

SERVICE PUBLIC FEDERAL JUSTICE,
SERVICE PUBLIC FEDERAL INTERIEUR
ET MINISTERE DE LA DEFENSE

[C – 2024/011702]

20 DECEMBRE 2024. — Arrêté royal portant exécution de la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, aux avis de sécurité et au service public réglementé

RAPPORT AU ROI

Sire,

Le présent projet soumis à Votre Signature respecte la circulaire du 27 mai 2024 du Premier Ministre relative aux affaires courantes. La circulaire précitée prévoit notamment que « les affaires qui n'exigent aucune initiative nouvelle de la part du Gouvernement et pour lesquelles la continuité du pouvoir impose l'intervention du Pouvoir exécutif sous peine de créer une carence préjudiciable aux citoyens, doivent être traitées. Il est toujours possible, après avoir recueilli l'avis du Conseil d'Etat, de finaliser des textes réglementaires dont la préparation a été entamée bien avant la période critique, et qui ont fait l'objet, d'une part, d'une négociation sectorielle clôturée par la signature d'un protocole d'accord et, d'autre part, de l'accord des Ministres compétents, particulièrement dans le cadre du contrôle administratif, budgétaire et de gestion ».

Le projet a été approuvé par le Conseil des Ministres du 26 avril 2024 et a ensuite été soumis à l'avis du Conseil d'Etat.

La loi du 7 avril 2023 portant modification de la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, attestations de sécurité et avis de sécurité (*Moniteur belge* du 9 juin 2023, éd. 1) a modifié la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, attestations de sécurité et avis de sécurité de manière fondamentale.

La loi du 7 avril 2023 est entrée en vigueur le 31 décembre 2023.

En exécution de la loi du 7 avril 2023, les modalités de protection des informations classifiées (y compris celles du nouveau niveau de classification « RESTREINT ») doivent être fixées par arrêté royal.

L'objectif de ces mesures de protection est de clarifier les règles relatives à l'utilisation des informations classifiées dans un monde où la dématérialisation est de plus en plus rapide et les besoins des acteurs privés et des partenaires étrangers en matière d'information sont accrus.

Le présent arrêté vise également à contrôler avec une rigueur accrue la manière dont la classification des informations est utilisée. La classification des informations s'applique uniquement si elle est strictement nécessaire à la protection de l'un des intérêts fondamentaux du pays, tels qu'énumérés de manière exhaustive à l'article 3, § 1^{er}, de la loi du 11 décembre relative à la classification, aux habilitations de sécurité, avis de sécurité et au service public réglementé (ci-après dénommée « Loi relative à la classification »). Le gouvernement souhaite toutefois également trouver un équilibre entre la protection de ces intérêts fondamentaux et la nécessité d'une transparence (accrue).

Optimiser la classification (sans nécessairement étendre ce processus) offre une meilleure protection. Classifier requiert toutefois une attention particulière : il convient de choisir le niveau de classification correct et le marquage doit être appliqué de manière juste et complète à l'information. Tant la surclassification que la sous-classification comportent un risque pour la sécurité du pays : (1) en cas de surclassification, l'autorité n'est pas toujours en mesure de réagir de manière appropriée ; cette surclassification entraîne une dévalorisation du secret protégé et une érosion progressive du respect des mesures de protection ; (2) en cas de sous-classification, l'accès à l'information est facilité pour les acteurs étrangers ou hostiles qui souhaitent nuire aux intérêts protégés.

Les règles de marquage permettent de garantir que toute personne qui entre en contact avec les informations sache clairement qu'il s'agit d'informations classifiées, et donc protégées. Le caractère protégé doit être clair, étant donné que l'utilisation inappropriée de ces informations peut être sanctionnée pénalement.

Par conséquent, la classification et la déclassification ne sont pas une sinécure et exigent des règles claires.

La loi du 7 avril 2023 susmentionnée a introduit un nouveau niveau de classification « RESTREINT », qui s'ajoute aux trois niveaux de classification existants : « CONFIDENTIEL », « SECRET » et « TRÈS SECRET ».

