REGLEMENTEN VAN ORDE EN REGLEMENTEN VOOR DE PROCESVOERING

BESLUIT Nr. 41/2021 VAN DE REKENKAMER

betreffende de veiligheidsvoorschriften voor de bescherming van gerubriceerde EU-informatie (EUCI)

DE EUROPESE REKENKAMER,

Gelet op artikel 13 van het Verdrag betreffende de Europese Unie,

Gelet op artikel 287 van het Verdrag betreffende de werking van de Europese Unie,

Gelet op artikel 257 van Verordening (EU, Euratom) 2018/1046 van het Europees Parlement en de Raad van 18 juli 2018 tot vaststelling van de financiële regels van toepassing op de algemene begroting van de Unie,

Gelet op artikel 1, lid 6, van de uitvoeringsvoorschriften bij het reglement van orde van de Rekenkamer (Besluit nr. 21/2021 van de Rekenkamer),

Gelet op de veiligheidsvoorschriften voor de bescherming van gerubriceerde EU-informatie van de andere instellingen, organen en instanties van de EU,

Gelet op het informatiebeveiligingsbeleid (DEC 127/15 FINAL) en het informatierubriceringsbeleid (Personeelsmededeling nr. 123/2020) van de Rekenkamer,

Overwegende hetgeen volgt:

(1) Overeenkomstig artikel 287, lid 3, VWEU heeft de Rekenkamer recht op toegang tot alle relevante documenten en informatie die zij nodig acht voor de uitvoering van haar mandaat, met inbegrip van gerubriceerde EU-informatie (EUCI), dat moet worden vervuld met volledige inachtneming van het beginsel van loyale samenwerking tussen de instellingen en het beginsel van bevoegdheidstoedeling; dat recht op toegang tot EUCI, verankerd in het VWEU, kan niet ter discussie worden gesteld door de bron van EUCI, terwijl de Rekenkamer kan worden verzocht bepaalde veiligheidsmaatregelen in te voeren en na te leven, zoals hieronder nader wordt beschreven.

(2) De leden van de Rekenkamer en haar ambtenaren en ander personeel zijn zelfs na beëindiging van de dienst gebonden aan een geheimhoudingsplicht uit hoofde van artikel 339 VWEU, artikel 17 van het Statuut en de op grond daarvan vastgestelde handelingen.

(3) Gezien de gevoelige aard ervan vereist de behandeling van EUCI dat de naleving van de geheimhoudingsplicht wordt gewaarborgd door middel van passende veiligheidsmaatregelen die een hoog beschermingsniveau voor die informatie kunnen waarborgen en die gelijkwaardig zijn aan die welke zijn vastgelegd in de voorschriften inzake de bescherming van EUCI die zijn vastgesteld door de andere instellingen, organen en instanties van de EU, met dien verstande dat, indien de Rekenkamer van oordeel is dat dergelijke veiligheidsmaatregelen niet gerechtvaardigd zijn in het licht van de aard en het soort EUCI, de Rekenkamer zich het recht voorbehoudt opmerkingen te maken die zij passend acht, met inachtneming van de rubriceringsgraad van EUCI.

(4) De veiligheidsmaatregelen ter bescherming van de vertrouwelijkheid, integriteit en beschikbaarheid van de aan de Rekenkamer verstrekte informatie moeten zijn afgestemd op de aard en het soort informatie in kwestie.

(5) De toegang tot gerubriceerde informatie aan de Rekenkamer moet worden verleend volgens het beginsel van noodzaak tot kennisname met het oog op de uitvoering van de taken die haar zijn toevertrouwd bij de Verdragen en bij op grond van de Verdragen vastgestelde rechtshandelingen.

(6) Gezien de aard en de gevoelige inhoud van bepaalde informatie is het passend om een speciale procedure vast te stellen voor de behandeling van documenten met EUCI door de Rekenkamer.

(7) De instelling moet ervoor zorgen dat dit besluit wordt uitgevoerd overeenkomstig alle toepasselijke voorschriften, met name de bepalingen inzake de bescherming van persoonsgegevens, de fysieke veiligheid van personen, gebouwen en IT, en de toegang van het publiek tot documenten,

BESLUIT:

Artikel 1

Onderwerp en toepassingsgebied

1. In dit besluit worden de basisbeginselen en minimumveiligheidsnormen vastgesteld voor de bescherming van gerubriceerde informatie die de Rekenkamer behandelt bij de uitoefening van haar mandaat.

2. Voor de toepassing van dit besluit wordt onder gerubriceerde informatie een of alle van de onderstaande soorten informatie verstaan:

a) "gerubriceerde EU-informatie" (EUCI) zoals gedefinieerd in de veiligheidsvoorschriften van andere instellingen, organen of instanties van de EU, die voorzien is van een van de onderstaande rubriceringsmarkeringen:

   — TRÈS SECRET UE/EU TOP SECRET: informatie en materiaal waarvan de ongeoorloofde openbaarmaking de wezenlijke belangen van de Europese Unie of van een of meer van haar lidstaten uitzonderlijk ernstig kan schaden;

   — SECRET UE/EU SECRET: informatie en materiaal waarvan de ongeoorloofde openbaarmaking de wezenlijke belangen van de Europese Unie of van een of meer van haar lidstaten ernstig kan schaden;

   — CONFIDENTIEL UE/EU CONFIDENTIAL: informatie en materiaal waarvan de ongeoorloofde openbaarmaking de wezenlijke belangen van de Europese Unie of van een of meer van haar lidstaten kan schaden;

   — RESTREINT UE/EU RESTRICTED: informatie en materiaal waarvan de ongeoorloofde openbaarmaking nadelig kan zijn voor de belangen van de Europese Unie of van een of meer van haar lidstaten.

b) gerubriceerde informatie die door lidstaten is verstrekt en een nationale rubriceringsmarkering heeft welke gelijkwaardig is aan een van de in punt a) genoemde rubriceringsmarkeringen voor EUCI ([1]);

c) gerubriceerde informatie die door derde landen of internationale organisaties aan de Europese Rekenkamer is verstrekt en een rubriceringsmarkering heeft welke gelijkwaardig is aan een van de in punt a) genoemde rubriceringsmarkeringen voor EUCI, overeenkomstig de betrokken informatiebeveiligingsovereenkomsten of bestuurlijke regelingen.

