IV

(Informatie)

INFORMATIE AFKOMSTIG VAN DE INSTELLINGEN, ORGANEN EN INSTANTIES VAN DE EUROPESE UNIE

EUROPEES PARLEMENT

BESLUIT VAN HET BUREAU VAN HET EUROPEES PARLEMENT

van 6 juni 2011

inzake de regels betreffende de behandeling van vertrouwelijke informatie door het Europees Parlement

(2011/C 190/02)

HET BUREAU VAN HET EUROPEES PARLEMENT,

Gelet op artikel 23, lid 12, van het Reglement van het Europees Parlement,

Overwegende hetgeen volgt:

(1) In het licht van het Kaderakkoord over de betrekkingen tussen het Europees Parlement en de Europese Commissie [1], dat op 20 oktober 2010 werd ondertekend („het Kaderakkoord"), is het nodig het besluit van het Bureau van 13 november 2006 over de regels betreffende de administratieve behandeling van vertrouwelijke documenten te herzien.

(2) Het Verdrag van Lissabon kent het Europees Parlement nieuwe taken toe en om de activiteiten van het Parlement te ontwikkelen op die gebieden die een bepaalde mate aan vertrouwelijkheid vereisen, is het nodig om basisbeginselen, minimumnormen inzake beveiliging en passende procedures vast te stellen voor de behandeling door het Europees Parlement van vertrouwelijke, waaronder gerubriceerde, informatie.

(3) De regels die in dit besluit zijn vastgelegd, beogen normen voor beveiliging en compatibiliteit te garanderen, die gelijkwaardig zijn aan de regels die zijn vastgesteld door andere instellingen, instanties, bureaus en agentschappen van de EU die krachtens of op basis van de Verdragen zijn opgericht, of door de lidstaten, teneinde te komen tot een soepele werking van het besluitvormingsproces van de Europese Unie.

(4) De voorschriften van dit besluit gelden onverminderd artikel 15 van het Verdrag betreffende de werking van de Europese Unie (VWEU) en Verordening (EG) nr. 1049/2001 van het Europees Parlement en de Raad van 30 mei 2001 inzake de toegang van het publiek tot documenten van het Europees Parlement, de Raad en de Commissie [2].

(5) De voorschriften van dit besluit gelden onverminderd artikel 16 VWEU en Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad van 18 december 2000 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de communautaire instellingen en organen en betreffende het vrije verkeer van die gegevens [3].

HEEFT HET VOLGENDE BESLUIT VASTGESTELD:

Artikel 1

Doelstelling

Dit besluit regelt het genereren, het ontvangen, het verstrekken en het bewaren van vertrouwelijke informatie door het Europees Parlement met het oog op een passende bescherming van het vertrouwelijke karakter daarvan. Het geeft in het bijzonder uitvoering aan Bijlage 2 bij het Kaderakkoord.

[1] PB L 304 van 20.11.2010, blz. 47.

[2] PB L 145 van 31.5.2001, blz. 43.

[3] PB L 8 van 12.1.2001, blz. 1.

Artikel 2

Definities

Voor de toepassing van dit besluit wordt verstaan onder:

a) „informatie": elke schriftelijke of mondelinge informatie, ongeacht de drager of de auteur;

b) „vertrouwelijke informatie": gerubriceerde EU-gegevens („EU Classified Information", EUCI) of gerubriceerde gegevens afkomstig van de lidstaten, derde staten of internationale organisaties, en niet-gerubriceerde andere vertrouwelijke informatie;

c) „gerubriceerde EU-gegevens" (EUCI): gegevens en materiaal, gerubriceerd als „TRÈS SECRET UE/TOP SECRET EU", „SECRET UE/EU SECRET", „CONFIDENTIEL UE/EU CONFIDENTIAL" of „RESTREINT UE/EU RESTRICTED", waarvan openbaarmaking zonder machtiging de belangen van de Unie of van één of meer van haar lidstaten in meerdere of mindere mate zou kunnen schaden, ongeacht of dergelijke informatie afkomstig is van de instellingen, instanties, bureaus en agentschappen die krachtens of op basis van de Verdragen zijn opgericht, of van de lidstaten, derde staten of internationale organisaties. In dit verband:

— „TRÈS SECRET UE/TOP SECRET EU" is de rubricering voor gegevens en materiaal waarvan de openbaarmaking zonder machtiging uitzonderlijk nadelig zou kunnen zijn voor de wezenlijke belangen van de Europese Unie of van één of meer van haar lidstaten in uitzonderlijke mate;

— „SECRET UE/EU SECRET" is de rubricering voor gegevens en materiaal waarvan de openbaarmaking zonder machtiging ernstige gevolgen zou kunnen hebben voor de wezenlijke belangen van de Europese Unie of van één of meer van haar lidstaten;

— „CONFIDENTIEL UE/EU CONFIDENTIAL" is de rubricering voor gegevens en materiaal waarvan de openbaarmaking zonder machtiging nadelige gevolgen zou kunnen hebben voor de wezenlijke belangen van de Europese Unie of van één of meer van haar lidstaten;

— „RESTREINT UE/EU RESTRICTED" is de rubricering voor gegevens en materiaal waarvan de openbaarmaking zonder machtiging nadelig zou kunnen zijn voor de belangen van de Europese Unie of van één of meer van haar lidstaten;

d) „andere vertrouwelijke informatie": enig ander niet-gerubriceerde vertrouwelijke informatie, met inbegrip van informatie waarop gegevensbeschermingsregels van toepassing zijn of die onder het beroepsgeheim valt, die binnen het Europees Parlement is gegenereerd of die door andere instellingen, instanties, bureaus en agentschappen die krachtens of op basis van de Verdragen zijn opgericht, of door de lidstaten aan het Europees Parlement is verstrekt;

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

f) „materiaal": documenten, of machines of uitrustingen die zijn of worden vervaardigd;

g) „need-to-know": de noodzaak voor een persoon toegang te hebben tot vertrouwelijke informatie om een officiële functie of taak te kunnen vervullen;

h) „machtiging": een besluit (screeningsbesluit), vastgesteld door de voorzitter in het geval van leden van het Europees Parlement en door de secretaris-generaal in het geval van ambtenaren van het Europees Parlement en andere parlementaire medewerkers die in dienst van de politieke groepen werkzaam zijn, om een persoon tot op een bepaald niveau toegang tot EUCI te geven op basis van een positief resultaat van een veiligheidsscreening (doorlichting) dat door een nationale autoriteit overeenkomstig nationale rechtsvoorschriften en in overeenstemming met de bepalingen van Bijlage I, deel 2, is uitgevoerd;

i) „lager rubriceren" (downgrading): het verlagen van het niveau van rubricering;

j) „derubricering" (declassification): het opheffen van een rubricering;

k) „opsteller": de gemachtigde auteur van EUCI of andere vertrouwelijke informatie;

l) „veiligheidsmededelingen": de technische uitvoeringsmaatregelen van Bijlage II ([1]).

Artikel 3

Basisbeginselen en minimumnormen

1. De behandeling van vertrouwelijke informatie door het Europees Parlement moet plaatsvinden volgens de basisbeginselen en minimumnormen van Bijlage I, deel 1.