FEDERALE OVERHEIDSDIENST JUSTITIE,
FEDERALE OVERHEIDSDIENST BINNENLANDSE ZAKEN
EN MINISTERIE VAN LANDSVERDEDIGING

[C – 2024/011702]

20 DECEMBER 2024. — Koninklijk besluit tot uitvoering van de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, de veiligheidsadviezen en de publiek gereguleerde dienst

VERSLAG AAN DE KONING

Sire,

Dit ontwerp dat U ter ondertekening wordt voorgelegd, respecteert de omzendbrief van de Eerste Minister van 27 mei 2024 betreffende de lopende zaken. De voornoemde omzendbrief bepaalt onder meer dat "de zaken waarvoor geen nieuw initiatief van de Regering is vereist en die met het oog op de continuïteit van het gezag door de Uitvoerende Macht moeten worden behandeld, omdat anders een voor de burgers nadelig vacuüm zou ontstaan, moeten worden voortgezet. Het blijft steeds mogelijk om, na het inwinnen van het advies van de Raad van State, reglementaire teksten te finaliseren waarvan de voorbereiding aangevat werd lang vóór de kritieke periode, en die na sectorale onderhandelingen, enerzijds, geleid hebben tot de ondertekening van een protocolakkoord en, anderzijds, geleid hebben tot een akkoord van de bevoegde Ministers, in het bijzonder in het raam van de administratieve, begrotings- en beheerscontrole".

Het ontwerp werd goedgekeurd door de Ministerraad van 26 april 2024 en vervolgens voor advies voorgelegd aan de Raad van State.

De wet van 7 april 2023 houdende wijziging van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen (*Belgisch Staatsblad* 9 juni 2023, éd. 1) wijzigde de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen op fundamentele wijze.

De wet van 7 april 2023 trad in werking op 31 december 2023.

In uitvoering van de wet van 7 april 2023 moeten de nadere regels van de bescherming van geclassificeerde informatie (waaronder deze voor het nieuwe classificatieniveau "BEPERKT") bij koninklijk besluit worden vastgelegd.

Het doel van deze beschermingsmaatregelen is om in een wereld van steeds snellere dematerialisatie en groeiende informatienoden van particuliere actoren en buitenlandse partners de regels te verduidelijken met betrekking tot de aanwending van geclassificeerde informatie.

Voorliggend besluit beoogt tevens met een verhoogde rigiditeit toe te zien op de wijze waarop een beroep wordt gedaan op het classificeren van informatie. Het classificeren van informatie kan enkel indien dit strikt gezien noodzakelijk is voor de bescherming van één van de fundamentele belangen van het land zoals exhaustief opgesomd in artikel 3, § 1 van de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, de veiligheidsadviezen en de publiek gereguleerde dienst (hierna "Classificatiewet"). Het is echter ook de wens van de regering om een evenwicht te vinden tussen de bescherming van deze fundamentele belangen en de nood aan (meer) openheid.

Beter (maar niet noodzakelijk meer) classificeren leidt tot een betere bescherming. Classificeren vereist echter zorgvuldigheid: zo dient het correcte classificatieniveau gekozen te worden en moet de markering juist en volledig aangebracht worden op de informatie. Zowel het overals het onderclassificeren houden een risico in voor de veiligheid van het land: (1) indien er wordt overgeclassificeerd, leidt dit ertoe dat de overheid niet altijd op de gepaste manier kan reageren; het leidt tot een devaluatie van het geheim dat wordt beschermd en een geleidelijke erosie van de naleving van de beschermingsmaatregelen; (2) indien er wordt ondergeclassificeerd wordt de toegang van de informatie vergemakkelijkt voor buitenlandse of vijandige actoren die afbreuk wensen te doen aan de beschermde belangen.

De regels inzake het aanbrengen van de markering zorgen ervoor dat eenieder die in aanraking komt met de informatie duidelijk weet dat het om geclassificeerde -en dus beschermde- informatie gaat. Aangezien de niet-geëigende aanwending strafrechtelijk kan gesanctioneerd worden moet het beschermde karakter duidelijk zijn.

Classificeren en declassificeren zijn bijgevolg geen sinecure en vereisen duidelijke regels.

