Rådet for
Den Europæiske Union

Bruxelles, den 29. marts 2022
(OR. en)

7670/22
ADD 7

Interinstitutionel sag:
2022/0084(COD)

CSC 128
CSCI 45
CYBER 100
INST 99
INF 40
CODEC 385
IA 34

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.:	SWD(2022) 65 final
Vedr.:	ARBEJDSDOKUMENT FRA KOMMISSIONENS TJENESTEGRENE RESUMÉ AF KONSEKVENSANALYSEN Ledsagedokument til Forslag til EUROPA-PARLAMENTETS OG RÅDETS FORORDNING om informationssikkerhed i EU's institutioner, organer, kontorer og agenturer

Hermed følger til delegationerne dokument SWD(2022) 65 final.

Bilag: SWD(2022) 65 final

EUROPA-
KOMMISSIONEN

Bruxelles, den 22.3.2022
SWD(2022) 65 final

ARBEJDSDOKUMENT FRA KOMMISSIONENS TJENESTEGRENE

RESUMÉ AF KONSEKVENSANALYSEN

Ledsagedokument til

Forslag til EUROPA-PARLAMENTETS OG RÅDETS FORORDNING

om informationssikkerhed i EU's institutioner, organer, kontorer og agenturer

{COM(2022) 119 final} - {SWD(2022) 66 final}

Resumé

Konsekvensanalyse, der ledsager forslaget til forordning om informationssikkerhed i EU's institutioner, organer, kontorer og agenturer.

A. Politisk baggrund

I forbindelse med Det Europæiske Råds strategiske dagsorden 2019-2024 opfordres institutionerne til at beskytte EU's informations- og kommunikationsnetværk og dets beslutningsprocesser mod alle former for ondsindede aktiviteter, herunder cyber- og hybridangreb. Derfor erklærede Rådet for Almindelige Anliggender i sine konklusioner af december 2019, at EU's institutioner og organer bør udvikle og gennemføre et omfattende sæt foranstaltninger med henblik på at sikre deres informationssikkerhed.

I juli 2020 vedtog Kommissionen sin strategi for EU's sikkerhedsunion, ved hvilken den forpligtede sig til at supplere den nationale indsats på alle områder for sikkerhed. Som en del af denne strategi foreslog Kommissionen at fastsætte et sæt minimumsregler for informations- og cybersikkerhed på tværs af alle EU's institutioner og organer.

B. Hvad er problemstillingen?

Hovedproblemstillingerne er: i) betydelig forskel i sikkerhedsniveauet i EU's institutioner og organer afhængig af deres interne informationssikkerhedsregler og ii) mangel på koordinering mellem EU's institutioner og organer i forbindelse med udførelsen af deres sikkerhedsopgaver.

EU's institutioner og organer har i dag hver deres egne informationssikkerhedsregler, og nogle enheder har slet ikke har fastsat regler. Fragmenteringen af de relevante retlige rammer har ført til forskellige kategorier af ikkeklassificerede informationer, forskellige mærkninger og forskellige håndteringsinstrukser over hele linjen. For så vidt angår EUCI er de relevante systemers interoperabilitet fortsat begrænset, og det forhindrer gnidningsløs overførsel af informationer mellem EU's institutioner og organer og med medlemsstaterne.

Situationen øger risikoen for at angribere skaber et brud på sikkerheden ved det svageste led og anvender dette som udgangspunkt for yderligere angreb på andre EU-institutioner og -organer.

C. Hvilke resultater skal der opnås?

Det generelle mål med dette initiativ er at fastsætte informationssikkerhedsregler, der er fælles for alle EU's institutioner og organer, med henblik på at sikre øget og konsekvent beskyttelse mod de foranderlige trusler mod deres informationer.

Det generelle mål omsættes til fire specifikke mål:

- Oprette harmoniserede og dækkende informationskategorier.
- Identificere sikkerhedshuller og gennemføre de nødvendige foranstaltninger.
- Oprette en lean-samarbejdsordning om informationssikkerhed mellem EU's institutioner og organer.
- Modernisere informationssikkerhedspolitikkerne, idet der tages højde for den digitale omstilling og

telearbejde.

D. Hvad er de forskellige interessenters synspunkter?

De hørte interessenter (EU's institutioner og organer, medlemsstaternes nationale sikkerhedsmyndigheder og forskningseksperter fra Det Fælles Forskningscenter) var enige om, at der er behov for fælles standarder for informationssikkerhed for alle EU's institutioner og organer, idet der bør fokuseres på følgende:

- Der bør tages højde for mangfoldigheden og de forskellige forretningsmiljøer i hver EU-institution og -organ, og lokale løsninger bør være tilladt.
- Størstedelen af EU's institutioner og organer er parate til at samarbejde med deres modparter i fælles organer med henblik på informationssikkerhed, men de er ikke villige til at uddelegere deres beslutningskompetence.
- Et forslag til forordning bør udarbejdes under hensyntagen til den mellemstatslige aftale[1] mellem medlemsstaterne om beskyttelse af klassificerede informationer.

E. Hvad er virkningen af forslaget?

Fordele

Ved at etablere et referencescenarie for informationssikkerhedsregler på tværs af EU's institutioner og organer øger forslaget til forordning det samlede informationssikkerhedsniveau og reducerer de nuværende antal uoverensstemmelser. Det forventes også bidrage til at eliminere potentielle svage led og beskytte de informationer, der deles i den europæiske forvaltning.

Set ud fra et effektivitetssynspunkt bør forslaget til forordning føre til gevinster fra den koordinerede udførelse af fælles informationssikkerhedsopgaver (f.eks. godkendelser, akkreditering af CIS'er) og oprettelsen af fælles forvaltningsorganer (f.eks. den interinstitutionelle koordinationsgruppe, de tekniske undergrupper).

Finansiel virkning

For så vidt angår EU's institutioner og organer forventes den indsats, der er nødvendig i forbindelse med gennemførelsen af den nye lovgivning, at blive opvejet af effektivitetsgevinsterne, mens ekstra omkostninger kan dækkes via de eksisterende programmer til forbedring af informationssikkerheden i hver enhed. På lang sigt vil de drage fordel af den sammenhængende tilgang til håndteringen af de foranderlige trusler mod informationssikkerheden.

Europa-Kommissionen bør sikre koordinationsgruppen om informationssikkerheds permanente sekretariat og tildele menneskelige ressourcer til denne opgave (en AD-stilling og en AST-stilling).

Der forventes ingen finansiel virkning for medlemsstaternes forvaltninger eller for den private sektor.

[1] Aftale mellem Den Europæiske Unions medlemsstater, forsamlet i Rådet, om beskyttelse af klassificerede informationer, der udveksles i Den Europæiske Unions interesse (EUT C 202 af 8.7.2011, s. 13).

F. Opfølgning
Hvornår vil foranstaltningen blive taget op til fornyet overvejelse?
Der foretages en fuld evaluering hvert femte år fra datoen for anvendelsen med henblik på at vurdere virkningerne og gennemførelsen af forslaget til forordning. Kommissionen fremlægger en rapport om resultaterne heraf og fremsender den til Europa-Parlamentet og Rådet.