3. De Rekenkamer behandelt informatie met rubricering RESTREINT UE/EU RESTRICTED op haar locaties en neemt daartoe alle nodige beschermingsmaatregelen. Er worden regelingen getroffen zodat het personeel van de Rekenkamer dat toegang moet krijgen tot EUCI met hogere rubriceringsgraden, dit kan doen op geschikte locaties van andere instellingen, organen en instanties van de EU.

4. Dit besluit is van toepassing op alle diensten en locaties van de Rekenkamer.

5. Behalve wanneer een bepaling betrekking heeft op specifieke categorieën personeel, is dit besluit van toepassing op de leden van de Rekenkamer, het personeel van de Rekenkamer dat valt onder het Statuut en de Regeling welke van toepassing is op de andere personeelsleden van de Europese Unie ([2]), de nationale deskundigen die bij de Rekenkamer zijn gedetacheerd (GND's), de verstrekkers van diensten en hun personeel, stagiairs en alle andere personen die toegang hebben tot de gebouwen en andere eigendommen van de Rekenkamer, of tot informatie die wordt beheerd door de Rekenkamer.

6. Tenzij anders bepaald, zijn de bepalingen inzake EUCI op gelijkwaardige wijze van toepassing op de gerubriceerde informatie als bedoeld in lid 2, punten b) en c), van dit artikel.

([1]) Zie de 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) en de bijlage daarbij.

([2]) Verordening nr. 31 (EEG) tot vaststelling van het Statuut van de ambtenaren en de Regeling welke van toepassing is op de andere personeelsleden, zoals gewijzigd (PB 45 van 14.6.1962, blz. 1385/62) (https://eur-lex.europa.eu/eli/reg/1962/31 (1)/2020-01-01).

Artikel 2

Definities

Voor de toepassing van dit besluit wordt verstaan onder:

a) "machtiging tot toegang tot EUCI": een besluit van de directeur Personeelszaken, Financiën en Algemene Diensten van de Rekenkamer op grond van een van een bevoegde autoriteit van een lidstaat verkregen zekerheid dat een ambtenaar van de Rekenkamer, een ander personeelslid of een GND, mits zijn/haar noodzaak tot kennisname is vastgesteld en hij/zij op passende wijze in kennis is gesteld van zijn/haar verantwoordelijkheden, tot een bepaalde rubriceringsgraad (CONFIDENTIEL UE/EU CONFIDENTIAL of hoger) en tot een bepaalde datum toegang wordt verleend tot EUCI; van die persoon wordt dan gezegd dat hij/zij "gemachtigd" is;

b) "rubricering": de toekenning van een rubriceringsgraad aan informatie op basis van de mate waarin schade kan worden berokkend door de ongeoorloofde openbaarmaking ervan;

c) "encryptiemateriaal": encryptiealgoritmen, hard- en softwaremodules voor encryptie en encryptieproducten, inclusief nadere informatie betreffende de uitvoering en bijbehorende documentatie en bedieningsmateriaal;

d) "derubricering": de opheffing van een rubricering;

e) "document": opgeslagen informatie, ongeacht de vorm of fysieke kenmerken ervan;

f) "lagere rubricering": verlaging van de rubriceringsgraad;

g) "veiligheidsverklaring voor een vestiging": een administratieve beslissing van een bevoegde veiligheidsautoriteit waaruit blijkt dat de vestiging vanuit beveiligingsoogpunt een afdoend niveau van bescherming biedt voor EUCI met een bepaalde rubriceringsgraad;

h) "behandeling": alle mogelijke handelingen waaraan EUCI tijdens de gehele levenscyclus kan worden onderworpen: het genereren, de registratie, het verwerken, het vervoer, lagere rubricering, derubricering, en de vernietiging van de informatie. Met betrekking tot communicatie- en informatiesystemen (Communication and Information Systems — CIS) behoren hiertoe ook het verzamelen, tonen, overdragen en opslaan van de informatie;

i) "houder": een naar behoren gemachtigde persoon van wie de noodzaak tot kennisname vaststaat en die gerubriceerde informatie in zijn bezit heeft en derhalve voor de bescherming daarvan verantwoordelijk is;

j) "autoriteit voor informatiebeveiliging": de functionaris voor informatiebeveiliging van de Rekenkamer, die de in dit besluit vastgestelde taken geheel of gedeeltelijk kan delegeren;

k) "informatie": elke schriftelijke of mondelinge informatie, ongeacht het medium of de auteur;

l) "materiaal": een medium, gegevensdrager of enigerlei onderdeel van machines of uitrustingen;

m) "bron": de instelling, het agentschap of orgaan van de EU, of de lidstaat, het derde land of de internationale organisatie onder het gezag waarvan informatie is gegenereerd en/of ingevoerd in de structuren van de EU;

n) "veiligheidsverklaring voor personeel" (PSC): een verklaring van een bevoegde autoriteit van een lidstaat, die wordt afgelegd na voltooiing van een veiligheidsonderzoek door de bevoegde autoriteiten van een lidstaat, waarbij wordt bevestigd dat de betrokkene, mits zijn noodzaak tot kennisname is vastgesteld en hij/zij terdege is geïnstrueerd over zijn verantwoordelijkheden, tot een bepaalde datum toegang kan krijgen tot EUCI tot op een bepaald niveau (CONFIDENTIEL UE/EU CONFIDENTIAL of hoger);

o) "certificaat van veiligheidsverklaring voor personeel" (PSCC): een door de directeur Personeelszaken, Financiën en Algemene Diensten van de Rekenkamer afgegeven certificaat waarin wordt bevestigd dat een betrokkene in het bezit is van een geldige veiligheidsverklaring of veiligheidsmachtiging, en dat de rubriceringsgraad vermeldt van EUCI waartoe hij/zij toegang mag hebben (CONFIDENTIEL UE/EU CONFIDENTIAL of hoger), alsook de geldigheidsduur van die veiligheidsverklaring of -machtiging en de datum waarop de geldigheid van het certificaat zelf afloopt;