2. Het Europees Parlement zet in overeenstemming met de basisbeginselen en minimumnormen een beheerssysteem voor informatieveiligheid (Information Security Management System, ISMS) op, dat gericht is op het ondersteunen van het parlementaire en administratieve werk, terwijl het tegelijkertijd de bescherming van door het Europees Parlement behandelde vertrouwelijke informatie waarborgt, met volledige inachtneming van de regels die door de opsteller van de bewuste informatie zijn vastgesteld zoals opgenomen in de veiligheidsmededelingen.

De verwerking van vertrouwelijke informatie middels de geautomatiseerde informatiesystemen (IS) van het Europees Parlement vindt plaats in overeenstemming met het concept informatiezekerheid (IA) en op de wijze die in de veiligheidsmededelingen is vastgesteld.

([1]) Bijlage moet nog worden vastgesteld.

3. De leden van het Europees Parlement kunnen informatie die tot en met het niveau CONFIDENTIEL UE/EU CONFIDENTIAL is gerubriceerd zonder veiligheidsmachtiging raadplegen. Voor informatie die als CONFIDENTIEL UE/EU CONFIDENTIAL is gerubriceerd, ondertekenen zij een plechtige verklaring dat zij de inhoud daarvan niet aan derden bekend zullen maken. Informatie die boven het niveau CONFIDENTIEL UE/EU CONFIDENTIAL is gerubriceerd, wordt alleen aan leden ter beschikking gesteld die over de passende veiligheidsmachtiging beschikken.

4. De ambtenaren van het Europees Parlement en andere parlementaire medewerkers die in dienst van de politieke groepen zijn, mogen vertrouwelijke informatie raadplegen indien zij een vastgestelde „need-to-know"-status hebben, en mogen vertrouwelijke gegevens die boven het niveau CONFIDENTIEL UE/EU CONFIDENTIAL is gerubriceerd raadplegen, indien zij over de passende veiligheidsmachtiging beschikken.

Artikel 4

Het genereren van vertrouwelijke informatie en de administratieve behandeling daarvan door het Europees Parlement

1. De voorzitter van het Europees Parlement, de voorzitters van de betreffende parlementaire commissie en de secretaris-generaal en/of elk persoon die voldoende door hem of haar schriftelijk is gemachtigd, mag vertrouwelijke informatie genereren en/of informatie rubriceren, zoals bedoeld in de veiligheidsmededelingen.

2. Bij het genereren van gerubriceerde informatie, past de opsteller het passende niveau van rubricering toe in overeenstemming met de internationale normen en definities die in Bijlage I zijn opgenomen. De opsteller bepaalt, als algemene regel, ook de geadresseerden die moeten worden gemachtigd om de informatie te raadplegen overeenkomstig het niveau van rubricering. Deze informatie wordt aan de Dienst vertrouwelijke informatie (Confidential Information Service, CIS) meegedeeld op het moment dat de document bij de CIS wordt ingediend.

3. Vertrouwelijke informatie die onder het beroepsgeheim valt, wordt behandeld in overeenstemming met de instructies voor behandeling, zoals gedefinieerd in de veiligheidsmededelingen.

Artikel 5

Het ontvangst van vertrouwelijke informatie door het Europees Parlement

1. Vertrouwelijke informatie die door het Europees Parlement wordt ontvangen, worden als volgt doorgegeven:

— EUCI die als als „RESTREINT UE/EU RESTRICTED" is gerubriceerd en andere vertrouwelijke gegevens: aan het secretariaat van het parlementaire bureau/ambtsdrager die het verzoek daartoe heeft ingediend,

— EUCI die als „CONFIDENTIEL UE/CONFIDENTIEL EU" en hoger is gerubriceerd: aan de CIS.

2. De registratie, het bewaren en de traceerbaarheid van vertrouwelijke informatie worden hetzij door het secretariaat van het bureau/ambtsdrager die de informatie heeft ontvangen, hetzij door de CIS verzekerd.

3. In het geval van vertrouwelijke informatie die door de Commissie op basis van het Kaderakkoord wordt verstrekt, worden de overeengekomen regelingen zoals bedoeld in Bijlage II, punt 3.2 van het Kaderakkoord (in onderlinge overeenstemming vastgelegd en betrekking hebbend op geadresseerden, raadplegingsprocedure, onder meer de veilige leeskamer, vergadering achter gesloten deuren of andere zaken), die bedoeld zijn om de vertrouwelijkheid van de informatie te waarborgen, samen met de vertrouwelijke informatie gedeponeerd bij het parlementaire bureau/ambtsdrager of bij de CIS wanneer de informatie als „CONFIDENTIEL UE/CONFIDENTIEL EU" of hoger is gerubriceerd.

4. De regelingen als bedoeld in lid 3 kunnen *mutatis mutandis* worden toegepast in het geval van vertrouwelijke informatie die door andere instellingen, instanties, bureaus en agentschappen van de EU die krachtens of op basis van de Verdragen zijn opgericht, of door de lidstaten worden verstrekt.

5. EUCI die als „TRÈS SECRET UE/ TOP SECRET EU" is gerubriceerd moeten aan het Europees Parlement worden gestuurd in overeenstemming met nadere regelingen die worden overeengekomen door het parlementaire bureau/ambtsdrager die het verzoek voor de betreffende gegevens heeft ingediend, en de EU-instelling of de lidstaat die de informatie heeft verstrekt. De Conferentie van voorzitters richt een comité van toezicht op. Het comité van toezicht heeft tot taak om een beschermingsniveau te waarborgen dat overeenstemt met het niveau van rubricering.

Artikel 6

Verstrekking van EUCI door het Europees Parlement aan derden

Het Europees Parlement mag, indien de opsteller daarmee instemt, EUCI verstrekken aan andere instellingen, instanties, bureaus en agentschappen die krachtens of op basis van de Verdragen zijn opgericht, of aan de lidstaten op voorwaarde dat zij waarborgen dat, bij de behandeling van EUCI, binnen hun diensten en binnen hun vestigingen regels worden toegepast die gelijkwaardig zijn aan de regels die zijn vastgelegd in het onderhavige besluit.

Artikel 7

Opslag en raadpleging van vertrouwelijke informatie in veilige ruimten (veilige leeskamers)

1. Veilige leeskamers voorzien in veilige bewaarplaatsen en bevat geen fotokopieerapparatuur, telefoons, faxapparaten, scanners of andere technische middelen voor het vermenigvuldigen of het verzenden van documenten.

2. De volgende voorwaarden gelden voor de toegang van de veilige leeskamer:

a) Alleen de onderstaande personen hebben toegang tot de veilige leeskamer:

— de leden van het Europees Parlement, ambtenaren van het Europees Parlement en andere parlementaire medewerkers die in dienst van de politieke groepen zijn, naar behoren geïdentificeerd, overeenkomstig de regelingen in artikel 4, lid 2, of artikel 5, lid 3 en lid 4;

— de ambtenaren van het Europees Parlement die met het beheer van de CIS zijn belast;

— indien nodig, de ambtenaren van het Europees Parlement die met veiligheid en brandveiligheid zijn belast.

