Europeiska unionens råd

Bryssel den 29 mars 2022
(OR. en)

7670/22
ADD 7

Interinstitutionellt ärende:
2022/0084(COD)

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

FÖLJENOT

från:	Europeiska kommissionens generalsekreterare, undertecknat av Martine DEPREZ, direktör
inkom den:	22 mars 2022
till:	Jeppe TRANHOLM-MIKKELSEN, generalsekreterare för Europeiska unionens råd
Komm. dok. nr:	SWD(2022) 65 final
Ärende:	ARBETSDOKUMENT FRÅN KOMMISSIONENS AVDELNINGAR SAMMANFATTNING AV KONSEKVENSBEDÖMNINGSRAPPORTEN Följedokument till förslag till Europaparlamentets och rådets förordning om informationssäkerhet i unionens institutioner, organ och byråer

För delegationerna bifogas dokument – SWD(2022) 65 final.

Bilaga: SWD(2022) 65 final

EUROPEISKA
KOMMISSIONEN

Bryssel den 22.3.2022
SWD(2022) 65 final

ARBETSDOKUMENT FRÅN KOMMISSIONENS AVDELNINGAR

SAMMANFATTNING AV KONSEKVENSBEDÖMNINGSRAPPORTEN

Följedokument till

förslag till Europaparlamentets och rådets förordning

om informationssäkerhet i unionens institutioner, organ och byråer

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

Sammanfattning

Konsekvensanalys av informationssäkerheten vid unionens institutioner, organ och byråer

A. Politisk bakgrund

I Europeiska rådets strategiska agenda för 2019–2024 uppmanas institutionerna att skydda EU:s informations- och kommunikationsnät och dess beslutsprocesser från skadlig verksamhet av alla slag, inbegripet cyberhot och hybridhot. Till följd av detta konstaterade rådet (allmänna frågor) i december 2019 att EU:s institutioner och organ bör utarbeta och genomföra en omfattande uppsättning åtgärder för att säkerställa sin informationssäkerhet.

I juli 2020 antog kommissionen sin strategi för EU:s säkerhetsunion, genom vilken den åtog sig att komplettera de nationella insatserna på säkerhetsområdet. Som en del av denna strategi föreslog kommissionen att man skulle skapa en minimiuppsättning regler för informationssäkerhet och cybersäkerhet för alla unionens institutioner och organ.

B. Vad är problemet?

De största problemen är i) betydande skillnad mellan säkerhetsnivån för unionens institutioner och organ beroende på deras interna informationssäkerhetsregler och ii) bristande samordning mellan unionens institutioner och organ när de utför sina säkerhetsuppgifter.

Unionens institutioner och organ har för närvarande sina egna informationssäkerhetsregler eller har inte antagit sådana regler alls. Den tillämpliga rättsliga ramens fragmentering har lett till att det finns olika kategorier av icke-säkerhetsskyddsklassificerade uppgifter, olika märkningar och olika hanteringsanvisningar över hela linjen. När det gäller säkerhetsskyddsklassificerade EU-uppgifter är interoperabiliteten mellan de relevanta systemen fortfarande begränsad, vilket förhindrar en smidig överföring av uppgifter mellan institutioner och organ och med medlemsstaterna.

Denna situation ökar risken för att angripare skapar en säkerhetsöverträdelse i den svagaste länken och använder detta som utgångspunkt för ytterligare attacker mot andra institutioner eller organ.

C. Vad bör uppnås?

Det allmänna syftet med initiativet är att skapa informationssäkerhetsregler för alla unionens institutioner och organ i syfte att säkerställa ett förstärkt och konsekvent skydd mot framväxande hot mot deras information.

Det allmänna målet omsätts i fyra specifika mål:

- Fastställa harmoniserade och heltäckande informationskategorier.
- Identifiera säkerhetsbrister och genomföra de åtgärder som krävs.
- Upprätta ett smidigt samarbete om informationssäkerhet mellan unionens institutioner och organ.
- Modernisera informationssäkerhetspolitiken med beaktande av den digitala omvandlingen och distansarbetet.

D. Vilka är de olika intressenternas åsikter?

De berörda parter som rådfrågats (unionens institutioner och organ, medlemsstaternas nationella säkerhetsmyndigheter och forskningsexperter från JRC) var eniga om behovet av gemensamma standarder för informationssäkerhet för alla unionens institutioner och organ, med fokus på följande punkter:

- Mångfalden och de olika företagsklimateten i unionens institutioner och organ bör beaktas och lokala lösningar bör tillåtas.
- De flesta institutioner och organ är beredda att samarbeta med sina motsvarigheter i gemensamma organ för informationssäkerhetsändamål, men de är inte villiga att delegera sina beslutsbefogenheter.
- Utkastet till förordning bör utarbetas med beaktande av medlemsstaternas mellanstatliga avtal[1] om skydd av säkerhetsskyddsklassificerade uppgifter.

E. Vilka konsekvenser har förslaget?

Fördelar

Genom att skapa en baslinje för informationssäkerhetsregler inom unionens institutioner och organ kommer utkastet till förordning att öka de övergripande informationssäkerhetsnivåerna och samtidigt minska de nuvarande skillnaderna. Detta bör också bidra till att undanröja potentiella svaga länkar och samtidigt skydda den information som delas inom den europeiska förvaltningen.

Ur effektivitetssynpunkt bör utkastet till förordning leda till vinster genom det samordnade utförandet av gemensamma informationssäkerhetsuppgifter (t.ex. godkännande, ackreditering av kommunikations- och informationssystem) och inrättandet av gemensamma styrande organ (t.ex. den interinstitutionella samordningsgruppen, de tekniska undergrupperna).

Ekonomiska konsekvenser

För unionens institutioner och organ förväntas de ansträngningar som krävs för att genomföra den nya lagstiftningen kompenseras av effektivitetsvinster, medan ytterligare kostnader kan täckas inom ramen för varje organisations befintliga program för förbättrad informationssäkerhet. På lång sikt kommer de att gynnas av den konsekventa strategin för att hantera de ständigt föränderliga hoten mot informationssäkerheten.

Europeiska kommissionen bör ombesörja det ständiga sekretariatet för den interinstitutionella samordningsgruppen och anslå personalresurser för denna uppgift (en AD-tjänsteman och en AST-tjänsteman).

Inga ekonomiska konsekvenser förväntas för medlemsstaternas förvaltningar och den privata sektorn.

D. Uppföljning

När kommer åtgärderna att ses över?

En fullständig utvärdering kommer att göras vart femte år efter tillämpningsdatumet för att bedöma

[1] Avtal mellan Europeiska unionens medlemsstater, församlade i rådet, om skydd av säkerhetsskyddsklassificerade uppgifter som utbyts i Europeiska unionens intresse, 2011/C202/05.

konsekvenserna och genomförandet av utkastet till förordning. Kommissionen ska lägga fram en rapport med sina resultat och överlämna den till Europaparlamentet och rådet.