p) "autoriteit voor fysieke veiligheid": het hoofd van de veiligheidsdienst van de Rekenkamer, dat verantwoordelijk is voor de uitvoering van de nodige maatregelen en procedures voor fysieke veiligheid ter bescherming van EUCI;

q) "archief": wordt beheerd door het secretariaat van de Rekenkamer en is ondergebracht in een administratieve zone onder de verantwoordelijkheid van de directeur Personeelszaken, Financiën en Algemene Diensten van de Rekenkamer. Het is verantwoordelijk voor het in- en uitgaan van informatie met rubricering RESTREINT UE/EU RESTRICTED, of het equivalent daarvan, die/dat wordt uitgewisseld met de Rekenkamer;

r) "EUCI-register": een zone binnen een beveiligde zone. Dit register wordt beheerd door de registercontrolefunctionaris van de Rekenkamer, die over een veiligheidsverklaring en -machtiging beschikt. Het is verantwoordelijk voor het in- en uitgaan van informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of hoger, of het equivalent daarvan, die/dat wordt uitgewisseld met de Rekenkamer;

s) "veiligheidshomologatieautoriteit (SAA)": de directeur Personeelszaken, Financiën en Algemene Diensten van de Rekenkamer.

Artikel 3

Maatregelen ter bescherming van EUCI

1. De Rekenkamer waarborgt de bescherming van alle gerubriceerde informatie die haar wordt verstrekt op een wijze die in verhouding staat tot het door de bron vastgestelde rubriceringsniveau, en in overeenstemming met dit besluit.

2. Daartoe stelt de Rekenkamer de behandeling van EUCI afhankelijk van fysieke en, in voorkomend geval, personeelsgerelateerde veiligheidsmaatregelen, met inbegrip van machtigingen tot toegang voor de geïdentificeerde personen en maatregelen ter bescherming van communicatie- en informatiesystemen. Deze maatregelen worden beschreven in de artikelen 4, 5 en 6 en zijn van toepassing gedurende de gehele levenscyclus van de EUCI. Deze maatregelen dienen evenredig te zijn met de rubricering van de EUCI, de vorm en de omvang van de informatie of het materiaal, de locatie en constructie van de faciliteiten waar de EUCI in is ondergebracht en de lokaal beoordeelde dreiging of kwaadwillige en/of criminele activiteiten, met inbegrip van spionage, sabotage en terrorisme.

3. EUCI wordt beschermd door middel van fysieke veiligheidsmaatregelen en informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of hoger wordt ook beschermd door middel van personeelsgerelateerde veiligheidsmaatregelen.

4. EUCI mag alleen worden verstrekt aan personen met een noodzaak tot kennisname binnen de instelling. De houder van enige EUCI moet deze beschermen overeenkomstig dit besluit.

5. EUCI mag niet mondeling of schriftelijk openbaar worden gemaakt. De preliminaire opmerkingen, verslagen, adviezen, persberichten en andere producten van de Rekenkamer, haar website en intranet, mondelinge opmerkingen, antwoorden op verzoeken om toegang tot documenten ([3]) en spraak- of video-opnamen mogen geen EUCI of uittreksels daarvan bevatten en er niet naar verwijzen. Indien de bron documenten of informatie met een verwijzing naar EUCI heeft gepubliceerd, mag die verwijzing evenwel worden vermeld.

6. Niettegenstaande lid 5 kunnen de Rekenkamer en de bron overeenkomen dat de Rekenkamer in geval van een specifieke controle elementen van EUCI mag overnemen of gebruiken in een document. In dat geval wordt dat document van de Rekenkamer eerst vóór of tijdens de contradictoire procedure voorgelegd aan de bron van de EUCI in kwestie. In deze situatie bereiken de Rekenkamer en de bron overeenstemming over de vraag of het door de Rekenkamer uitgebrachte document al dan niet moet worden gerubriceerd. Wanneer een rapporterend lid van de Rekenkamer het noodzakelijk acht een controleverslag dat geheel of gedeeltelijk is gerubriceerd, aan bepaalde geadresseerden van het Europees Parlement of de Raad voor te leggen — rekening houdend met alle veiligheidsmaatregelen uit hoofde van dit besluit — moet de bron van de gerubriceerde informatie hiervoor toestemming geven. Het rechtskader en de procedure voor de uitwisseling van dergelijke documenten zijn vastgesteld in artikel 7.

7. Wanneer de uitoefening van haar mandaat vereist dat bepaalde elementen van een gerubriceerd document of gerubriceerde informatie op grotere schaal worden gedeeld, raadpleegt de Rekenkamer, door terdege rekening te houden met de rubriceringsmarkering, de bron voordat zij besluit die elementen of informatie te gebruiken, indien zij van oordeel is dat dit een hoger openbaar belang dient. De informatie wordt in het verslag alleen op zodanige wijze gebruikt dat de belangen van de bron niet kunnen worden geschaad. Dit zou op passende wijze kunnen worden gewaarborgd door de bron te verzoeken opmerkingen te maken om overeenstemming te bereiken over de wijze waarop de informatie kan worden geanonimiseerd, ingekort of veralgemeend enz., en tegelijkertijd de belangen van de voornaamste betrokkenen bij de gepubliceerde informatie te eerbiedigen.

([3]) Overeenkomstig Besluit nr. 12/2005 van de Rekenkamer inzake de toegang van het publiek tot documenten van de Rekenkamer, als gewijzigd bij Besluit nr. 14/2009 (PB C 67 van 20.3.2009, blz. 1).

8. De Rekenkamer verstrekt geen EUCI aan andere instellingen, organen of instanties van de EU, lidstaten, derde landen of internationale organisaties zonder voorafgaande raadpleging en uitdrukkelijke schriftelijke toestemming van de bron.