De veilige leeskamer wordt alleen schoongemaakt in aanwezigheid van en onder strikt toezicht van een ambtenaar die bij de CIS werkt.

b) Ieder persoon die toegang tot de vertrouwelijke informatie wenst, stuurt zijn of haar naam naar de CIS. De CIS controleert de identiteit van elk persoon die een aanvraag voor raadpleging van vertrouwelijke informatie indient en gaat na, indien van toepassing, of de betrokken persoon beschikt over de noodzakelijke veiligheidsmachtiging en geautoriseerd is om in overeenstemming met de regelingen in artikel 4, lid 2, of artikel 5, lid 3 en lid 4, de informatie te raadplegen.

c) De CIS is bevoegd om toegang te weigeren aan elk persoon die op grond van het hierboven genoemde onder a) en b) niet gemachtigd is om de kamer te betreden. Tegen de besluiten van de CIS kan beroep worden ingesteld bij de voorzitter (in het geval van de leden van het Europees Parlement), respectievelijk de secretaris-generaal, in alle andere gevallen.

3. Raadpleging van vertrouwelijke informatie in de veilige leeskamer vindt plaats onder de volgende voorwaarden:

a) De personen die gemachtigd zijn om vertrouwelijke informatie te raadplegen en die aanvraag hebben ingediend, zoals bedoeld in het bovenstaande lid 2 onder b), melden zich bij de CIS.

Behoudens in uitzonderlijke omstandigheden (bijv. wanneer een groot aantal aanvragen voor raadpleging in een kort tijdsbestek zijn ingediend), wordt slechts één persoon tegelijkertijd tot de veilige leeskamer toegelaten om vertrouwelijke gegevens te raadplegen, altijd in aanwezigheid van een ambtenaar van de CIS.

Die ambtenaar brengt de persoon die aldus gemachtigd is om vertrouwelijke gegevens te raadplegen, op de hoogte van zijn/haar verplichtingen en vraagt hem/haar, in het bijzonder, een plechtige verklaring te tekenen dat hij/zij de inhoud van de gegevens niet aan een derde bekend zal maken.

b) Tijdens het proces van raadpleging zijn het hebben van contact met de buitenwereld (inclusief via het gebruik van telefoon of andere technische hulpmiddelen), het maken van aantekeningen en het fotokopiëren of het fotograferen van de geraadpleegde vertrouwelijke gegevens verboden.

c) Alvorens een persoon toestemming te geven de leeskamer te verlaten, gaat de verantwoordelijke ambtenaar van de CIS na dat de geraadpleegde vertrouwelijke gegevens aanwezig, onaangetast en volledig zijn.

4. In het geval van een overtreding van deze regels stelt de verantwoordelijke ambtenaar van de CIS de secretaris-generaal op de hoogte, die de zaak naar de voorzitter verwijst indien de dader een lid van het Europees Parlement is.

Artikel 8

Minimumnormen voor raadpleging van vertrouwelijke informatie

1. Wat de administratieve verwerking van vertrouwelijke informatie tijdens een vergadering achter gesloten deuren betreft, draagt het secretariaat van het parlementaire bureau/de ambtsdrager dat/die voor de vergadering verantwoordelijk is, ervoor zorg dat:

— alleen de personen die aan de vergadering deelnemen en die over de noodzakelijke veiligheidsmachtiging beschikken, worden toegestaan om de vergaderruimte betreden;

— alle documenten genummerd zijn, aan het begin van de vergadering worden uitgedeeld en aan het eind worden opgehaald, en dat er geen notities en/of fotokopieën of foto's van deze documenten worden gemaakt;

— in de notulen van de vergadering geen melding wordt gemaakt van de inhoud van de bespreking over de gegevens die volgens de vertrouwelijke procedure zijn behandeld;

— vertrouwelijke informatie die mondeling aan ontvangers in het Parlement wordt verstrekt onder hetzelfde niveau van bescherming wordt gebracht als die geldt voor vertrouwelijke gegevens die in schriftelijke vorm is verstrekt. Dit kan een plechtige verklaring van de ontvangers van de bedoelde informatie omvatten, dat zij de inhoud ervan niet aan een derde bekend zullen maken.

2. De volgende regels gelden voor de administratieve behandeling van vertrouwelijke gegevens door het secretariaat van het parlementaire bureau/de ambtsdrager buiten de vergadering achter gesloten deuren:

— de papieren versie van de documenten worden persoonlijk aan het hoofd van het secretariaat overgedragen, die de documenten registreert en die een bewijs van ontvangst verstrekt;

— dergelijke documenten worden, wanneer ze niet worden gebruikt, op een afgesloten plaats bewaard, onder de verantwoordelijkheid van het secretariaat;

— onverminderd de administratieve behandeling van vertrouwelijke gegevens tijdens een vergadering achter gesloten deuren zoals hierboven in lid 1 aangegeven, mogen de documenten nooit worden vermenigvuldigd, op een andere drager worden opgeslagen of aan derden worden verzonden;

— de toegang tot dergelijke documenten is beperkt tot de geadresseerden daarvan en vindt plaats onder toezicht van het secretariaat, overeenkomstig de regelingen van artikel 4, lid 2, en artikel 5, lid 3 en lid 4;

— het secretariaat houdt een lijst van de personen bij, die de documenten hebben geraadpleegd, inclusief de datum en de tijd van raadpleging. Deze lijst wordt aan de CIS verstrekt met het oog op het opstellen van het jaarverslag zoals bedoeld in artikel 12.

Artikel 9

Archiveren van vertrouwelijke informatie

1. In de gebouwen van het Parlement wordt voorzien in veilige archiveringsfaciliteiten.

Vertrouwelijke informatie die definitief bij de CIS of bij het parlementaire bureau/de ambtsdrager wordt gedeponeerd, wordt zes maanden na de laatste raadpleging en, ten laatste één jaar na de deponering ervan, naar het veilige archief bij de CIS overgebracht.

2. De CIS is verantwoordelijk voor het beheer van de veilige archieven, in overeenstemming met de standaard archiveringscriteria.

3. Vertrouwelijke gegegevens die in de veilige archieven wordt bewaard, mag worden geraadpleegd onder de volgende voorwaarden:

— alleen de personen die aan de hand van hun naam of hun kantoor worden geïdentificeerd in het begeleidende document dat werd opgesteld op het moment dat de vertrouwelijke gegevens werd gedeponeerd, zijn gemachtigd deze gegevens te raadplegen;

— aanvragen voor het raadplegen van vertrouwelijke gegevens moeten worden ingediend bij de CIS, die het desbetreffende document naar de veilige leeskamer overbrengt;

— de in artikel 7 bedoelde procedures en voorwaarden voor het raadplegen van vertrouwelijke gegevens zijn van toepassing.

Artikel 10

Lager rubriceren en derubriceren van EUCI

1. EUCI kunnen alleen lager gerubriceerd of gederubriceerd worden met de toestemming van de opsteller en, zo nodig, na bespreking met de betrokken partijen. Lager rubriceren en derubricering moeten schriftelijk worden bevestigd. De opsteller van het document is er verantwoordelijk voor dat de geadresseerden van de wijziging op de hoogte worden gebracht; en deze geadresseerden zijn er op hun beurt verantwoordelijk voor dat de daaropvolgende geadresseerden, aan wie zij het document hebben gezonden of voor wie zij het hebben gekopieerd, van de wijziging op de hoogte worden gebracht. Indien mogelijk, vermelden de opstellers op gerubriceerde documenten een datum, een periode of een gebeurtenis waarna de inhoud lager gerubriceerd of gederubriceerd kan worden. Zo niet, verifiëren zij de documenten uiterlijk om de vijf jaar om zich ervan te vergewissen of de oorspronkelijke rubricering moet worden gehandhaafd.

