virkninger

☐ **Begrænset varighed**

– ☐ gældende fra [DD/MM]ÅÅÅÅ til [DD/MM]ÅÅÅÅ

– ☐ finansielle virkninger fra ÅÅÅÅ til ÅÅÅÅ for forpligtelsesbevillinger og fra ÅÅÅÅ til ÅÅÅÅ for betalingsbevillinger

☑ **Ubegrænset varighed**

– Den finansielle virkning bør indarbejdes i det første budget, der vedtages efter forordningens ikrafttræden. Der vil blive gennemført en omfordeling af ressourcer fra EU's institutioner og primære organer til Kommissionen i løbet af det første år, der betragtes som et overgangsår. Denne og andre omfordelinger/tildelinger af ressourcer vil foregå inden for rammerne af de årlige budgetter. Hvis denne forordning vedtages i 2022, vil 2023 være overgangsår, mens fuld drift forventes i 2024.

1.7. Planlagt(e) forvaltningsmetode(r)[12]

☑ Direkte forvaltning ved Kommissionen og ved hver EU-institution, organ og agentur

– ☑ i dens tjenestegrene, herunder ved dens personale i EU's delegationer

– ☐ i forvaltningsorganerne

☐ **Delt forvaltning** i samarbejde med medlemsstaterne

☐ **Indirekte forvaltning** ved at overlade budgetgennemførelsesopgaver til:

– ☐ tredjelande eller organer, som tredjelande har udpeget

– ☐ internationale organisationer og deres agenturer (angives nærmere)

– ☐ Den Europæiske Investeringsbank og Den Europæiske Investeringsfond

– ☐ de organer, der er omhandlet i finansforordningens artikel 70 og 71

– ☐ offentligretlige organer

– ☐ privatretlige organer, der har fået overdraget offentlige tjenesteydelsesopgaver, i det omfang de har fået stillet tilstrækkelige finansielle garantier

– ☐ privatretlige organer, undergivet lovgivningen i en medlemsstat, som har fået overdraget gennemførelsen af et offentlig-privat partnerskab, og som har fået stillet tilstrækkelige finansielle garantier

– ☐ personer, der har fået overdraget gennemførelsen af specifikke aktioner i den fælles udenrigs- og sikkerhedspolitik i henhold til afsnit V i traktaten om Den Europæiske Union, og som er anført i den relevante basisretsakt

– *Hvis der angives flere forvaltningsmetoder, gives der en nærmere forklaring i afsnittet "Bemærkninger".*

Bemærkninger

Med hensyn til anvendelsen af de administrative og finansielle procedurer referer CERT-EU til Kommissionen.

[12] Forklaringer vedrørende forvaltningsmetoder og henvisninger til finansforordningen findes på webstedet BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx

Supplerende ressourcer afledt af forslaget til forordning:

Gennemførelsen af artikel 12 og 13 i forslaget til forordning medfører en udvidelse af tjenestekataloget med flere basistjenester. Følgende supplerende ressourcer vil skulle tilføres (indtil udgangen af 2027, når den flerårige finansielle ramme ophører), når fuld drift er opnået: 21 årsværk og 14,05 mio. EUR.

De supplerende ressourcer til budgettet fordeles på de forskellige opgaver som følger:

(a) Udførelsen af opgaver for EU's institutioner, organer og agenturer, jf. artikel 12, stk. 2, litra a), b), c) og e): 13,75 årsværk og 11,275 mio. EUR.

(b) Udførelsen af opgaver, jf. artikel 12, stk. 3 (bidrag til den fælles cyberenhed): 2 årsværk og 381 000 EUR.

(c) Udførelsen af opgaver, jf. artikel 12, stk. 4 (struktureret samarbejde med ENISA): 0,25 årsværk og 236 000 EUR.

(d) Udførelsen af opgaver, jf. artikel 12, stk. 6 (cybersikkerhedsøvelser): 0,25 årsværk og 79 000 EUR.

(e) Udførelsen af opgaver, jf. artikel 12, stk. 2, litra d), og artikel 13 (analyse af og rapportering om gennemførelsen af forordningen, udarbejdelse af vejledende dokumenter, henstillinger og opfordringer til tiltag): 3,75 årsværk og 2,079 mio. EUR.

(f) Udførelsen af opgaver til støtte for Det Interinstitutionelle Råd for Cybersikkerheds (IICB's) sekretariat. 1 årsværk.