Voormelde wet van 7 april 2023 voerde een nieuw classificatieniveau "BEPERKT" in, naast de drie reeds bestaande classificatieniveaus: "VERTROUWELIJK", "GEHEIM" en "ZEER GEHEIM".

La protection assurée par chacun de ces niveaux de classification consiste en un ensemble de mesures de protection minimales. Ces mesures sont réparties en cinq catégories : les mesures applicables à la gestion des informations classifiées, la sécurité des personnes (morales), les mesures de protection liées aux marchés publics, la sécurité physique et la sécurité des systèmes de communication et d'information (voir l'article 7 de la loi relative à la classification). Ces cinq catégories figurent également dans le cadre réglementaire de l'UE, de l'OTAN et de l'ESA, dont les auteurs du présent arrêté se sont inspirés.

Le présent arrêté régit également le contrôle de la mise en œuvre de ces mesures de protection.

En outre, il clarifie les rôles et les responsabilités de chaque acteur impliqué dans la protection des informations classifiées. Lorsque tous les membres d'une organisation connaissent leurs tâches et responsabilités spécifiques en matière d'informations classifiées, le risque de malentendu et de négligence est considérablement réduit. Une structure dûment définie permet de réagir rapidement et efficacement aux éventuels incidents de sécurité et à la compromission d'informations classifiées. Les bonnes personnes sont mobilisées au bon moment.

Dans son avis, le Conseil d'État a émis la recommandation suivante : « Dans un souci de sécurité juridique et compte tenu de la matière sensible réglée par le projet, la publication au *Moniteur belge* de l'arrêté qui en résultera gagnerait à être accompagnée d'un rapport au Roi permettant d'en expliciter les dispositions ». Voici qui répond à cette recommandation.

De manière générale, le Conseil d'État a fait remarquer qu'en vertu des articles 4, 13, 22, 23, 29, 31, 39, 41, 49, 54, 58, 60, 64, 70, 84, alinéa 2, 95, 96 et 98 du projet initial, le Conseil national de Sécurité était chargé de prendre des mesures qualifiées de mesures complémentaires de nature administrative et technique ou de proposer des directives, mais que les mesures que le Conseil national de Sécurité pouvait prendre en vertu des articles précités du projet semblaient avoir un caractère réglementaire, ce qui n'était pas acceptable et devait dès lors faire l'objet d'une révision. Le Conseil d'État a ajouté que, selon une pratique consultative établie, les délégations telles que celles envisagées dans le projet ne pouvaient être acceptées que pour des raisons pratiques et dans la mesure où celles-ci avaient une portée très limitée ou principalement technique, et pour autant que l'on puisse partir du principe que les organismes chargés d'appliquer ou de contrôler la réglementation en question soient également les mieux placés pour l'élaborer en connaissance de cause. Chaque disposition mentionnant les directives du Conseil national de Sécurité a donc été examinée à la lumière de cet avis quant à (1) la nature et la nécessité des directives et (2) la question de savoir si la délégation prévue était effectivement fondée sur des raisons pratiques et avait une portée très limitée (par exemple, parce qu'elle ne s'adresse qu'à certaines entités qui utilisent des informations classifiées ou qu'elle ne s'adresse qu'aux officiers de sécurité) ou essentiellement technique, ce qui permet de partir du principe que seule l'Autorité nationale de Sécurité, qui exerce le contrôle sur le respect des mesures de protection, est la mieux placée pour se prononcer en connaissance de cause. Les projets des nouvelles directives feront préalablement l'objet de concertation avec les experts des services partenaires qui siègent dans le Comité de coordination pour le Renseignement et la Sécurité, compte tenu des coûts que la mise en œuvre de telles directives peut entraîner. Cette concertation préalable a pour but d'expliquer et de clarifier les directives, si nécessaire.

À la suite de la remarque formulée par le Conseil d'État selon laquelle aucune base juridique n'autorisait le Roi à prendre des dispositions au sujet des informations non classifiées et, le cas échéant, à qualifier ces informations de « SENSIBLE NON CLASSIFIÉ », le titre IV a été supprimé du projet d'arrêté. Par conséquent, le présent arrêté ne compte plus que cinq titres au lieu de six. Les dispositions transitoires et finales prévoient cependant une réglementation pour les informations portant la mention « DIFFUSION RESTREINTE » afin de pouvoir les distinguer des informations classifiées au niveau de protection « RESTREINT ». Cette disposition est indépendante des éventuelles autres législations ou réglementations visant la protection des informations non classifiées.