2. Derubricering van documenten die in de veilige archieven worden gehouden, vindt plaats ten laatste na 30 jaar, overeenkomstig de bepalingen van Verordening (EEG, Euratom) nr. 354/83 van de Raad van 1 februari 1983 inzake het voor het publiek toegankelijk maken van de historische archieven van de Europese Economische Gemeenschap en de Europese Gemeenschap voor Atoomenergie [1]. Derubricering zal worden verwezenlijkt door de opsteller van de gerubriceerde informatie of door de dienst die verantwoordelijk is overeenkomstig Bijlage I, deel 1, onder 10.

Artikel 11

Inbreuken op vertrouwelijkheid

1. Inbreuken op de vertrouwelijkheid in het algemeen, en op dit besluit in het bijzonder, leiden in het geval van leden van het Europees Parlement tot de toepassing van de desbetreffende bepalingen inzake sancties, zoals opgenomen in het Reglement van het Europees Parlement.

2. Inbreuken die zijn begaan door ambtenaren leidt tot de toepassing van de relevante procedures en de sancties die zijn voorzien, respectievelijk, in het Statuut van de ambtenaren en de regeling welke van toepassing is op de andere personeelsleden van de Europese Unie, zoals vastgelegd in Verordening (EEG. Euratom, ECSC) 259/68 [2] („het Statuut").

3. De voorzitter en de secretaris-generaal organiseren eventueel noodzakelijke onderzoeken.

Artikel 12

Aanpassing van dit besluit en de uitvoeringsregels en jaarlijkse rapportage over de toepassing van dit besluit

1. De secretaris-generaal doet de nodige voorstellen voor de aanpassing van dit besluit en de uitvoeringsregels in de bijlagen, en legt deze voorstellen voor aan het Bureau voor een besluit.

2. De secretaris-generaal doet het Bureau een jaarverslag over de toepassing van dit besluit toekomen.

[1] PB L 43 van 15.2.1983, blz. 1.
[2] PB L 56 van 4.3.1968, blz. 1.

Artikel 13

Overgangsbepalingen en slotbepalingen

1. Vertrouwelijke informatie die zich vóór de toepassing van dit besluit bij de CIS of in de archieven bevindt, wordt als „RESTREINT UE/EU RESTRICTED" gerubriceerd, tenzij de opsteller ervan uiterlijk binnen één jaar na de inwerkingtreding van deze regels besluit de informatie niet te rubriceren of op een hoger niveau te rubriceren, of besluit ze van een markering te voorzien.

2. Indien de opsteller besluit de informatie op een hoger niveau te rubriceren, worden de documenten door de opsteller of zijn gedelegeerden, in overleg met de CIS en in overeenstemming met de criteria in Bijlage I bij dit besluit, op het laagst mogelijke niveau gerubriceerd.

3. Het besluit van het Bureau van 13 november 2006 over de regels betreffende de administratieve behandeling van vertrouwelijke documenten wordt ingetrokken.

4. Het besluit van het Bureau van 24 oktober 2005 waarin de secretaris-generaal wordt opgedragen een comité voor derubricering op te richten en besluiten met betrekking tot derubricering goed te keuren, wordt ingetrokken.

Artikel 14

Inwerkingtreding

1. Dit besluit treedt in werking op de dag van zijn bekendmaking in het *Publicatieblad van de Europese Unie*.

2. Het besluit is van toepassing vanaf 1 juli 2011.

BIJLAGE I

DEEL 1

BASISBEGINSELEN EN MINIMUMNORMEN INZAKE VEILIGHEID VOOR DE BESCHERMING VAN VERTROUWELIJKE INFORMATIE

1. **Inleiding**

Deze voorschriften bevatten de grondbeginselen en minimumnormen inzake veiligheid die door het Europees Parlement in al zijn standplaatsen en door alle ontvangers van gerubriceerde EU-gegevens (EUCI) en andere vertrouwelijke informatie moeten worden nageleefd, zodat de veiligheid wordt gegarandeerd en alle betrokkenen er zeker van kunnen zijn dat er een gemeenschappelijke norm voor de bescherming geldt. Zij worden aangevuld met regels betreffende de verwerking van vertrouwelijke informatie door parlementaire commissies en andere parlementaire instanties/ambtsdragers.

2. **Algemene beginselen**

Het veiligheidsbeleid van het Europees Parlement maakt integraal onderdeel uit van zijn algemeen beleid inzake intern beheer en is dus gebaseerd op de beginselen van dat algemeen beleid. Deze beginselen zijn: wettigheid, transparantie, verantwoordingsplicht en subsidiariteit (proportionaliteit).

Het beginsel van wettigheid houdt in dat de uitoefening van veiligheidsfuncties strikt binnen het geldende rechtskader moeten worden uitgeoefend en dat de toepasselijke regelgeving moet worden nageleefd. Voorts betekent dit beginsel dat de verantwoordelijkheden inzake veiligheid op adequate rechtsvoorschriften moeten worden gebaseerd. Het Statuut is volledig van toepassing, en in het bijzonder artikel 17 daarvan inzake de verplichting van de personeelsleden om zich te onthouden van het niet-geautoriseerde openbaar maken van informatie die in dienst is ontvangen, en titel VI inzake tuchtmaatregelen. Ten slotte betekent het dat veiligheidsinbreuken die onder de verantwoordelijkheid van het Europees Parlement vallen, behandeld moeten worden op een wijze die strookt met het beleid van het Europese Parlement inzake tuchtmaatregelen.

Het beginsel van transparantie houdt in dat alle veiligheidsvoorschriften en -bepalingen duidelijk moeten zijn, dat er een evenwicht moet worden gevonden tussen de verschillende diensten en de verschillende gebieden (fysieke veiligheid in verhouding tot de bescherming van gegevens, enz.) en dat een coherent en gestructureerd beleid inzake veiligheidsbewustzijn moet worden gevoerd. Het betekent ook dat duidelijke schriftelijke richtsnoeren nodig zijn voor de uitvoering van de veiligheidsmaatregelen.

Het beginsel van verantwoordingsplicht houdt in dat de verantwoordelijkheden op het gebied van de veiligheid duidelijk worden vastgesteld. Voorts houdt dit beginsel in dat regelmatig moet worden nagegaan, of deze verantwoordelijkheden correct worden uitgeoefend.

Het beginsel van subsidiariteit (of proportionaliteit) betekent dat de veiligheid op het laagst mogelijke niveau moet worden georganiseerd en zo dicht mogelijk bij de directoraten-generaal en de diensten van het Europees Parlement. Voorts houdt het proportionaliteitsbeginsel in dat de beveiligingsactiviteiten strikt worden beperkt tot die gebieden waarvoor het werkelijk nodig is en dat de veiligheidsmaatregelen in verhouding moeten staan tot de te beschermen belangen en tot de feitelijke of mogelijke bedreiging van deze belangen, zodat deze belangen op een zodanige wijze kunnen worden beschermd, waardoor zo weinig mogelijk ontwrichting wordt veroorzaakt.