Oversigt over de aktuelle ressourcer og overgangen til fuld drift:

I september 2021 blev CERT-EU drevet med følgende ressourcer:

— faste og udstationeringsstillinger: 14 årsværk

— kontraktansatte finansieret under serviceleveranceaftaler: 24 årsværk

— i alt 38 årsværk.

I 2020 var CERT-EU's budget på: 250 000 EUR finansieret over Kommissionens budget plus 3,5 mio. EUR i formålsbestemte indtægter i henhold til serviceleveranceaftaler. I alt: 3,75 mio. EUR. Disse midler udgjorde CERT-EU's samlede budget, som dækker uddannelse, hardware, software, missioner, support, kontraktansatte og konferencer.

Når denne forordning er trådt i kraft forventes CERT-EU's fremtidige ressourcer at løbe op i:

— faste stillinger: 34 årsværk

— kontraktansatte: 15 årsværk

— i alt 49 årsværk og dermed en nettoforøgelse på 11 årsværk.

Ændringen i forholdet mellem faste stillinger og kontraktstillinger afspejler de væsentlige hindringer for rekruttering og fastholdelse af erfarne fagfolk inden for cybersikkerhed som følge af manglen på sådanne på arbejdsmarkedet.

Derudover er der brug for 1 årsværk til kontraktansatte i Kommissionens Generaldirektorat for Informationsteknologi, der skal yde støtte til IICB (Det Interinstitutionelle Råd for Cybersikkerhed).

Der er således brug for i alt 21 årsværk mere til at gennemføre forordningen (20 årsværk til CERT-EU og 1 årsværk til Kommissionens Generaldirektorat for Informationsteknologi).

Dette kompenseres med en parallel reduktion på 9 årsværk til kontraktansatte i CERT-EU, som tidligere blev finansieret ved hjælp af formålsbestemte indtægter i henhold til serviceleveranceaftaler.

CERT-EU's budget til andre ressourcer end de menneskelige vil i 2024 efter overgangen omfatte de opgaver, der er anført ovenfor i litra a) til e), og forventes finansieret som følger:

— 8,921 mio. EUR om året fra de EU-institutioner, der finansieres under udgiftsområde 7 i EU-budgettet

— 2,459 mio. EUR fra de EU-institutioner, -organer og -agenturer, der finansieres under udgiftsområde 1-6 i EU-budgettet

— 2,670 mio. EUR fra selvfinansierende EU-institutioner, -organer og -agenturer

— CERT-EU-budget i alt: 14,05 mio. EUR.

De opgaver, der er omhandlet i artikel 12, stk. 5, er ikke beskrevet i tjenestekataloget, de er betalingspligtige. Der er tale om accessoriske tjenester til en relativt lav pris, og som for det meste er midlertidige, og omkostningerne ved disse tjenester opkræves hos kunden i henhold til en serviceleveranceaftale eller en skriftlig aftale.

Hvad angår bidrag til CERT-EU's personale: EU-institutionerne og de primære organer bidrager med en retfærdig andel proportionel med den respektive andel af enhedens andel af faste stillinger. Det bør overvejes, om ECB og EIB også kan bidrage med en retfærdig andel i form af udstationeret fastansat personale.

2. FORVALTNINGSFORANSTALTNINGER

2.1. Bestemmelser om overvågning og rapportering

Angiv hyppighed og betingelser.

Med hjælp fra IICB og CERT-EU vil Kommissionen regelmæssigt gennemgå denne forordnings funktion og rapportere til Europa-Parlamentet og Rådet herom, første gang senest 48 måneder efter forordningens ikrafttræden og derefter hvert tredje år.

De datakilder, der anvendes til gennemgangen vil hovedsagelig komme fra IICB og CERT-EU. Derudover kan der anvendes særlige dataindsamlingsværktøjer efter behov (f.eks. rundspørger udarbejdet af EU's institutioner, organer og agenturer, ENISA eller CSIRT-netværket).

2.2. Forvaltnings- og kontrolsystem(er)

2.2.1. Begrundelse for den/de foreslåede forvaltningsmetode(r), finansieringsmekanisme(r), betalingsvilkår og kontrolstrategi

Tiltag afledt af forordningen forvaltes af hver enkelt EU-institution, -organ eller -agentur i overensstemmelse med dennes relevante gældende regler og bestemmelser.