De bescherming die elk van deze classificatieniveaus biedt, bestaat uit een reeks minimale beschermingsmaatregelen. Deze maatregelen worden onderverdeeld in vijf categorieën: maatregelen van toepassing voor het beheer van geclassificeerde informatie, (rechts-) persoonsgebonden beveiliging, beschermingsmaatregelen verbonden aan overheidsopdrachten, fysieke beveiliging en de beveiliging van communicatie- en informatiesystemen (zie artikel 7 van de Classificatiewet). Deze vijf categorieën komen ook voor in het regelgevend kader van de EU, NAVO en ESA, dat ter inspiratie diende voor de opstellers van voorliggend besluit.

Ook het toezicht op de tenuitvoerlegging van deze beschermingsmaatregelen wordt door voorliggend besluit geregeld.

Daarnaast verduidelijkt voorliggend besluit ook de rollen en verantwoordelijkheden van ieder die betrokken is bij de bescherming van de geclassificeerde informatie. Wanneer iedereen in een organisatie op de hoogte is van zijn of haar specifieke taken en verantwoordelijkheden met betrekking tot geclassificeerde informatie, wordt de kans op misverstanden en nalatigheid aanzienlijk verminderd. Een goed gedefinieerde structuur maakt het mogelijk om snel en doeltreffend te reageren op voorkomende veiligheidsincidenten en compromittering van geclassificeerde informatie. De juiste personen worden op het juiste moment ingeschakeld.

De Raad van State raadde in haar advies aan om “ter wille van de rechtszekerheid en rekening houdend met de gevoelige aangelegenheid die bij het ontwerp geregeld wordt, het besluit, in het vooruitzicht van de bekendmaking ervan in het *Belgisch Staatsblad*, te voorzien van een verslag aan de Koning waarin de bepalingen toegelicht worden”. Bij deze wordt voldaan aan deze aanbeveling.

In het algemeen maakte de Raad van State de opmerking dat bij de artikelen 4, 13, 22, 23, 29, 31, 39, 41, 49, 54, 58, 60, 64, 70, 84, tweede lid, 95, 96 en 98 van het oorspronkelijke ontwerp de Nationale Veiligheidsraad ermee wordt belast maatregelen te treffen die aangemerkt kunnen worden als bijkomende maatregelen van administratieve en technische aard of om richtlijnen voor te stellen, maar deze maatregelen die de Nationale Veiligheidsraad kan treffen krachtens de voornoemde artikelen van het ontwerp evenwel van veronderstelde aard blijken te zijn, hetgeen niet aanvaardbaar is en bijgevolg herzien moet worden. De Raad van State voegde er aan toe dat volgens een vaste adviespraktijk delegaties zoals die welke beoogd worden in het ontwerp enkel kunnen worden gebillijkt op grond van praktische redenen en voor zover zij een zeer beperkte of een hoofdzakelijk technische draagwijdte hebben, en voor zover ervan uitgegaan mag worden dat de instellingen die de betrokken reglementering dienen toe te passen of er toezicht op moeten uitoefenen, ook het best geplaatst zijn om deze met kennis van zaken uit te werken. Elke bepaling die de richtlijnen van de Nationale Veiligheidsraad vermeldde, werd dan ook in het licht van dit advies herzien op (1) de aard en de noodzaak van de richtlijnen en (2) of de opgenomen delegatie wel degelijk gegrond is op praktische redenen en een zeer beperkte (bijvoorbeeld omdat de richtlijn uitsluitend gericht is tot bepaalde entiteiten die geclassificeerde informatie aanwenden of omdat de richtlijn uitsluitend gericht is aan de veiligheidsofficieren) of een hoofdzakelijk technische draagwijdte heeft, waardoor ervan uitgegaan kan worden dat enkel de Nationale Veiligheidsraad, die ook het toezicht uitoefent op de naleving van de beschermingsmaatregelen, het best geplaatst is om zich daar met kennis van zaken over uit te spreken. De ontwerpen van nieuwe richtlijnen zullen ook voorafgaandelijk overlegd worden met de experts van de partnerdiensten die zetelen in het Coördinatiecomité voor Inlichting en Veiligheid, gelet op de implementatiekosten die dergelijke richtlijnen met zich kunnen meebrengen. Dit voorafgaandelijk overleg heeft als doel de richtlijn toe te lichten en te verduidelijken indien nodig.