3. **Fundamenten voor gegevensbeveiliging**

De fundamenten voor een goede gegegevensbeveiliging zijn:

a) de aanwezigheid in het Europees Parlement van een Infosec- (Information security assurance service) autoriteit (IA), die met de betrokken veiligheidsautoriteit samenwerkt om informatie en advies te verschaffen over technische bedreigingen voor de veiligheid en de middelen om zich daartegen te beschermen;

b) nauwe samenwerking tussen de verantwoordelijke diensten van het Europees Parlement en de veiligheidsdiensten van de overige EU-instellingen.

4. **Beginselen van de gegevensbeveiliging**

4.1. *Doelstellingen*

De hoofddoelstellingen van gegevensbeveiliging zijn als volgt:

a) beveiliging van EUCI en overig vertrouwelijke informatie tegen spionage, compromittering of openbaarmaking zonder machtiging;

b) bescherming van EUCI die in communicatie- en informatiesystemen en -netwerken worden verwerkt, tegen gevaren met betrekking tot het vertrouwelijke karakter, de integriteit en de beschikbaarheid ervan;

c) beveiliging van de locaties van het Europees Parlement waar EUCI zijn ondergebracht, tegen sabotage en kwaadwillige beschadiging;

d) in geval van veiligheidsinbreuk, beoordeling van de aangerichte schade, beperking van de gevolgen ervan, uitvoering van een veiligheidsonderzoek en vaststelling van corrigerende maatregelen.

4.2. *Rubricering*

4.2.1. Waar geheimhouding van belang is, zijn zorg en ervaring nodig bij de selectie van de informatie en het materiaal die moeten worden beschermd en bij de beoordeling van de mate van vereiste bescherming. Het is van fundamenteel belang dat de mate van bescherming overeenstemt met de gevoeligheid in termen van beveiliging van de te beschermen informatie of het materiaal. Om voor een soepele informatiestroom te zorgen, moeten zowel een te hoge als te lage rubricering worden voorkomen.

4.2.2. Het rubriceringssysteem is het instrument waarmee gevolg wordt gegeven aan de beginselen die in deel I uiteen worden gezet; een soortgelijk rubriceringssysteem moet worden gebruikt voor het plannen en organiseren van de bestrijding van spionage, sabotage, terrorisme en andere bedreigingen, zodat de grootste mate van bescherming wordt geboden aan de belangrijkste locaties waar EUCI zijn ondergebracht, en binnen die locaties aan de gevoeligste elementen.

4.2.3. Voor de rubricering van informatie is alleen de opsteller van de betreffende gegevens verantwoordelijk.

4.2.4. Het rubriceringsniveau mag uitsluitend worden bepaald op basis van de inhoud van de gegevens.

4.2.5. Wanneer verschillende stukken informatie bijeen worden gebracht, moet op het geheel een rubriceringsniveau worden toegepast dat minstens even hoog is als de hoogste rubricering dat individueel aan deze stukken is toegepast. Een informatieverzameling kan evenwel een hogere rubricering krijgen dan de bestanddelen ervan.

4.2.6. Rubricering wordt alleen toegekend als dit nodig is en zolang als dit nodig is.

4.3. *Doel van de veiligheidsmaatregelen*

De veiligheidsmaatregelen moeten:

a) betrekking hebben op alle personen die toegang hebben tot EUCI, dragers van EUCI en andere vertrouwelijke informatie, alsmede op alle locaties waar zich deze informatie bevindt en belangrijke installaties;

b) zodanig ontworpen zijn dat personen detecteert, wiens positie de veiligheid van de bedoelde informatie en van belangrijke installaties waar deze informatie is ondergebracht, in gevaar kan brengen, en moeten in de uitsluiting of verwijdering van deze personen voorzien;

c) voorkomen dat een niet-gemachtigde persoon toegang krijgt tot de bedoelde informatie of tot installaties die deze informatie bevatten;

d) ervoor zorgen dat de bedoelde informatie alleen verspreid wordt op basis van het „need to know"-beginsel, dat fundamenteel is voor alle aspecten van de veiligheid;

e) de integriteit (d.w.z. het voorkomen van schending of van wijziging of verwijdering van informatie zonder machtiging) en de beschikbaarheid (d.w.z. dat de toegang niet geweigerd wordt aan degene die de informatie nodig heeft en tot toegang gemachtigd is) waarborgen van alle informatie, al dan niet gerubriceerd, en in het bijzonder van informatie die in elektromagnetische vorm wordt opgeslagen, verwerkt of verzonden.

5. **Gemeenschappelijke minimumnormen**

Het Europees Parlement zorgt ervoor dat gemeenschappelijke minimumnormen inzake veiligheid in acht worden genomen door alle ontvangers van EUCI, zowel in de instelling als onder haar bevoegdheid vallend, namelijk alle afdelingen en contractanten, zodat deze informatie kan worden doorgegeven in het vertrouwen dat zij met dezelfde zorg zal worden behandeld. Deze minimumnormen omvatten criteria voor de veiligheidsmachtiging van ambtenaren en personeelsleden van het Europees Parlement en andere parlementaire medewerkers die in dienst van de politieke groepen zijn, en procedures voor de bescherming van vertrouwelijke informatie.

Het Europees Parlement verleent externe instanties alleen toegang tot de bedoelde informatie op voorwaarde dat deze instanties ervoor zorgen dat deze informatie wordt behandeld in overeenstemming met voorschriften die minstens volstrekt gelijkwaardig aan deze minimumnormen zijn.

Dergelijke gemeenschappelijke minimumnormen moeten ook worden toegepast, wanneer het Europees Parlement uit hoofde van een opdracht of een subsidieovereenkomst taken aan industriële of andere entiteiten toekent, waarbij vertrouwelijke informatie in het geding is.

6. **Veiligheid voor de ambtenaren van het Europees Parlement en andere personeelsleden van het Parlement die in dienst van de politieke groepen zijn**

6.1. *Veiligheidsinstructies voor ambtenaren van het Europees Parlement en andere parlementaire medewerkers die in dienst van de politieke groepen zijn*

Ambtenaren van het Europees Parlement en andere parlementaire medewerkers die in dienst van de politieke groepen zijn, in functies waardoor zij toegang kunnen hebben tot gerubriceerde EUCI, krijgen bij het opnemen van hun taak en daarna met regelmatige tussenpozen grondige instructies over de noodzaak van beveiliging en de procedures om die beveiliging door te voeren. Deze personen moeten schriftelijk bevestigen dat zij de toepasselijke bepalingen inzake veiligheid hebben gelezen en volledig hebben begrepen.

6.2. *Verantwoordelijkheden van leidinggevenden*

Leidinggevenden zijn ertoe verplicht de leden van hun personeel die bij werkzaamheden betreffende vertrouwelijke informatie betrokken zijn, of toegang hebben tot beveiligde communicatie- of informatiesystemen, te kennen en om incidenten of manifeste zwakke plekken die gevolgen voor de veiligheid kunnen hebben, te registreren en te melden.

6.3. *Veiligheidsstatus van ambtenaren en andere parlementaire medewerkers die in dienst van de politieke groepen zijn*

Er worden procedures ingesteld om ervoor te zorgen dat, wanneer negatieve informatie bekend wordt over een ambtenaar van het Europees Parlement of een andere parlementaire medewerker die werkzaam is voor een fractie, stappen worden ondernomen om vast te stellen of het werk van deze persoon hem of haar in contact heeft gebracht met vertrouwelijke informatie en of hij of zij toegang heeft tot beveiligde communicatie- of informatiesystemen, en dat de bevoegde dienst van het Europees Parlement wordt ingelicht. Als vast komt te staan dat de bedoelde persoon een veiligheidsrisico met zich meebrengt, zal hij of zij uitgesloten of ontheven worden van zijn of haar taken, waar hij of zij de veiligheid in gevaar kan brengen.