9. Tenzij de bron van een document met rubricering SECRET UE/EU SECRET of lager beperkingen heeft opgelegd aan het dupliceren of vertalen ervan, mogen dergelijke documenten worden gedupliceerd of vertaald op verzoek van de houder en met inachtneming van de praktische werkinstructies van de autoriteit voor informatiebeveiliging van de Rekenkamer. De veiligheidsmaatregelen die voor het originele document gelden, zijn ook van toepassing op kopieën en vertalingen ervan.

10. Indien de Rekenkamer van oordeel is dat een gerubriceerd document dat zij heeft ontvangen of waartoe zij toegang heeft, een lagere rubricering moet krijgen of gederubriceerd moet worden, raadpleegt zij de bron om deze te verzoeken een lager gerubriceerde of gederubriceerde versie van het document te verstrekken.

Artikel 4

Personeelsgerelateerde veiligheid

1. Uit hoofde van hun functie zijn de leden van de Rekenkamer gemachtigd om toegang te krijgen tot alle EUCI en deel te nemen aan vergaderingen waar EUCI wordt behandeld. De leden worden in kennis gesteld van hun veiligheidsverplichtingen met betrekking tot de bescherming van EUCI en bevestigen schriftelijk dat zij verantwoordelijk zijn voor de bescherming van dergelijke informatie.

2. Personeelsleden van de Rekenkamer, ongeacht of het gaat om ambtenaren, personeelsleden die onder de Regeling welke van toepassing is op de andere personeelsleden vallen, of GND's, krijgen alleen toegang tot EUCI nadat:

i) hun noodzaak tot kennisname is vastgesteld;

ii) zij in kennis zijn gesteld van de veiligheidsvoorschriften voor de bescherming van EUCI en de relevante veiligheidsnormen en -richtsnoeren, en zij schriftelijk hebben bevestigd dat zij verantwoordelijk zijn voor de bescherming van dergelijke informatie;

iii) in het geval van informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of hoger, hun een veiligheidsverklaring en een machtiging tot toegang is verleend.

3. De procedure om te bepalen of een ambtenaar of een ander personeelslid van de Rekenkamer gemachtigd kan worden om toegang te krijgen tot informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of hoger, rekening houdend met de loyaliteit, integriteit en betrouwbaarheid van de betrokkene, en na van de bevoegde autoriteiten van een lidstaat zekerheid te hebben verkregen als bedoeld in artikel 2, punt n), wordt vastgesteld in een overeenkomstig artikel 10, lid 10, vastgesteld gedelegeerd besluit. Besluiten waarbij een machtiging tot toegang wordt verleend, worden genomen door de directeur Personeelszaken, Financiën en Algemene Diensten van de Rekenkamer.

4. De directeur Personeelszaken, Financiën en Algemene Diensten van de Rekenkamer kan PSCC's afgeven met vermelding van de rubriceringsgraad waarvoor betrokkenen toegang kunnen krijgen tot EUCI (CONFIDENTIEL UE/EU CONFIDENTIAL of hoger), de geldigheidsduur van de overeenkomstige machtiging tot toegang en de datum waarop de geldigheid van het PSCC afloopt.

5. Alleen personen met de in lid 2, punt iii), bedoelde machtiging en leden van de Rekenkamer overeenkomstig lid 1 mogen deelnemen aan vergaderingen waar informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of hoger wordt behandeld. De Rekenkamer en de bron stellen per geval de praktische regelingen voor dergelijke vergaderingen vast.

6. De diensten van de Rekenkamer die belast zijn met de organisatie van vergaderingen waarop informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of hoger moet worden behandeld, stellen de autoriteit voor informatiebeveiliging tijdig in kennis van de data, tijdstippen en locaties van vergaderingen, met lijsten van deelnemers.

7. Alle personen die in het bezit zijn van EUCI zonder de vereiste machtiging en/of zonder vastgestelde noodzaak tot kennisname moeten de situatie zo spoedig mogelijk melden aan de autoriteit voor informatiebeveiliging en ervoor zorgen dat de EUCI overeenkomstig dit besluit wordt beschermd.

Artikel 5

Fysieke veiligheidsmaatregelen ter bescherming van gerubriceerde informatie

1. Fysieke beveiliging is het gebruik van fysieke en technische beschermingsmaatregelen om toegang zonder machtiging tot EUCI te voorkomen.

2. Met de fysieke veiligheidsmaatregelen wordt beoogd het binnendringen door list of geweld te verhinderen, acties waarvoor geen toestemming is verleend te ontmoedigen, te verhinderen en op te sporen en op basis van het principe van noodzaak tot kennisname ten aanzien van toegang tot EUCI onderscheid tussen personeelsleden mogelijk te maken. Dergelijke maatregelen worden vastgesteld op basis van een risicobeheersprocedure, overeenkomstig dit besluit.

3. Zones waar EUCI wordt behandeld of opgeslagen, worden regelmatig geïnspecteerd door de bevoegde veiligheidsautoriteit van de Rekenkamer.

4. Voor de behandeling en opslag van EUCI wordt alleen gebruikgemaakt van apparatuur of voorzieningen die voldoen aan de voorschriften die binnen de instellingen, organen en instanties van de EU gelden voor de bescherming van EUCI.

5. Personeelsleden van de Rekenkamer kunnen toegang krijgen tot EUCI met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of hoger, of het equivalent daarvan, in beveiligde zones buiten de gebouwen van de Rekenkamer.

6. De Rekenkamer kan een overeenkomst inzake dienstverleningsniveau sluiten met een andere EU-instelling in Luxemburg om informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of hoger te kunnen behandelen en opslaan in een beveiligde zone van die instelling. Tenzij de bron hier specifiek mee instemt, wordt deze EUCI niet behandeld of opgeslagen in de gebouwen van de Rekenkamer en wordt deze niet gedupliceerd of vertaald door de Rekenkamer.

7. Ontvangen informatie met rubricering RESTREINT UE/EU RESTRICTED wordt geregistreerd door de Rekenkamer. De raadpleging van informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of hoger, of het equivalent daarvan, buiten de gebouwen van de Rekenkamer wordt geregistreerd voor veiligheidsdoeleinden.