Ten gevolge van de opmerking van de Raad van State dat er geen rechtsgrond aanwezig is die de Koning ertoe machtigt om te voorzien in bepalingen betreffende niet-geclassificeerde informatie en om die informatie, in voorkomend geval, te voorzien van de vermelding “GEVOELIG NIET-GECLASSIFICEERD” werd titel IV geschrapt uit het ontwerpbesluit. In de plaats van zes titels zijn er bijgevolg nog vijf titels in voorliggend besluit. In de overgangs- en slotbepalingen werd er wel nog een regeling voorzien voor de informatie die de vermelding “BEPERKTE VERSPREIDING” draagt om het onderscheid te kunnen maken met geclassificeerde informatie met het beschermingsniveau “BEPERKT”. Deze bepaling staat los van eventuele andere wet- of regelgeving die de bescherming van niet-geclassificeerde informatie beoogt.

Discussion des articles.

TITRE I. — DéfinitionsArticle 1^{er}

Le titre 1^{er} ne contient qu'un seul article, qui fournit une série de définitions.

1° La définition de la « loi » n'appelle pas de commentaire supplémentaire ;

2° La définition du « fonctionnaire dirigeant » est reprise de l'arrêté royal du 24 mars 2000. Les termes « et son remplaçant » sont maintenant ajoutés.

Le Comité permanent R note dans son avis que la délégation au remplaçant n'a pas de fondement juridique et renvoie à cet égard à l'article 1^{er}, 3°, de la loi relative à la classification. Le Comité permanent R estime qu'il n'existe aucune disposition permettant de déléguer cette tâche.

Les auteurs du projet soulignent que l'article 1^{er}, 3°, de la loi relative à la classification - auquel le Comité permanent R se réfère dans son avis - est inexistant. La définition de « fonctionnaire dirigeant » figure bien à l'article 1^{er}, 3°, de l'arrêté royal du 24 mars 2000. Dans le projet d'arrêté royal, les termes « et son remplaçant » ont été ajoutés pour que les compétences puissent être exercées par le chef faisant fonction en cas d'absence et/ou d'empêchement du fonctionnaire dirigeant ;

3° et 4° Les définitions de « compromission » et d'« incident de sécurité » sont reprises du document C-M(2002)49-REV 1 de l'OTAN du 20 novembre 2020. La distinction entre les deux termes réside dans le fait que, dans le cas d'une compromission, les données ont été mises en péril (et non potentiellement mises en péril). Dans le cas d'un incident de sécurité, seule une règle a été enfreinte sans qu'il ait été établi que les données ont été mises en péril. Dans son avis (p. 44), le Conseil d'État relève que la signification de la notion de « mettre en péril » correspond quant au fond à celle de « compromission ». En effet, ces deux notions peuvent être considérées comme des synonymes, étant entendu qu'en cas d'incident de sécurité, l'accent est mis sur « potentiellement ».

La définition de la compromission inclut la situation dans laquelle des services et moyens d'appui ont perdu leur intégrité ou leur disponibilité, en ce compris le déni de service. Le « déni de service » fait référence au fait de ne plus fonctionner correctement. À titre d'exemple, on cite une armoire cassée ou un réseau qui n'est pas opérationnel ;

5° et 6° Les définitions d'« Autorité nationale de Sécurité » et de « Conseil national de Sécurité » n'appellent pas de commentaires ;