7. **Fysieke veiligheid**

Fysieke veiligheid houdt in: de toepassing van fysieke en technische beschermingsmaatregelen om niet-geautoriseerde toegang tot EUCI te voorkomen.

7.1. *De noodzaak van bescherming*

Het niveau van de fysieke beveiligingsmaatregelen die moeten worden toegepast om de bescherming van EUCI te waarborgen, moet in verhouding staan tot de rubricering en tot de omvang van, en de bedreiging voor, de aanwezige gegevens en het aanwezige materiaal. Alle houders van gerubriceerde EU-gegevens volgen voor de rubricering van die gegevens uniforme praktijken en moeten voldoen aan gemeenschappelijke beschermingsnormen met betrekking tot bewaring, overdracht en verwijdering van informatie en materiaal die moeten worden beschermd.

7.2. *Controle*

Alvorens zones die EUCI bevatten, onbeheerd achter te laten, zorgen personen die met de bewaring zijn belast, ervoor dat de gegevens veilig zijn opgeborgen en dat alle beveiligingsmiddelen (sloten, alarmen enz.) geactiveerd zijn. Aanvullende onafhankelijke controles worden na afloop van de werktijden uitgevoerd.

7.3. *Beveiliging van gebouwen*

Gebouwen waar EUCI of beveiligde communicatie- en informatiesystemen zijn ondergebracht, worden tegen niet-geautoriseerde toegang beschermd.

De aard van de bescherming die voor EUCI wordt gebruikt, bijvoorbeeld tralies voor vensters, deursloten, bewakers bij de ingangen, automatische toegangscontrolesystemen, veiligheidscontroles en -patrouilles, alarmsystemen, indringerdetectiesystemen en waakhonden, hangt af van:

a) de rubricering, het volume en de locatie binnen het gebouw, van de te beschermen gegevens en het materiaal;

b) de kwaliteit van de opbergmiddelen voor de beveiliging van de betreffende gegevens en materiaal; en

c) de fysieke aard en locatie van het gebouw.

De aard van de bescherming die wordt gebruikt voor communicatie- en informatiesystemen, hangt af van een beoordeling van de waarde van deze systemen en de potentiële schade als zij gecompromitteerd zouden worden, de fysieke aard en locatie van het gebouw waar het systeem is ondergebracht, en van de locatie van dat systeem binnen het gebouw.

7.4. *Noodplannen*

Er worden vooraf gedetailleerde plannen opgesteld voor de bescherming van vertrouwelijke informatie gedurende noodsituaties.

8. **Beveiligingsindicatoren, markeringen, het aanbrengen en het beheer van de rubriceringen**

8.1. *Beveiligingsindicatoren*

Andere rubriceringen dan gedefinieerd in artikel 2 van dit besluit, zijn niet toegestaan.

Een overeengekomen beveiligingsindicator mag worden gebruikt om de geldigheidsduur van een rubricering te beperken (wat voor gerubriceerde gegevens inhoudt dat zij automatisch lager worden gerubriceerd of worden gederubriceerd). Deze beveiligingsindicator is hetzij „TOT … (uur/datum)" hetzij „TOT … (feit)".

Aanvullende beveiligingsindicatoren, zoals CRYPTO of andere door de EU erkende beveiligingsindicatoren, worden gebruikt wanneer er een behoefte is aan een beperkte verspreiding en een bijzondere behandeling die nodig is in aanvulling op de behandeling die geldt op grond van de rubricering.

Beveiligingsindicatoren worden alleen gebruikt in combinatie met een rubricering.

8.2. *Markeringen*

Er kan een markering worden gebruikt om te specificeren op welk domein het document betrekking heeft, om te specificeren dat er sprake is van een speciale verspreiding op een „need to know"-basis of, voor niet-gerubriceerde gegevens, om het einde van een publicatieverbod aan te geven.

Een markering is geen rubricering en mag niet in plaats daarvan worden gebruikt.

8.3. *Aanbrengen van een rubricering en van beveiligingsindicatoren*

De rubricering wordt als volgt aangebracht:

a) op documenten die als „RESTREINT UE/EU RESTRICTED" zijn gerubriceerd: met mechanische of elektronische middelen;

b) op documenten die als „CONFIDENTIEL UE/EU CONFIDENTIAL" zijn gerubriceerd: met mechanische middelen of met de hand of door het drukken op voorgemerkt, geregistreerd papier;

c) op documenten die als „SECRET UE/EU SECRET" en „TRÈS SECRET UE/EU TOP SECRET" zijn gerubriceerd: met mechanische middelen of met de hand.

Beveiligingsindicatoren worden aangebracht onmiddellijk onder de rubricering, met dezelfde middelen als die voor de rubricering zijn gebruikt.

8.4. *Beheer van de rubriceringen*

8.4.1. Algemeen

Gegevens worden alleen gerubriceerd wanneer dat noodzakelijk is. De rubricering wordt duidelijk en correct aangegeven en wordt slechts zo lang gehandhaafd als de gegevens beschermd moeten worden.

De verantwoordelijkheid voor het rubriceren van gegevens en een eventuele lagere rubricering of derubricering nadien, berust uitsluitend bij de bron.

Ambtenaren van het Europees Parlement rubriceren informatie, geven deze een lagere rubricering of derubriceren deze op instructie van of volgens een delegatie van de secretaris-generaal.

De gedetailleerde procedures voor de behandeling van gerubriceerde documenten zijn zo opgezet, dat zij een bescherming bieden die passend is voor de inhoud die zij bevatten.

Het aantal personen dat gemachtigd is om „TRÈS SECRET UE/EU TOP SECRET"-documenten op te stellen, wordt tot een minimum beperkt, en hun namen worden op een lijst geplaatst die door de CIS wordt bijgehouden.

8.4.2. Rubricering

Het rubriceringsniveau van een document wordt bepaald naar gelang van het niveau van gevoeligheid van de inhoud, overeenkomstig de definities in artikel 2, onder c. Het is belangrijk dat met rubricering op een correcte en zuinige wijze wordt omgesprongen, en in het bijzonder met betrekking tot de rubricering „TRÈS SECRET UE/EU TOP SECRET".

De rubricering van een brief of nota die bijvoegsels bevat, is even hoog als die van het hoogst gerubriceerde bijvoegsel. De opsteller moet duidelijk aangeven, welke rubricering op de brief of nota moet worden toegepast, indien deze van de bijvoegsels wordt gescheiden.

De opsteller van een te rubriceren document houdt rekening met de hierboven uiteengezette regels en moet weerstand bieden aan elke neiging om het document te hoog of te laag te rubriceren.

Afzonderlijke bladzijden, paragrafen, afdelingen, bijlagen, aanhangsels, aanhechtsels en bijvoegsels van een gegeven document kunnen verschillende rubriceringen vereisen en worden dienovereenkomstig gerubriceerd. De rubricering van het document als geheel is die van het hoogst gerubriceerde deel ervan.

9. **Inspecties**

De maatregelen voor de beveiliging van EUCI worden periodiek geïnspecteerd door het directoraat Veiligheid en risicobeoordeling van het Europees Parlement, dat voor deze taak kan worden bijgestaan door de CIS.

