



Raad van de
Europese Unie

Brussel, 29 maart 2022
(OR. en)

**Interinstitutioneel dossier:
2022/0084 (COD)**

7670/22
ADD 1

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

VOORSTEL

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.:	COM(2022) 119 final - Annex I
Betreft:	BIJLAGE 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 COM(2022) 119 final - Annex I.

Bijlage: COM(2022) 119 final - Annex I



Brussel, 22.3.2022
COM(2022) 119 final

ANNEX 1

BIJLAGE

bij het

Voorstel voor een VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD

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

{SWD(2022) 65 final} - {SWD(2022) 66 final}

BIJLAGE I

Beschermingsmaatregelen voor de verwerking van gevoelige niet-gerubriceerde informatie

Markering en verwerking van gevoelige niet-gerubriceerde informatie

1. Documenten die gevoelige niet-gerubriceerde informatie bevatten, moeten worden voorzien van een beveiligingsmarkering en, in voorkomend geval, een of meer verspreidingsmarkeringen of markeringen die de doelgroep aangeven. De standaardveiligheidsmarkering is het woord “SENSITIVE” in hoofdletters, behalve in de in artikel 15, lid 2, bedoelde gevallen.
2. Documenten die gevoelige niet-gerubriceerde informatie bevatten, mogen slechts toegankelijk zijn voor ontvangers met noodzaak tot kennisneming voor officiële doeleinden. Wanneer verspreidingsmarkeringen worden gebruikt, moet de instelling of het orgaan van de Unie waarvan de informatie afkomstig is, om toestemming worden gevraagd om het document verder te verspreiden.
3. Alle personen die gevoelige niet-gerubriceerde informatie verwerken, moeten op de hoogte worden gesteld van de verwerkingsinstructies.
4. Wanneer documenten als SENSITIVE zijn gemarkeerd, wordt de rubriceringsgraad verlaagd tot EU NORMAL of PUBLIC USE door verwijdering of doorhaling van de markeringen.
5. Wanneer de instellingen en organen van de Unie documenten met gevoelige niet-gerubriceerde informatie vernietigen, moet dit zodanig gebeuren dat zij niet gemakkelijk kunnen worden gereconstrueerd. Papieren exemplaren moeten worden versnipperd en elektronische kopieën moeten veilig worden overschreven, fysiek worden vernietigd of op een andere wijze onherstelbaar worden gemaakt.

Bescherming van gevoelige niet-gerubriceerde informatie bij werkzaamheden buiten de locaties van de instellingen en organen van de Unie

6. Gevoelige niet-gerubriceerde informatie moet worden beschermd tegen af luisteren en observatie tijdens telewerken en missies buiten het kantoor, en mag niet in het openbaar worden verwerkt of opgeslagen.
7. Documenten die gevoelige niet-gerubriceerde informatie bevatten, mogen alleen worden verwerkt en opgeslagen op apparatuur of met toepassingen die onder de verantwoordelijkheid van de instellingen en organen van de Unie op passende wijze beveiligd zijn.
8. De instellingen en organen van de Unie moeten middelen ter beschikking stellen om te voorkomen dat onbevoegden, onder wie familie- en gezinsleden, toegang krijgen tot gevoelige niet-gerubriceerde informatie die met apparatuur van een instelling of orgaan van de Unie wordt verwerkt of opgeslagen, wanneer personeelsleden buiten hun standplaats werken.
9. De instellingen en organen van de Unie moeten hun personeelsleden instrueren om:
 - a) apparatuur van de instellingen of organen van de Unie waarmee gevoelige niet-gerubriceerde informatie wordt verwerkt, te beschermen tegen diefstal, verlies en beschadiging, en alle beveiligingsincidenten die nadelige gevolgen hebben voor de apparatuur of de daarin vervatte informatie, onmiddellijk te melden;

- b) hun apparatuur niet te delen met onbevoegden;
 - c) de apparatuur niet te gebruiken voor activiteiten die geen verband houden met hun werkzaamheden.
10. De instellingen en organen van de Unie moeten waarborgen dat voor de verwerking en opslag van gevoelige niet-gerubriceerde documenten in elektronische vorm buiten hun locaties zoveel mogelijk gebruikt wordt gemaakt van hun apparatuur of hun naar behoren beveiligde toepassingen. De verwerking van fysieke kopieën van gevoelige niet-gerubriceerde documenten buiten het kantoor moet worden vermeden.
11. Wanneer gebruik wordt gemaakt van teleconferentie- of videoconferentievoorzieningen, moeten de instellingen en organen van de Unie het risico dat onbevoegden de besprekingen kunnen zien of horen tot een minimum beperken, door de deelnemers op passende wijze te authenticeren en gebruik te maken van versleutelde communicatiemiddelen die verenigbaar zijn met de noodzaak tot kennisneming.
12. De instellingen en organen van de Unie leiden al het personeel dat op afstand werkt op met betrekking tot de verwerking van gevoelige niet-gerubriceerde informatie wanneer zij buiten het kantoor werken.

Delen van gevoelige niet-gerubriceerde informatie

13. Documenten die gevoelige niet-gerubriceerde informatie bevatten, kunnen zonder bijkomende formaliteiten met instellingen en organen van de Unie worden gedeeld.
14. De instellingen en organen van de Unie mogen documenten die gevoelige niet-gerubriceerde informatie bevatten slechts delen met ontvangers buiten de instellingen en organen van de Unie indien de ontvanger zich ertoe verbindt de verwerkingsinstructies na te leven.
15. De instellingen en organen van de Unie moeten ontvangers van gevoelige niet-gerubriceerde informatie in kennis stellen van de verplichting om de informatie niet te delen met partijen buiten de door de verspreidingsmarkeringen aangegeven doelgroep, tenzij de auteur zulks toestaat.
16. De instellingen en organen van de Unie moeten gevoelige niet-gerubriceerde informatie die langs elektronische weg wordt verstrekt of uitgewisseld, beschermen met passende beveiligingsmaatregelen, waaronder versleuteling bij verzending door middel van passende cryptografische mechanismen.