Den administrative og finansielle forvaltning af CERT-EU's aktiviteter er omfattet af Kommissionens forvaltning og følger de gældende forvaltnings- og gennemførelsesmekanismer, betalingsvilkår og kontrolstrategier.

Kommissionens interne revisor har samme beføjelser over for CERT-EU som over for Kommissionens tjenestegrene.

2.2.2. Oplysninger om de konstaterede risici og det/de interne kontrolsystem(er), der etableres for at afbøde dem

Meget lav risiko, eftersom CERT-EU allerede er administrativt tilknyttet Kommissionen som en taskforce under generaldirektøren for informationsteknologi, og IICB oprettes efter CERT-EU's nuværende styrelsesråd. Økosystemet for den finansielle forvaltning og den interne kontrol er således allerede på plads.

2.2.3. Vurdering af og begrundelse for kontrolforanstaltningernes omkostningseffektivitet (forholdet mellem kontrolomkostningerne og værdien af de forvaltede midler) samt vurdering af den forventede risiko for fejl (ved betaling og ved afslutning)

Procedurerne for indkøb, finansiel forvaltning og kontrol er allerede på plads og godt afprøvet. Kontrollernes omkostningseffektivitet og den forventede risiko for fejl svarer til hver EU-institutions, -organs eller -agenturs og til Kommissionens for så vidt angår CERT-EU-aktiviteter.

2.3. Foranstaltninger til forebyggelse af svig og uregelmæssigheder

Angiv eksisterende eller påtænkte forebyggelses- og beskyttelsesforanstaltninger, f.eks. fra strategien til bekæmpelse af svig.

Kommissionens finansielle forvaltning og interne kontrolsystemer finder anvendelse på CERT-EU-aktiviteter.

Bestemmelserne i Europa-Parlamentets og Rådets forordning (EU, Euratom) nr. 883/2013 af 11. september 2013 om undersøgelser, der foretages af Det Europæiske

Kontor for Bekæmpelse af Svig (OLAF), finder ubegrænset anvendelse i forbindelse med bekæmpelsen af svig, korruption og andre retsstridige handlinger.

3. FORSLAGETS/INITIATIVETS ANSLÅEDE FINANSIELLE VIRKNINGER

3.1. Berørt(e) udgiftsområde(r) i den flerårige finansielle ramme og udgiftspost(er) på budgettet

- Eksisterende budgetposter

I samme rækkefølge som udgiftsområderne i den flerårige finansielle ramme og budgetposterne.

Udgiftsområde i den flerårige finansielle ramme	Budgetpost	Udgiftens art	Bidrag			
	Nummer	OB/IOB[13]	fra EFTA-lande[14]	fra kandidatlande[15]	fra tredjelande	iht. finansforordningens artikel 21, stk. 2, litra b)
1 til 6	Budgetposter, der omhandler EU-bidrag til decentrale agenturer og organer	OB	NEJ	NEJ	NEJ	NEJ
7	Budgetposter, der omhandler vederlag til personalet, IT-udgifter og andre administrationsudgifter i de forskellige afsnit af EU-budgettet	IOB	NEJ	NEJ	NEJ	NEJ

- Nye budgetposter, som der anmodes om

I samme rækkefølge som udgiftsområderne i den flerårige finansielle ramme og budgetposterne.

Udgiftsområde i den flerårige finansielle ramme	Budgetpost	Udgiftens art	Bidrag			
	Nummer	OB/IOB	fra EFTA-lande	fra kandidatlande	fra tredjelande	iht. finansforordningens artikel 21, stk. 2, litra b)
	Ingen		JA/NEJ	JA/NEJ	JA/NEJ	JA/NEJ

[13] OB = opdelte bevillinger/IOB = ikke-opdelte bevillinger.
[14] EFTA: Den Europæiske Frihandelssammenslutning.
[15] Kandidatlande og, hvis det er relevant, potentielle kandidater på Vestbalkan.