Het directoraat Veiligheid en risicobeoordeling van het Europees Parlement en de veiligheidsdiensten van andere EU-instellingen, instanties, bureaus en agentschappen die krachtens of op basis van de Verdragen zijn opgericht, waar gerubriceerde EU-gegevens zijn ondergebracht, kunnen ook overeenkomen wederzijdse beoordelingen van de maatregelen voor de beveiliging EUCI uit te voeren.

10. **Procedure voor derubricering**

10.1. De CIS onderzoekt EUCI en doet de opsteller voorstellen voor derubricering uiterlijk het 25ste jaar na de datum waarop een document is opgesteld. Documenten die niet bij het eerste onderzoek zijn gederubriceerd, worden op gezette tijden, maar ten minste om de vijf jaar, opnieuw onderzocht.

10.2. Naast de documenten die zich momenteel in het beveiligde archief bevinden en die naar behoren zijn gerubriceerd, kan het derubriceringsproces ook betrekking hebben op andere vertrouwelijke gegevens die zich of in de beveiligde archieven of in het Archief en documentatiecentrum van het Europees Parlement (CARDOC) bevinden.

10.3. De CIS is er namens de opsteller van het document verantwoordelijk voor dat de geadresseerden van het document van de wijziging op de hoogte worden gebracht, en deze geadresseerden zijn er op hun beurt verantwoordelijk voor dat de daaropvolgende geadresseerden, aan wie zij het document hebben toegezonden of voor wie zij het gekopieerd hebben, van de wijziging op de hoogte worden gebracht.

10.4. Derubricering heeft geen gevolgen voor eventuele markeringen die op het document zichtbaar zijn.

10.5. De oorspronkelijke rubricering boven- en onderaan elke pagina wordt doorgehaald. De eerste pagina (schutblad) van het document wordt afgestempeld en de referentie van de CIS wordt erop aangebracht.

10.6. De tekst van het gederubriceerde document wordt gehecht aan de elektronische fiche of het equivalente systeem waar het is geregistreerd.

10.7. In het geval van documenten die vallen onder de uitzondering betreffende de persoonlijke levenssfeer of de integriteit van het individu, of de uitzondering betreffende commerciële belangen van natuurlijke en rechtspersonen en in het geval van gevoelige documenten, geldt artikel 2 van Verordening (EEG, Euratom) nr. 354/83 van de Raad.

10.8. Naast de bepalingen van punten 10.1 tot en met 10.7 gelden de volgende regels:

a) voor de documenten van derden zal de CIS de derde raadplegen alvorens tot derubricering over te gaan. De derde heeft 8 weken om opmerkingen toe te zenden;

b) in verband met de uitzondering betreffende de persoonlijke levenssfeer en de integriteit van het individu zal bij de procedure voor derubricering rekening worden gehouden met, in het bijzonder, de instemming van de persoon in kwestie, de onmogelijkheid de persoon in kwestie te identificeren en/of het feit dat deze persoon niet meer in leven is;

c) in verband met de commerciële belangen van een natuurlijke persoon of een rechtspersoon kan de persoon in kwestie op de hoogte worden gebracht via publicatie in het *Publicatieblad van de Europese Unie*, met een tijdslimiet van 4 weken voor eventuele opmerkingen.

DEEL 2

PROCEDURE VOOR HET VEILIGHEIDSONDERZOEK

11. **Veiligheidsonderzoek voor leden van het Europees Parlement**

11.1. Gelet op de prerogatieven en de bevoegdheden van het Europees Parlement kan aan de leden toegang worden verleend tot EUCI tot en met het niveau „CONFIDENTIEL UE/EU CONFIDENTIEL", zonder veiligheidsmachtiging. Voor informatie die als „CONFIDENTIEL UE/EU CONFIDENTIAL" is gerubriceerd, tekenen zij een plechtige verklaring dat zij de inhoud van de documenten in kwestie niet aan een derde bekend zullen maken.

11.2. Om toegang te krijgen tot als „TRÈS SECRET UE/EU TOP SECRET" en „SECRET UE/EU SECRET" gerubriceerde informatie, moeten de leden van het Europees Parlement gemachtigd zijn volgens de procedure in de punten 11.3 en 11.4 van deze afdeling.

11.3. Machtiging wordt alleen verleend aan leden van het Europees Parlement die een veiligheidsonderzoek door de bevoegde nationale instanties van de lidstaten hebben ondergaan in overeenstemming met de procedure in de punten 11.9 tot en met 11.14. De voorzitter is verantwoordelijk voor het verlenen van machtiging aan de leden.

11.4. De voorzitter verleent een machtiging na verkrijging van het advies van de bevoegde nationale instanties van de lidstaten, dat gebaseerd is op het veiligheidsonderzoek dat overeenkomstig de punten 11.8 tot en met 11.13 is uitgevoerd.

11.5. Het directoraat Veiligheid en risicobeoordeling van het Europees Parlement houdt een bijgewerkte lijst bij van alle leden van het Europees Parlement, aan wie een machtiging is verleend, inclusief een voorlopige machtiging in de zin van punt 11.15.

11.6. Een machtiging is geldig voor een periode van vijf jaar of voor de duur van de taken, waarvoor de machtiging is verleend, welke het kortste is. Zij kan worden verlengd volgens de procedure van punt 11.4.

11.7. Een machtiging wordt door de voorzitter ingetrokken, als hij/zij van mening is dat hier gegronde redenen voor zijn. Van ieder besluit tot intrekking van een machtiging wordt kennis gegeven aan het lid van het Europees Parlement in kwestie, die kan verzoeken door de voorzitter te worden gehoord voordat de intrekking van kracht wordt, en aan de bevoegde nationale instantie.

11.8. Een veiligheidsonderzoek wordt uitgevoerd met de medewerking van het lid van het Europees Parlement in kwestie en op verzoek van de voorzitter. De nationale instantie van die de lidstaat, waarvan het lid aan wie een machtiging moet worden verleend onderdaan is, is bevoegd om het onderzoek uit te voeren.

11.9. Als onderdeel van het veiligheidsonderzoek moet het lid van het Europees Parlement in kwestie een formulier met persoonlijke gegevens invullen.

11.10. De voorzitter specificeert in zijn/haar verzoek aan de bevoegde nationale instanties het niveau van de gerubriceerde gegevens waartoe het lid in kwestie toegang moet krijgen, zodat zij het veiligheidsonderzoek kunnen uitvoeren.

11.11. Het gehele veiligheidsonderzoek dat door de nationale instanties wordt uitgevoerd, samen met het verkregen resultaat, moet voldoen aan de ter zake vigerende voorschriften in de lidstaat in kwestie, inclusief de regels inzake beroep.

11.12. Als de bevoegde nationale instanties van de lidstaat een positief advies uitbrengen, mag de voorzitter het lid van het Europees Parlement in kwestie de machtiging verlenen.

11.13. Een negatief advies van de bevoegde nationale instanties wordt kennis gegeven aan het lid van het Europees Parlement in kwestie, die mag vragen te worden gehoord door de voorzitter. Als de voorzitter het nodig acht, kan hij/zij de bevoegde nationale instanties vragen om een nadere toelichting te geven. Indien het negatieve advies wordt bevestigd, wordt geen machtiging verleend.