8. EUCI met rubricering RESTREINT UE/EU RESTRICTED mag worden opgeslagen in daarvoor geschikt afgesloten kantoormeubilair in een administratieve zone of een beveiligde zone. EUCI met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of SECRET UE/EU SECRET wordt krachtens een overeenkomst inzake dienstverleningsniveau opgeslagen in een beveiligd opbergmiddel in een beveiligde zone van een andere EU-instelling in Luxemburg.

9. Wanneer EUCI zich buiten het register bevindt, wordt deze als volgt tussen afdelingen en locaties overgedragen:

a) EUCI wordt over het algemeen overgedragen met elektronische middelen, beschermd door encryptieproducten die overeenkomstig artikel 6, lid 8, zijn goedgekeurd;

b) indien EUCI niet wordt overgedragen zoals beschreven in punt a), wordt deze overgedragen met gebruikmaking van een gegevensdrager (bijv. USB-geheugenstick, cd, harde schijf), beschermd door encryptieproducten die overeenkomstig artikel 6, lid 8, zijn goedgekeurd, of als een papieren exemplaar in een ondoorzichtige verzegelde envelop.

10. Informatie met rubricering RESTREINT UE/EU mag worden vernietigd door de houder, met inachtneming van de bij de Rekenkamer geldende voorschriften inzake archivering. Informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of hoger wordt alleen vernietigd door de registercontrolefunctionaris wanneer de houder of een bevoegde autoriteit daartoe opdracht geeft, overeenkomstig de bij de Rekenkamer geldende voorschriften inzake archivering. Documenten met rubricering SECRET UE/EU SECRET worden vernietigd in het bijzijn van een getuige met een veiligheidsverklaring voor ten minste de rubriceringsgraad van het document dat wordt vernietigd. De registercontrolefunctionaris en de getuige, als de aanwezigheid van deze laatste vereist is, ondertekenen een vernietigingscertificaat, dat wordt bewaard in het register. De registercontrolefunctionaris bewaart vernietigingscertificaten van documenten met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL en SECRET UE/EU SECRET gedurende ten minste vijf jaar.

11. De autoriteit voor fysieke veiligheid en de autoriteit voor informatiebeveiliging stellen, rekening houdend met de plaatselijke omstandigheden, een gezamenlijk plan op voor de bescherming van EUCI in crisissituaties, met inbegrip van, indien nodig, plannen voor de vernietiging of evacuatie ervan in noodsituaties. Zij geven dergelijke instructies die zij passend achten om te voorkomen dat EUCI in handen van onbevoegden valt.

12. Wanneer EUCI fysiek moet worden vervoerd, neemt de Rekenkamer de door de bron opgelegde maatregelen in acht om de informatie tijdens het vervoer te beschermen tegen ongeoorloofde openbaarmaking.

13. De fysieke veiligheidsmaatregelen die van toepassing zijn in administratieve zones waar informatie met rubricering RESTREINT UE/EU RESTRICTED wordt behandeld en opgeslagen, worden uiteengezet in de bijlage.

Artikel 6

Bescherming van EUCI in communicatie- en informatiesystemen

1. Voor de toepassing van dit artikel wordt onder "communicatie- en informatiesysteem" verstaan elk systeem waarmee informatie in elektronische vorm kan worden behandeld. Een communicatie- en informatiesysteem omvat alle functionele bestanddelen die voor het functioneren ervan vereist zijn, waaronder infrastructurele, organisatorische, personele en informatiemiddelen.

2. Een "legitieme gebruiker" is een lid, ambtenaar, ander personeelslid of GND van de Rekenkamer met een vastgestelde en erkende behoefte aan toegang tot een specifiek informatiesysteem.

3. De Rekenkamer waarborgt dat haar systemen de erin opgenomen informatie op passende wijze zullen beschermen en zullen functioneren zoals nodig en wanneer nodig, onder de controle van legitieme gebruikers. Daartoe waarborgen zij passende niveaus van:

— authenticiteit: de garantie dat informatie echt is en van bonafide bronnen afkomstig is;

— beschikbaarheid: de eigenschap dat informatie op verzoek van een gemachtigde entiteit toegankelijk en bruikbaar is;

— vertrouwelijkheid: de eigenschap dat informatie niet wordt vrijgegeven aan niet-gemachtigde personen, entiteiten of processen;

— integriteit: de eigenschap dat de nauwkeurigheid en de volledigheid van de goederen en de informatie is gewaarborgd;

— onweerlegbaarheid: de eigenschap dat bewezen kan worden dat een actie of gebeurtenis heeft plaatsgevonden, zodat deze actie of gebeurtenis niet achteraf kan worden ontkend.

Deze waarborging is op een risicobeheersprocedure gebaseerd. Een "risico" is de mogelijkheid dat een bepaald gevaar de interne en externe kwetsbaarheden van een organisatie of een van de door haar gebruikte systemen zal uitbuiten en daarbij schade zal toebrengen aan de organisatie en haar materiële en immateriële bestanddelen. Risico wordt gemeten als een combinatie van de waarschijnlijkheid dat gevaren zich zullen voordoen en het effect daarvan. De risicobeheersprocedure bestaat uit de volgende stappen: identificatie van het gevaar en de kwetsbaarheid, risicobeoordeling, risicobehandeling, risicoaanvaarding en risicocommunicatie.

— De "risicobeoordeling" bestaat uit het in kaart brengen van gevaren en kwetsbaarheden en het verrichten van de daarmee verband houdende risicoanalyse, dat wil zeggen het beoordelen van de waarschijnlijkheid en het effect.

— De "risicobehandeling" bestaat uit het verzachten, wegnemen, verkleinen (via een passende combinatie van technische, fysieke, organisatorische of procedurele maatregelen), overbrengen of onder toezicht houden van het risico.

— De "risicoaanvaarding" is het besluit om erin te berusten dat er na de risicobehandeling een residueel risico blijft bestaan.