7° La définition de « sécurité industrielle » repose, quant au fond, sur la définition du Conseil européen (Décision du Conseil européen du 23 septembre 2013 concernant les règles de sécurité aux fins de la protection des informations classifiées de l'UE (2013/488/UE) art. 11). Cette définition a été ajoutée pour garantir l'application des mesures de protection pendant la phase de négociation précontractuelle et pendant toute la durée des marchés publics classifiés. Les formulations utilisées dans cet article sont cohérentes avec les termes utilisés dans l'article 100 du présent arrêté ;

8° La définition de « titulaire » se fonde sur la définition du Conseil européen (Décision du Conseil européen du 23 septembre 2013 concernant les règles de sécurité aux fins de la protection des informations classifiées de l'UE (2013/488/UE) p. 42). La définition a été ajoutée afin de préciser qu'une distinction peut exister entre l'autorité d'origine et le titulaire d'informations classifiées. Ainsi, les personnes morales, telles que définies dans le cadre du présent arrêté, peuvent être détentrices d'informations classifiées, mais jamais autorités d'origine. Le titulaire a toujours un besoin d'en connaître ;

9° La définition de « porteur » est nouvelle. L'article 16 de l'arrêté royal du 24 mars 2000 faisait mention de « courrier spécial ». Ce terme prêtait à confusion, car sa signification exacte n'était pas claire.

Le terme « porteur » s'entend au sens large et inclut toute personne transportant des informations classifiées. Il s'agit notamment des entreprises publiques chargées de la distribution du courrier (par exemple Bpost), les entreprises de courrier privées et/ou les services de colis (par exemple DHL ou Fedex), les services postaux au sein d'une entreprise ou d'une administration (« courrier interne », huissiers, chauffeurs), etc.

Artikelsgewijze bespreking.

TITEL I. — Definities

Artikel 1

Titel 1 bevat slechts één artikel dat een aantal definities voorziet.

1° De definitie van “de wet” behoeft geen verdere commentaar;

2° De definitie van “leidend ambtenaar” werd overgenomen van het koninklijk besluit van 24 maart 2000. De woorden “en zijn plaatsvervanger” worden er nu aan toegevoegd.

Het Vast Comité I merkt in haar advies op dat de delegatie naar de plaatsvervanger geen wettelijke basis heeft en verwijst in dit verband naar artikel 1, 3° van de Classificatiewet. Er werd volgens het Vast Comité I niet voorzien in de mogelijkheid om deze opdracht te delegeren.

De opstellers van het ontwerp wijzen er op dat artikel 1, 3° van de Classificatiewet -waar het Vast Comité I naar verwijst in haar advies- onbestaande is. De definitie van “leidend ambtenaar” komt wel voor in artikel 1, 3° van het koninklijk besluit van 24 maart 2000. In het ontwerp koninklijk besluit werd “en zijn plaatsvervanger” toegevoegd om toe te laten dat de bevoegdheden konden uitgeoefend worden door het dienstdoende hoofd bij afwezigheid en/of verhindering van de leidende ambtenaar;

3° en 4° De definities van “compromittering” en “veiligheidsincident” zijn overgenomen uit NAVO document C-M (2002)49-REV 1 van 20 november 2020. Het onderscheid tussen beide begrippen ligt in het feit dat bij compromittering de gegevens in gevaar werden gebracht (en niet mogelijk in gevaar werden gebracht). Bij een veiligheidsincident werd er enkel een regel geschonden zonder dat het vaststaat dat de gegevens in gevaar gebracht werden. De Raad van State merkt op in haar advies (p. 44) dat de betekenis van de begrippen “in gevaar komen” inhoudelijk overeenkomen met die van “compromittering”. Beide begrippen zouden inderdaad kunnen worden opgevat als synoniemen met dien verstande dat bij veiligheidsincident de nadruk ligt op “mogelijk”.