3.2. Forslagets anslåede finansielle virkninger for bevillingerne

3.2.1. Sammenfatning af de anslåede virkninger for aktionsbevillingerne

– ☐ Forslaget/initiativet medfører ikke anvendelse af aktionsbevillinger

– ☑ Forslaget/initiativet medfører anvendelse af aktionsbevillinger som anført herunder:

i mio. EUR (tre decimaler)

Udgiftsområde i den flerårige finansielle ramme	1 til 6	Udgiftsområder, der omhandler bidrag til decentrale agenturer og organer

GD: Flere forskellige			År **2023**	År **2024**	År **2025**	År **2026**	År **2027**	**I ALT**
○Aktionsbevillinger								
Budgetposter, der omhandler EU-bidrag til decentrale agenturer (xx 10 xx xx)[16]	Forpligtelser	(1a)	2,459	2,459	2,459	2,459	2,459	12,293
	Betalinger	(2a)	2,459	2,459	2,459	2,459	2,459	12,293
Administrationsbevillinger finansieret over bevillingsrammen for særprogrammer[17]								
Budgetpost		(3)						
Bevillinger I ALT til GD: Flere forskellige	Forpligtelser	=1a+1b +3	2,459	2,459	2,459	2,459	2,459	12,293
	Betalinger	=2a+2b +3	2,459	2,459	2,459	2,459	2,459	12,293

[16] Ifølge den officielle budgetkontoplan.

[17] Teknisk og/eller administrativ bistand og udgifter til støtte for gennemførelsen af EU's programmer og/eller foranstaltninger (tidligere BA-poster), indirekte forskning, direkte forskning.

○ Aktionsbevillinger I ALT	Forpligtelser	(4)	2,459	2,459	2,459	2,459	2,459	12,293
	Betalinger	(5)	2,459	2,459	2,459	2,459	2,459	12,293
○ Administrationsbevillinger finansieret over bevillingsrammen for særprogrammer I ALT		(6)						
Bevillinger I ALT under UDGIFTSOMRÅDE 1-6 i den flerårige finansielle ramme	Forpligtelser	=4+ 6	2,459	2,459	2,459	2,459	2,459	12,293
	Betalinger	=5+ 6	2,459	2,459	2,459	2,459	2,459	12,293

Hvis flere aktionsrelaterede udgiftsområder berøres af forslaget/initiativet, indsættes der et tilsvarende afsnit for hvert udgiftsområde

○ Aktionsbevillinger I ALT (alle aktionsrelaterede udgiftsområder)	Forpligtelser	(4)	2,459	2,459	2,459	2,459	2,459	12,293
	Betalinger	(5)	2,459	2,459	2,459	2,459	2,459	12,293
Administrationsbevillinger finansieret over bevillingsrammen for særprogrammer I ALT (alle aktionsrelaterede udgiftsområder)		(6)						
Bevillinger I ALT under UDGIFTSOMRÅDE 1-6 i den flerårige finansielle ramme (referencebeløb)	Forpligtelser	=4+ 6	2,459	2,459	2,459	2,459	2,459	12,293
	Betalinger	=5+ 6	2,459	2,459	2,459	2,459	2,459	12,293

Udgiftsområde i den flerårige finansielle ramme	7	"Administrationsudgifter"

Dette afsnit skal udfyldes ved hjælp af arket vedrørende administrative budgetoplysninger, der først skal indføres i bilaget til finansieringsoversigten (bilag V til de interne regler), som uploades til DECIDE med henblik på høring af andre tjenestegrene.

i mio. EUR (tre decimaler)

		År **2023**	År **2024**	År **2025**	År **2026**	År **2027**	**I ALT**
GD: DIGIT (CERT-EU)							
○ Menneskelige ressourcer		1,184	2,126	2,754	3,225	3,225	12,514
○ Andre administrationsudgifter		7,938	8,921	8,921	8,921	8,921	43,622
I ALT GD DIGIT (CERT-EU)	Bevillinger	9,122	11,047	11,675	12,146	12,146	56,136

Bevillinger I ALT under UDGIFTSOMRÅDE 7 i den flerårige finansielle ramme	(Forpligtelser i alt = betalinger i alt)	9,122	11,047	11,675	12,146	12,146	**56,136**

i mio. EUR (tre decimaler)

		År 2023	År 2024	År 2025	År 2026	År 2027	**I ALT**
Bevillinger I ALT under UDGIFTSOMRÅDE 1-7 i den flerårige finansielle ramme(*)	Forpligtelser	11,581	13,506	14,134	14,605	14,605	68,429
	Betalinger	11,581	13,506	14,134	14,605	14,605	68,429

(*) Bidrag fra selvfinansierende EU-institutioner, -organer og -agenturer er anslået til 2,670 mio. EUR om året (13,350 mio. EUR i alt for de fem år). Bidragene udgør formålsbestemte indtægter for CERT-EU. Tabellerne ovenfor omfatter kun den anslåede samlede virkning for EU-budgettet og omfatter ikke disse bidrag.