— Het "residueel risico" is het risico dat blijft bestaan nadat er veiligheidsmaatregelen zijn genomen, aangezien niet alle dreigingen kunnen worden tegengegaan en niet alle kwetsbaarheden kunnen worden weggenomen.

— "Risicocommunicatie" houdt in dat er risicovoorlichtingscampagnes worden gevoerd, gericht op gebruikers van een communicatie- en informatiesysteem, dat goedkeuringsautoriteiten over die risico's worden geïnformeerd en dat er verslag over wordt uitgebracht aan de operationele autoriteiten.

4. Alle elektronische toestellen en apparatuur die worden gebruikt om EUCI te behandelen, voldoen aan de toepasselijke voorschriften inzake de bescherming van EUCI. De voorkeur gaat uit naar elektronische toestellen en apparatuur die reeds zijn gehomologeerd door andere instellingen, organen of instanties van de EU. De toestellen worden gedurende hun volledige levenscyclus beveiligd.

5. Het communicatie- en informatiesysteem van de Rekenkamer voor de behandeling van EUCI wordt gehomologeerd door een bevoegde autoriteit. Daartoe streeft de Rekenkamer naar een overeenkomst inzake dienstverleningsniveau (Service Level Agreement — SLA) met een veiligheidshomologatieautoriteit van een EU-instelling die CIS kan homologeren waarmee EUCI wordt behandeld, met het oog op het ontvangen van een homologatieverklaring voor informatie met rubricering RESTREINT UE/EU RESTRICTED die door het CIS van de Rekenkamer kan worden behandeld, en de voorwaarden daarvoor. De SLA verwijst ook naar de normen die moeten worden toegepast voor de homologatieprocedure en wordt gesloten volgens de in artikel 10, lid 3, vastgestelde procedure.

6. Indien de Rekenkamer haar eigen homologatieprocedure voor haar CIS moet vaststellen, wordt in een gedelegeerd besluit als bedoeld in artikel 10, lid 10, van dit besluit de procedure vastgesteld in overeenstemming met de normen voor de homologatieprocedure voor CIS waarmee EUCI worden behandeld in andere instellingen, organen en instanties van de EU.

7. De verantwoordelijkheid voor de voorbereiding van de homologatiedossiers en de documentatie in overeenstemming met de toepasselijke normen berust volledig bij de eigenaar van de CIS.

8. Wanneer EUCI wordt beschermd door encryptieproducten, geeft de Rekenkamer de voorkeur aan producten die zijn goedgekeurd door de Raad of de secretaris-generaal van de Raad in zijn/haar hoedanigheid van autoriteit voor de goedkeuring van encryptieproducten, of aan producten die zijn goedgekeurd voor de bescherming van EUCI door andere instellingen, organen en instanties van de EU.

9. Informatie met rubricering RESTREINT UE/EU RESTRICTED wordt alleen behandeld op elektronische toestellen (zoals werkstations, printers, fotokopieerapparaten) die zich in een administratieve zone of een beveiligde zone bevinden. Elektronische toestellen waarmee informatie met rubricering RESTREINT UE/EU RESTRICTED wordt behandeld, worden gescheiden van andere computernetwerken en worden beschermd door middel van passende fysieke of technische maatregelen.

10. Al het personeel van de Rekenkamer dat betrokken is bij het ontwerpen, ontwikkelen, testen, in werking stellen, beheren of gebruiken van CIS voor de behandeling van EUCI, meldt aan de functionaris voor informatiebeveiliging alle mogelijke tekortkomingen, incidenten, inbreuken of gevaren in verband met de veiligheid die een effect kunnen hebben op de bescherming van de CIS en/of de daarin opgenomen EUCI.

Artikel 7

Procedure voor het uitwisselen en toegankelijk maken van gerubriceerde informatie

1. Wanneer zij daartoe wettelijk verplicht zijn op grond van de Verdragen of rechtshandelingen die op grond van de Verdragen zijn vastgesteld, verlenen de instellingen, organen en instanties van de EU en de nationale autoriteiten op eigen initiatief of op schriftelijk verzoek van de president, het (de) rapporterende lid (leden) of de secretaris-generaal toegang tot EUCI aan de Rekenkamer volgens onderstaande procedure.

2. Verzoeken om toegang worden aan de betrokken instellingen toegezonden via het archief van de Rekenkamer.

3. Indien nodig treft de Rekenkamer een administratieve regeling betreffende de praktische aspecten van de uitwisseling van EUCI of gelijkwaardige informatie.

4. Met het oog op het treffen van dergelijke administratieve regelingen verstrekt de Rekenkamer de bron alle nodige informatie over haar informatiebeveiligingssysteem. Indien nodig kan een evaluatiebezoek worden georganiseerd.

5. Deze administratieve regelingen worden getroffen met volledige inachtneming van de in artikel 13 van het Verdrag betreffende de Europese Unie neergelegde beginselen van bevoegdheidstoedeling en loyale samenwerking. Ze worden getroffen volgens de in artikel 10, lid 4, vastgestelde procedure.

6. Indien er geen administratieve regeling met een instelling, orgaan of instantie van de EU, een derde land of een internationale organisatie bestaat voor het verstrekken van gerubriceerde informatie aan de Rekenkamer, ondertekent de Rekenkamer een verklaring waarin zij zich ertoe verbindt de door haar ontvangen gerubriceerde informatie te beschermen.

Artikel 8

Inbreuk op de beveiliging, het verlies of de compromittering van gerubriceerde informatie

1. Een inbreuk op de beveiliging is iemands handeling of nalatigheid, in strijd met de beveiligingsvoorschriften van dit besluit en de uitvoeringsbepalingen daarbij.

2. Compromittering van EUCI doet zich voor wanneer, ten gevolge van een inbreuk op de beveiliging, EUCI geheel of gedeeltelijk is bekendgemaakt aan onbevoegden.

3. Inbreuken of vermoedelijke inbreuken op de beveiliging moeten onmiddellijk worden gemeld aan de autoriteit voor informatiebeveiliging van de Rekenkamer.

