Raad van de
Europese Unie

Brussel, 29 maart 2022
(OR. en)

7670/22
ADD 7

Interinstitutioneel dossier:
2022/0084(COD)

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

BEGELEIDENDE NOTA

van:	de secretaris-generaal van de Europese Commissie, ondertekend door mevrouw Martine DEPREZ, directeur
ingekomen:	22 maart 2022
aan:	de heer Jeppe TRANHOLM-MIKKELSEN, secretaris-generaal van de Raad van de Europese Unie
nr. Comdoc.:	SWD(2022) 65 final
Betreft:	WERKDOCUMENT VAN DE DIENSTEN VAN DE COMMISSIE SAMENVATTING VAN HET EFFECTBEOORDELINGSVERSLAG bij het Voorstel voor een VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD betreffende informatiebeveiliging in de instellingen, organen en instanties van de Unie

Hierbij gaat voor de delegaties document SWD(2022) 65 final.

Bijlage: SWD(2022) 65 final

EUROPESE
COMMISSIE

Brussel, 22.3.2022
SWD(2022) 65 final

WERKDOCUMENT VAN DE DIENSTEN VAN DE COMMISSIE

SAMENVATTING VAN HET EFFECTBEOORDELINGSVERSLAG

bij het

Voorstel voor een VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD

betreffende informatiebeveiliging in de instellingen, organen en instanties van de Unie

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

Samenvatting

Effectbeoordeling inzake informatiebeveiliging in de instellingen, organen en instanties van de Unie

A. Politieke context

In de strategische agenda van de Europese Raad voor 2019-2024 worden de instellingen opgeroepen de informatie- en communicatienetwerken van de EU en haar besluitvormingsprocessen te beschermen tegen kwaadwillige activiteiten van allerlei aard, waaronder cyber- en hybride dreigingen. Bijgevolg concludeerde de Raad Algemene Zaken van december 2019 dat de instellingen en organen van de EU een uitgebreide reeks maatregelen moeten uitwerken en toepassen om hun informatiebeveiliging te waarborgen.

In juli 2020 heeft de Commissie de EU-strategie voor de veiligheidsunie vastgesteld, waarin zij zich ertoe verbond de nationale inspanningen op het gebied van veiligheid aan te vullen. In het kader van deze strategie heeft de Commissie voorgesteld een minimumpakket regels inzake informatiebeveiliging en cyberbeveiliging vast te stellen voor alle instellingen en organen van de Unie.

B. Wat is het probleem?

De belangrijkste problemen zijn: i) een aanzienlijk verschil tussen het beveiligingsniveau van de instellingen en organen van de Unie, afhankelijk van hun interne regels inzake informatiebeveiliging, en ii) een gebrek aan coördinatie tussen de instellingen en organen van de Unie bij de uitvoering van hun beveiligingstaken.

De instellingen en organen van de Unie hebben momenteel hun eigen regels inzake informatiebeveiliging of hebben dergelijke regels helemaal niet vastgesteld. De versnippering van het toepasselijke rechtskader heeft geleid tot verschillende categorieën niet-gerubriceerde informatie, verschillende markeringen en verschillende verwerkingsinstructies over de hele linie. Wat gerubriceerde EU-informatie betreft, blijft de interoperabiliteit van de relevante systemen beperkt, waardoor een naadloze overdracht van informatie tussen instellingen en organen en met de lidstaten wordt verhinderd.

Deze situatie vergroot het risico dat aanvallers in de zwakste schakel een beveiligingsinbreuk veroorzaken en dit als uitgangspunt gebruiken voor verdere aanvallen op andere instellingen of organen.

C. Wat moet er worden bereikt?

De algemene doelstelling van het initiatief is het opstellen van regels voor informatiebeveiliging voor alle instellingen en organen van de Unie met het oog op een betere en consistente bescherming tegen de zich ontwikkelende informatiedreigingen.

De algemene doelstelling wordt vertaald in vier specifieke doelstellingen:

- geharmoniseerde en omvattende categorieën informatie vaststellen;
- lacunes in de beveiliging in kaart brengen en de vereiste maatregelen uitvoeren;
- een vlotte samenwerking inzake informatiebeveiliging tussen de instellingen en organen van de Unie bewerkstelligen;
- het beleid inzake informatiebeveiliging moderniseren, rekening houdend met de digitale

transformatie en telewerken.

D. Wat zijn de standpunten van de verschillende belanghebbenden?

De geraadpleegde belanghebbenden (instellingen en organen van de Unie, nationale veiligheidsinstanties van de lidstaten en onderzoeksdeskundigen van het JRC) waren het eens over de noodzaak van gemeenschappelijke normen voor informatiebeveiliging voor alle instellingen en organen van de Unie, met bijzondere aandacht voor de volgende punten:

- er moet rekening worden gehouden met de diversiteit en het verschillende bedrijfsklimaat van elke instelling en elk orgaan van de Unie en lokale oplossingen moeten mogelijk zijn;
- de meeste instellingen en organen zijn bereid samen te werken met hun tegenhangers in gemeenschappelijke organen voor informatiebeveiligingsdoeleinden, maar zijn niet bereid hun besluitvormingsbevoegdheden te delegeren;
- de ontwerpverordening moet worden opgesteld met inachtneming van de intergouvernementele overeenkomst[1] van de lidstaten over de bescherming van gerubriceerde informatie.

E. Wat is het effect van het voorstel?

Voordelen

Door voor alle instellingen en organen van de Unie een basis van informatiebeveiligingsregels te creëren, zal de ontwerpverordening het algemene niveau van informatiebeveiliging verhogen en tegelijkertijd de huidige discrepanties verkleinen. Het voorstel moet ook helpen om potentiële zwakke schakels weg te werken en tegelijkertijd de binnen de Europese administratie gedeelde informatie te beschermen.

Vanuit het oogpunt van efficiëntie moet de ontwerpverordening voordelen opleveren door een gecoördineerde uitvoering van gemeenschappelijke taken op het gebied van informatiebeveiliging (bv. machtigingen, accreditatie van communicatie- en informatiesystemen) en de oprichting van gemeenschappelijke bestuursorganen (bv. de interinstitutionele coördinatiegroep, de technische subgroepen).

Economische gevolgen

Voor de instellingen en organen van de Unie zullen de inspanningen die nodig zijn om de nieuwe wetgeving uit te voeren, naar verwachting worden gecompenseerd door de efficiëntiewinst, terwijl extra kosten kunnen worden gedekt door de bestaande programma's ter verbetering van de informatiebeveiliging van elke organisatie. Op de lange termijn zullen zij baat hebben bij een coherente aanpak van de steeds veranderende bedreigingen van de informatiebeveiliging.

De Europese Commissie moet zorgen voor het permanente secretariaat van de interinstitutionele coördinatiegroep en voor deze taak personele middelen toewijzen (één AD-ambtenaar en één AST-ambtenaar).

[1]Overeenkomst tussen de lidstaten van de Europese Unie, in het kader van de Raad bijeen, betreffende de bescherming van in het belang van de Europese Unie uitgewisselde gerubriceerde informatie (PB C 202 van 8.7.2011, blz. 13).

Er worden geen economische gevolgen verwacht op het niveau van de overheden van de lidstaten en de particuliere sector.
F. Follow-up
Wanneer wordt dit beleid geëvalueerd?
Om de 5 jaar na de datum van toepassing zal een volledige evaluatie worden uitgevoerd om de effecten en de uitvoering van de ontwerpverordening te beoordelen. De Commissie presenteert een verslag met haar bevindingen en dient dit in bij het Europees Parlement en de Raad.