3.2.2. Anslåede resultater finansieret med aktionsbevillinger

Forpligtelsesbevillinger i mio. EUR (tre decimaler)

Angiv mål og resultater ⇩			År **n**		År **n+1**		År **n+2**		År **n+3**		Indsæt så mange år som nødvendigt for at vise virkningernes varighed (jf. punkt 1.6)						**I ALT**	
	RESULTATER																	
	Type[18]	Gnsntl. omkostninger	Nej	Omkostninger	Nej	Omkostninger	Nej	Omkostninger	Nej	Omkostninger	Nej	Omkostninger	Nej	Omkostninger	Nej	Omkostninger	Antal resultater i alt	Omkostninger i alt
SPECIFIKT MÅL NR. 1[19]...																		
— Resultat																		
— Resultat																		
— Resultat																		
Subtotal for specifikt mål nr. 1																		
SPECIFIKT MÅL NR. 2																		
— Resultat																		
Subtotal for specifikt mål nr. 2																		
I ALT																		

[18] Resultater er de produkter og tjenesteydelser, der skal leveres (f.eks.: antal finansierede studenterudvekslinger, antal km bygget vej osv.).

[19] Som beskrevet i punkt 1.4.2 "Specifikt/specifikke mål".

3.2.3. Sammenfatning af de anslåede virkninger for administrationsbevillingerne

– ☐ Forslaget/initiativet medfører ikke anvendelse af administrationsbevillinger

– ☑ Forslaget/initiativet medfører anvendelse af administrationsbevillinger som anført herunder:

i mio. EUR (tre decimaler)

	År 2023	År 2024	År 2025	År 2026	År 2027	**I ALT**
UDGIFTSOMRÅDE 7 i den flerårige finansielle ramme						
Menneskelige ressourcer						
Fastansat personale (AD'ere)	1,099	2,041	2,669	3,14	3,14	12,089
Kontraktansatte	0,085	0,085	0,085	0,085	0,085	0,425
Andre administrationsudgifter	7,938	8,921	8,921	8,921	8,921	43,622
Subtotal UDGIFTSOMRÅDE 7 i den flerårige finansielle ramme	9,122	11,047	11,675	12,146	12,146	56,136
Uden for UDGIFTSOMRÅDE 7[20] i den flerårige finansielle ramme						
Menneskelige ressourcer						
Andre administrationsudgifter						
Subtotal uden for UDGIFTSOMRÅDE 7 i den flerårige finansielle ramme						
I ALT	9,122	11,047	11,675	12,146	12,146	56,136

Bevillingerne til menneskelige ressourcer og andre administrationsudgifter vil blive dækket ved hjælp af de bevillinger, som generaldirektoratet allerede har afsat til forvaltning af foranstaltningen, og/eller ved intern omfordeling i generaldirektoratet, eventuelt suppleret med yderligere bevillinger, som tildeles det ansvarlige generaldirektorat i forbindelse med den årlige tildelingsprocedure under hensyntagen til de budgetmæssige begrænsninger.

[20] Teknisk og/eller administrativ bistand og udgifter til støtte for gennemførelsen af EU's programmer og/eller foranstaltninger (tidligere BA-poster), indirekte forskning, direkte forskning.

3.2.3.1. Anslået behov for menneskelige ressourcer

– ☐ Forslaget/initiativet medfører ikke anvendelse af menneskelige ressourcer

– ☑ Forslaget/initiativet medfører anvendelse af menneskelige ressourcer som anført herunder:

Overslag angives i årsværk

		År 2023	År 2024	År 2025	År 2026	År 2027		
O Stillinger i stillingsfortegnelsen (tjenestemænd og midlertidigt ansatte)								
20 01 02 01 (i Kommissionens hovedsæde og repræsentationskontorer)		7	13	17	20	20		
20 01 02 03 (i delegationerne)								
01 01 01 01 (indirekte forskning)								
01 01 01 11 (direkte forskning)								
Andre budgetposter (angiv nærmere)								
O Eksternt personale (i årsværk) [21]								
20 02 01 (KA, UNE, V under den samlede bevillingsramme)		1	1	1	1	1		
20 02 03 (KA, LA, UNE, V og JMD i delegationerne)								
XX 01 xx **yy zz** [22]	— i hovedsædet							
	— i delegationerne							
01 01 01 02 (KA, UNE, V – indirekte forskning)								
01 01 01 12 (KA, UNE, V – direkte forskning)								
Andre budgetposter (angiv nærmere)								
I ALT		**8**	**14**	**18**	**21**	**21**		

XX angiver det berørte politikområde eller budgetafsnit.