4. Indien vaststaat of er redelijke gronden zijn om aan te nemen dat EUCI is gecompromitteerd of verloren is gegaan, stelt de autoriteit voor informatiebeveiliging de directeur Personeelszaken, Financiën en Algemene Diensten en de secretaris-generaal van de Rekenkamer daarvan in kennis. De directeur Personeelszaken, Financiën en Algemene Diensten stelt de respectieve veiligheidsautoriteit van de bron onmiddellijk in kennis. De bovengenoemde directeur van de Rekenkamer voert een onderzoek uit en stelt de secretaris-generaal van de Rekenkamer en de veiligheidsautoriteit van de bron in kennis van de resultaten en de maatregelen die zijn genomen om te voorkomen dat de situatie zich herhaalt. Wanneer een lid van de Rekenkamer betrokken is, treedt de president van de Rekenkamer op in samenwerking met de secretaris-generaal van de Rekenkamer.

5. Elke ambtenaar of elk ander personeelslid van de Rekenkamer die/dat verantwoordelijk is voor een inbreuk op de beveiligingsvoorschriften van dit besluit en de uitvoeringsbepalingen daarbij, is onderworpen aan de sancties waarin het Statuut en de Regeling welke van toepassing is op de andere personeelsleden van de Europese Unie voorzien.

6. Elk lid van de Rekenkamer dat de bepalingen van dit besluit niet naleeft, is onderworpen aan de in artikel 286, lid 6, van het Verdrag vastgestelde maatregelen en sancties.

7. Eenieder die verantwoordelijk is voor het verloren gaan of compromitteren van EUCI, stelt zich bloot aan disciplinaire maatregelen en/of strafvervolging, in overeenstemming met de geldende wetten, regels en voorschriften.

Artikel 9

Beveiliging in geval van externe interventie

1. De Rekenkamer kan aan contractanten die in een lidstaat zijn geregistreerd, taken toevertrouwen die op grond van hun contract toegang tot EUCI inhouden of vereisen. Dit kan met name het geval zijn bij het onderhoud van communicatie- en informatiesystemen en het computernetwerk.

2. In geval van externe interventie neemt de Rekenkamer alle nodige veiligheidsmaatregelen als bedoeld in lid 3 van dit artikel, met inbegrip van een verzoek om een veiligheidsverklaring voor een vestiging om ervoor te zorgen dat EUCI gedurende de gehele duur van een aanbestedingsprocedure wordt beschermd door gegadigden en inschrijvers, en gedurende de gehele looptijd van een opdracht door contractanten en subcontractanten. De aanbestedende dienst ziet erop toe dat de minimumveiligheidsnormen waarin dit besluit voorziet, worden vermeld in overeenkomsten om de contractanten te verplichten deze na te leven.

3. Veiligheidsvoorschriften, aanbestedingsprocedures en templates en modellen voor contracten en onderaannemingen die toegang tot EUCI behelzen, aankondigingen van opdrachten, informatie over de omstandigheden waarin veiligheidsverklaringen voor vestigingen en personeel zijn vereist, programma-/projectbeveiligingsinstructies, memoranda over de beveiligingsaspecten, bezoeken en de overdracht en het vervoer van EUCI in het kader van dergelijke contracten en onderaannemingen, moeten in overeenstemming zijn met de voorschriften, templates en modellen die de Europese Commissie voor gerubriceerde contracten heeft vastgesteld in Besluit (EU, Euratom) 2015/444 van de Commissie ([4]) betreffende de veiligheidsvoorschriften voor de bescherming van gerubriceerde EU-informatie.

([4]) Besluit (EU, Euratom) 2015/444 van de Commissie van 13 maart 2015 betreffende de veiligheidsvoorschriften voor de bescherming van gerubriceerde EU-informatie (PB L 72 van 17.3.2015, blz. 53).

Artikel 10

Uitvoering van het besluit en daarmee samenhangende verantwoordelijkheden

1. De diensten van de Rekenkamer nemen alle noodzakelijke maatregelen die binnen hun verantwoordelijkheid vallen om de toepassing van dit besluit en de relevante uitvoeringsbepalingen te waarborgen bij de behandeling of opslag van EUCI of enige andere gerubriceerde informatie.

2. De secretaris-generaal is het tot aanstelling bevoegde gezag en het tot het sluiten van arbeidsovereenkomsten bevoegde gezag voor alle ambtenaren en andere personeelsleden. De secretaris-generaal kan aan de directeur Personeelszaken, Financiën en Algemene Diensten de verantwoordelijkheid delegeren voor het verlenen van machtiging aan ambtenaren en andere personeelsleden om toegang te krijgen tot informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of hoger, voor de uitoefening van zijn functie als veiligheidshomologatieautoriteit en voor het toezicht op het secretariaat van de Rekenkamer wat de behandeling van EUCI betreft.

3. De secretaris-generaal is bevoegd om SLA's te sluiten inzake de homologatie van de communicatie- en informatieapparatuur en -systemen van de Rekenkamer, het gebruik van een beveiligde zone in een andere EU-instelling en de procedure voor verzoeken om persoonlijke veiligheidsverklaringen voor toegang tot EUCI.

4. De directeur Personeelszaken, Financiën en Algemene Diensten is bevoegd om administratieve regelingen te treffen met de instellingen, organen en instanties van de EU voor de uitwisseling van EUCI die de Rekenkamer nodig heeft om haar mandaat uit te voeren. Deze directeur kan ook administratieve regelingen treffen met derde landen of internationale organisaties inzake de bescherming van ontvangen gerubriceerde informatie.

5. De directeur Personeelszaken, Financiën en Algemene Diensten is bevoegd om verklaringen te ondertekenen waarin hij/zij zich ertoe verbindt EUCI te beschermen die in het kader van een uitzonderlijke ad-hocvrijgave moet worden verstrekt.