11.14. Alle leden van het Europees Parlement aan wie een machtiging wordt verleend als bedoeld in 11.3, ontvangen op het tijdstip dat de machtiging wordt verleend en vervolgens daarna met regelmatige tussenpozen, alle noodzakelijke richtlijnen over de bescherming van vertrouwelijke informtie en de wijze waarop deze bescherming kan worden gewaarborgd. Deze leden ondertekenen een verklaring waarin zij de ontvangst van deze richtlijnen bevestigen.

11.15. In uitzonderlijke omstandigheden mag de voorzitter, nadat hij/zij de nationale bevoegde instanties heeft geïnformeerd en mits deze niet binnen een maand reageren, aan een lid van het Europees Parlement een voorlopige machtiging geven voor een periode van hoogstens zes maanden, in afwachting van het resultaat van het onderzoek als bedoeld onder 11.11. De voorlopige machtigingen die aldus worden verleend, geven geen toegang tot gegevens die als „TRÈS SECRET UE/EU TOP SECRET" zijn gerubriceerd.

12. **Veiligheidsonderzoek van de ambtenaren van het Parlement en andere Parlementaire medewerkers die in dienst van de politieke groepen zijn**

12.1. Alleen ambtenaren en andere parlementaire medewerkers die in dienst van de politieke groepen zijn, die wegens hun functie en de eisen van hun dienst, kennis moeten nemen of gebruik moeten maken van gerubriceerde gegevens, krijgen toegang tot deze gegevens.

12.2. Om toegang te krijgen tot gegevens die als „TRÈS SECRET UE/EU TOP SECRET, SECRET UE/EU SECRET" en „CONFIDENTIEL UE/EU CONFIDENTIAL" zijn gerubriceerd, moeten de in onder 12.1 genoemde personen gemachtigd zijn volgens de procedure zoals neergelegd onder 12.3 en 12.4 van deze afdeling.

12.3. Machtiging wordt alleen verleend aan de onder 12.1 genoemde personen die een veiligheidsonderzoek door de bevoegde nationale instanties van de lidstaten (NSA's) hebben ondergaan, in overeenstemming met de procedure genoemd onder 12.9 tot en met 12.14. De secretaris-generaal is verantwoordelijk voor de verlening van de machtiging voor ambtenaren van het Europees Parlement en andere parlementaire medewerkers die in dienst van de politieke groepen zijn.

12.4. De secretaris-generaal verleent een machtiging nadat hij of zij het advies van de bevoegde nationale instanties van de lidstaten heeft gekregen, dat is gebaseerd op een veiligheidsonderzoek dat in overeenstemming met de punten 12.8 tot en met 12.13 is uitgevoerd.

12.5. Het directoraat Veiligheid en risicobeoordeling van het Europees Parlement houdt een bijgewerkte lijst bij van alle posten waarvoor een veiligheidsmachtiging nodig is, zoals aangegeven door de betrokken afdelingen van het Europees Parlement, alsmede een lijst van alle personen aan wie een machtiging, inclusief een tijdelijke machtiging, als bedoeld in artikel 12.15, is verleend.

12.6. De machtiging wordt verleend voor een periode van vijf jaar of voor de duur van de taken, waarvoor de machtiging verleend is, welke het kortste is. Zij kan worden verlengd volgens de procedure genoemd onder 12.4.

12.7. Een machtiging wordt door de secretaris-generaal ingetrokken, als hij/zij van mening is dat hier gegronde redenen voor zijn. Van ieder besluit tot intrekking van een machtiging wordt kennis gegeven aan de betreffende ambtenaar van het Europees Parlement of aan de betreffende parlementaire medewerker die voor de fracties werkt. Die kan verzoeken om door de secretaris-generaal te worden gehoord voordat de intrekking van kracht wordt, en aan de bevoegde nationale instantie.

12.8. Een veiligheidsonderzoek wordt uitgevoerd met de medewerking van de persoon in kwestie en op verzoek van de secretaris-generaal. De nationale instantie die bevoegd is om het onderzoek uit te voeren, is die van de lidstaat waarvan de persoon aan wie een machtiging moet worden verleend, onderdaan is. Als de nationale wet- en regelgeving dit toestaan, mogen NSA's of andere bevoegde nationale autoriteiten onderzoeken uitvoeren naar niet-onderdanen die toegang tot informatie vragen die als „CONFIDENTIEL UE/EU CONFIDENTIAL" of hoger zijn gerubriceerd.

12.9. Als onderdeel van het veiligheidsonderzoek moet de betreffende ambtenaar van het Europees Parlement of de betreffende parlementaire medewerker die werkt voor de fracties, een formulier met persoonlijke gegevens invullen.

12.10. De secretaris-generaal specificeert in zijn/haar verzoek aan de nationale autoriteiten het niveau van de gerubriceerde gegevens die aan de betreffende persoon ter beschikking moet worden gesteld, zodat de bevoegde nationale instanties het veiligheidsonderzoek kunnen uitvoeren en hun advies kunnen geven over het machtigingsniveau dat voor de persoon in kwestie geschikt is.

12.11. Het gehele veiligheidsonderzoek dat door de nationale instanties wordt uitgevoerd, samen met het verkregen resultaat, moet voldoen aan de ter zake vigerende voorschriften in de lidstaat in kwestie, inclusief de regels inzake beroep.

12.12. Als de bevoegde nationale instanties van de lidstaat een positief advies uitbrengen, kan de secretaris-generaal de persoon in kwestie de machtiging verlenen.

12.13. Van een negatief advies van de bevoegde nationale instanties wordt kennis gegeven aan de betreffende ambtenaar van het Europees Parlement of de betreffende parlementaire medewerker die werkt voor de fracties. Die mag vragen te worden gehoord door de secretaris-generaal. Als de secretaris-generaal het nodig acht, kan hij/zij de bevoegde nationale instanties vragen waar mogelijk een nadere toelichting te geven. Indien het negatieve advies wordt bevestigd, wordt geen machtiging verleend.

12.14. Alle ambtenaren van het Europees Parlement en alle parlementaire medewerkers die in dienst van de politieke groepen zijn, aan wie machtiging wordt verleend in de zin van de punten 12.4 en 12.5, ontvangen op het tijdstip dat de machtiging wordt verleend en vervolgens daarna met regelmatige tussenpozen, alle noodzakelijke richtlijnen betreffende de bescherming van vertrouwelijke informatie en de wijze waarop deze kan worden gewaarborgd. Deze ambtenaren van het Europees Parlement en de andere parlementaire medewerkers die in dienst van de politieke groepen zijn, ondertekenen een verklaring waarin zij erkennen de richtlijnen te hebben ontvangen en zich ertoe verplichten deze op te volgen.

12.15. In uitzonderlijke omstandigheden mag de secretaris-generaal, nadat hij/zij de nationale bevoegde instanties heeft geïnformeerd en mits deze niet binnen een maand hebben gereageerd, een voorlopige machtiging verlenen aan een ambtenaar van het Parlement of een parlementaire medewerker die in dienst van de politieke groepen is, voor een periode van hoogstens zes maanden, in afwachting van het resultaat van het onderzoek als bedoeld onder 11.11. De voorlopige machtigingen die aldus worden verleend, geven geen toegang tot gegevens die als „TRÈS SECRET UE/EU TOP SECRET” zijn gerubriceerd.