Personalebehovet vil blive dækket ved hjælp af det personale, som generaldirektoratet allerede har afsat til forvaltning af foranstaltningen, og/eller ved interne rokader i generaldirektoratet, eventuelt suppleret med yderligere bevillinger, som tildeles det ansvarlige generaldirektorat i forbindelse med den årlige tildelingsprocedure under hensyntagen til de budgetmæssige begrænsninger.

Opgavebeskrivelse:

Tjenestemænd og midlertidigt ansatte	Tjenestemænd udfører CERT-EU-opgaver og -aktiviteter i henhold til forordningen, særlig kapitel IV og V.
Eksternt personale	Kontraktansatte bistår Det Interinstitutionelle Råd for Cybersikkerheds sekretariatsfunktioner.

[21] KA: kontraktansatte, LA: lokalt ansatte, UNE: udstationerede nationale eksperter, V: vikarer, JMD: juniormedarbejdere i delegationerne.

[22] Delloft for eksternt personale under aktionsbevillingerne (tidligere BA-poster).

3.2.4. Forenelighed med indeværende flerårige finansielle ramme

Forslaget/initiativet:

– ☑ kan finansieres fuldt ud gennem omfordeling inden for det relevante udgiftsområde i den flerårige finansielle ramme (FFR)

Gør rede for omlægningen med angivelse af de berørte budgetposter og de beløb, der er tale om. I tilfælde af omfattende omlægning gives oplysningerne i form af en exceltabel.

– ☐ kræver anvendelse af den uudnyttede margen under det relevante udgiftsområde i FFR og/eller anvendelse af særlige instrumenter som fastlagt i FFR-forordningen

Gør rede for behovet med angivelse af de berørte udgiftsområder og budgetposter, de beløb, der er tale om, og de instrumenter, der foreslås anvendt.

– ☐ kræver en revision af FFR

Gør rede for behovet med angivelse af de berørte udgiftsområder og budgetposter og de beløb, der er tale om.

3.2.5. Bidrag fra tredjemand

Forslaget/initiativet:

– ☑ indeholder ikke bestemmelser om samfinansiering med tredjemand[23]

– ☐ indeholder bestemmelser om samfinansiering med tredjemand, jf. følgende overslag:

Bevillinger i mio. EUR (tre decimaler)

	År **n**[24]	År **n+1**	År **n+2**	År **n+3**	Indsæt så mange år som nødvendigt for at vise virkningernes varighed (jf. punkt 1.6)			I alt
Angiv det organ, der deltager i samfinansieringen								
Samfinansierede bevillinger I ALT								

[23] De formålsbestemte indtægter, som stammer fra leveringen af ydelser til ikke-deltagende organisationer, jf. artikel 12, stk. 5, litra c), er ikke beregnet, eftersom de forventes at være marginale.

[24] År n er det år, hvor gennemførelsen af forslaget/initiativet påbegyndes. Erstat "n" med det forventede første gennemførelsesår (f.eks.: 2021). Dette gælder også for de efterfølgende år.

3.3. Anslåede virkninger for indtægterne

– ☑ Forslaget/initiativet har ingen finansielle virkninger for indtægterne

– ☐ Forslaget/initiativet har følgende finansielle virkninger:

– – ☐ for egne indtægter

– – ☐ for andre indtægter

– – Angiv, om indtægterne er formålsbestemte ☐

i mio. EUR (tre decimaler)

Indtægtspost på budgettet	Bevillinger til rådighed i indeværende regnskabsår	Forslagets/initiativets virkninger[25]						
		År **n**	År **n+1**	År **n+2**	År **n+3**	Indsæt så mange år som nødvendigt for at vise virkningernes varighed (jf. punkt 1.6)		
Artikel …								

For indtægter, der er formålsbestemte, angives det, hvilke af budgettets udgiftsposter der berøres.

Andre bemærkninger (f.eks. om hvilken metode, der er benyttet til at beregne virkningerne for indtægterne).

[25] Med hensyn til EU's traditionelle egne indtægter (told og sukkerafgifter) opgives beløbene netto, dvs. bruttobeløb, hvorfra der er trukket opkrævningsomkostninger på 20 %.