6. De functionaris voor informatiebeveiliging van de Rekenkamer treedt op als autoriteit voor informatiebeveiliging. De functionaris voor informatiebeveiliging en de personen aan wie hij/zij zijn taken geheel of gedeeltelijk delegeert, beschikken over een passende veiligheidsverklaring. De autoriteit voor informatiebeveiliging kwijt zich van haar verantwoordelijkheden in nauwe samenwerking met het directoraat Personeelszaken, Financiën en Algemene Diensten, het directoraat Informatie, Werkomgeving en Innovatie en het Comité belast met de kwaliteitsbewaking van de controle (zie met name de artikelen 4, 6 en 8). De autoriteit voor informatiebeveiliging is ook verantwoordelijk voor opleidingen en voorlichtingsbijeenkomsten over informatiebeveiliging en voor periodieke inspecties om na te gaan of dit besluit wordt nageleefd, ook in geval van externe interventie en maatregelen die moeten worden genomen om de naleving te waarborgen.

7. Het hoofd van de veiligheidsdienst is verantwoordelijk voor de fysieke veiligheidsmaatregelen (met name artikel 5).

8. Een bij het secretariaat van de Rekenkamer ondergebracht archief is het in- en uitgangspunt voor informatie met rubricering RESTREINT UE/EU RESTRICTED die de Rekenkamer kan uitwisselen met andere instellingen, organen en instanties van de EU en de lidstaten. Het is ook het in- en uitgangspunt voor gelijkwaardige informatie van derde landen en internationale organisaties. Het archief wordt beheerd zoals bepaald in een gedelegeerd besluit. De archiefambtenaar neemt de volgende hoofdverantwoordelijkheden op zich:

a) registratie van het in- en uitgaan van informatie met rubricering RESTREINT UE/EU RESTRICTED;

b) beheer van specifieke administratieve zones voor de registratie van het behandelen, opslaan en raadplegen van EUCI met rubricering RESTREINT UE/EU RESTRICTED.

9. In het kader van een SLA wordt een register opgezet voor het gebruik van de beveiligde zone van een andere EU-instelling. Dit register, dat wordt beheerd door het secretariaat van de Rekenkamer onder de verantwoordelijkheid van de directeur Personeelszaken, Financiën en Algemene Diensten van de Rekenkamer, is het in- en uitgangspunt voor informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of hoger die de Rekenkamer kan uitwisselen met andere instellingen, organen en instanties van de EU en de lidstaten. Het is ook het in- en uitgangspunt voor gelijkwaardige

informatie van derde landen en internationale organisaties. Het is uitgerust met passende kluizen en andere beveiligingsapparatuur die geschikt is voor de bescherming van informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of hoger. Het register wordt beheerd zoals bepaald in een gedelegeerd besluit. De registercontrolefunctionaris beschikt over een passende veiligheidsverklaring en neemt de volgende hoofdverantwoordelijkheden op zich:

a) beheer van operaties in verband met de registratie, raadpleging, bewaring, reproductie, vertaling, overdracht, verzending en, in voorkomend geval, vernietiging van EUCI;

b) andere taken in verband met de bescherming van EUCI als vastgesteld in een gedelegeerd besluit.

10. Het Administratief Comité stelt een gedelegeerd besluit met uitvoeringsbepalingen voor dit besluit vast. De functionaris voor informatiebeveiliging stelt richtsnoeren voor informatiebeveiliging op. Het Comité belast met de kwaliteitsbewaking van de controle stelt controlerichtsnoeren op.

Artikel 11

Inwerkingtreding

Dit besluit treedt in werking op de dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Gedaan te Luxemburg, 3 juni 2021.

Voor de Rekenkamer
De president
Klaus-Heiner LEHNE

BIJLAGE

FYSIEKE VEILIGHEIDSMAATREGELEN MET BETREKKING TOT ADMINISTRATIEVE ZONES VOOR EUCI

1. Deze bijlage bevat voorschriften ter uitvoering van artikel 5 van het besluit. Dit zijn minimumvoorschriften voor de fysieke bescherming van administratieve zones voor informatie met rubricering RESTREINT UE/EU RESTRICTED bij de Rekenkamer: zones die zijn aangewezen voor het registreren, opslaan en raadplegen van informatie met rubricering RESTREINT UE/EU RESTRICTED.

2. Fysieke veiligheidsmaatregelen in administratieve zones hebben tot doel de ongeoorloofde toegang tot deze zones als volgt te voorkomen:

   a) er wordt een duidelijk omschreven afscheiding ingesteld waar personen kunnen worden gecontroleerd;

   b) toegang zonder begeleiding wordt alleen toegestaan aan personen die naar behoren door de autoriteit voor informatiebeveiliging van de Rekenkamer of een andere bevoegde autoriteit gemachtigd zijn;

   c) alle andere personen worden altijd begeleid of aan gelijkwaardige controles onderworpen.

3. De autoriteit voor informatiebeveiliging van de Rekenkamer kan bij wijze van uitzondering toegang verlenen aan onbevoegden, onder meer voor werkzaamheden in een administratieve zone, op voorwaarde dat dit geen toegang tot EUCI inhoudt, die veilig opgeborgen blijft. Deze personen mogen alleen binnenkomen indien zij worden begeleid door en voortdurend onder toezicht staan van de autoriteit voor informatiebeveiliging of de registercontrolefunctionaris.

4. De autoriteit voor informatiebeveiliging stelt procedures vast voor de controle van de sleutels en/of codecombinaties voor alle administratieve zones en al het beveiligd meubilair. Deze procedures moeten ongeoorloofde toegang verhinderen.

5. De codecombinaties worden gememoriseerd door het kleinst mogelijke aantal personen die er kennis van moeten nemen. De codecombinaties voor beveiligd meubilair dat wordt gebruikt voor de opslag van informatie met rubricering van RESTREINT UE/EU RESTRICTED worden gewijzigd:

   — bij ontvangst van een nieuw beveiligd meubelstuk;

   — in geval van een wijziging in het personeel dat de combinatie kent;

   — indien de code is gecompromitteerd of een vermoeden daarvan bestaat;

   — indien aan een slot onderhoud of reparaties is/zijn verricht;

   — ten minste om de twaalf maanden.

6. De autoriteit voor informatiebeveiliging en het hoofd van de veiligheidsdienst zijn verantwoordelijk voor de naleving van deze voorschriften.