De definitie van compromittering omvat de situatie waarin ondersteunende diensten en middelen hun integriteit en beschikbaarheid verloren hebben met inbegrip van ontzegging van dienst. Met “ontzegging van dienst” wordt bedoeld het niet meer naar behoren functioneren. Als voorbeeld vermelden we een kast die stuk is of een netwerk dat niet operationeel is;

5° en 6° De definities van “Nationale Veiligheidsoverheid” en “Nationale Veiligheidsraad” behoeven geen commentaar;

7° De definitie van “industriële veiligheid” is inhoudelijk gebaseerd op de definitie van de Europese Raad (Besluit van de Europese Raad van 23 september 2013 betreffende de beveiligingsvoorschriften voor de bescherming van gerubriceerde EU-informatie (2013/488/EU) art. 11). Deze definitie werd toegevoegd om de toepassing van de beschermingsmaatregelen te garanderen tijdens de precontractuele onderhandelingsfase en tijdens de volledige looptijd van geclassificeerde overheidsopdrachten. De bewoordingen gebruikt in dit artikel zijn in overeenstemming met het woordgebruik in artikel 100 van onderhavig besluit;

8° De definitie van “houder” is gebaseerd op de definitie van de Europese Raad (Besluit van de Europese Raad van 23 september 2013 betreffende de beveiligingsvoorschriften voor de bescherming van gerubriceerde EU-informatie (2013/488/EU) p. 43). De definitie werd toegevoegd om duidelijk te maken dat er een onderscheid kan bestaan tussen de overheid van oorsprong en de houder van geclassificeerde informatie. Zo kunnen rechtspersonen, zoals gedefinieerd in het kader van voorliggend besluit, wel houder zijn van geclassificeerde informatie, maar nooit overheid van oorsprong. Een houder beschikt steeds over de noodzaak tot kennisname;

9° De definitie van “drager” is nieuw. Artikel 16 van het koninklijk besluit van 24 maart van 2000 sprak over “speciale koerier”. Deze term gaf aanleiding tot verwarring, daar het onduidelijk was wat dit juist betekende.

De term “drager” heeft een ruime betekenis en omvat eenieder die geclassificeerde informatie vervoert. Hieronder wordt onder andere begrepen: overheidsbedrijven verantwoordelijk voor postbedeling (vb. Bpost), private koerierondernemingen en/of pakjesdiensten (vb. DHL of Fedex), postdiensten binnen een onderneming of overheid (“binnenpost”, bodes, chauffeurs), enz.

La définition a été ajoutée pour préciser qu'un porteur doit être titulaire d'une habilitation de sécurité. Cette exigence se justifie par le fait que l'expédition est souvent effectuée par la même personne. De plus, cette personne est en possession d'informations classifiées alors qu'elle n'a pas de « besoin d'en connaître ».

Cette exigence d'habilitation de sécurité est analogue à l'exigence de posséder une habilitation de sécurité pour l'accès à durée indéterminée d'une personne à une zone sécurisée, sans que cette personne ait accès aux informations classifiées proprement dites.

L'exigence d'habilitation de sécurité s'applique à tous les « porteurs », y compris aux huissiers et aux chauffeurs du ministère public ;

10° La définition des « organes » de la personne morale.

L'article 1bis, 10°, b), de la loi utilise les notions de « organes » et « préposés ». Dans la pratique de l'Autorité nationale de Sécurité, il est devenu nécessaire de définir et distinguer clairement ces deux concepts. Parallèlement, sur avis du Conseil d'État, le terme « personne morale » est également défini au point 12°.

Le terme « organes » désigne les personnes ou les collèges de personnes déterminés par le Code des sociétés et des associations, de manière obligatoire ou facultative, qui accomplissent une tâche spécifique dans la structure des personnes morales et qui, dans la mesure où leur rôle n'est pas purement interne, représentent à titre permanent la personne morale à l'égard de tiers. Tant le comportement effectif de l'organe que les actes juridiques posés par celui-ci sont directement imputés à la personne morale. À l'égard des tiers, l'organe et la personne morale sont considérés comme étant identiques. (VAN DEN BRANDEN, S., MARYSSE, S., Focus op de besloten vennootschap, 77-94 (18 p.)).

Il en ressort que les « dirigeants de fait », y compris les « dirigeants de l'ombre », qui exercent un véritable pouvoir de direction en coulisses, relèvent également du terme « organes ».

Ce terme doit être clairement distingué de celui de « préposé », défini au point 11° ;

11° La définition du terme « préposé ». « Préposer » est compris dans son acception courante, à savoir « charger, employer » (dictionnaire Le Robert) et requiert un lien de subordination, à savoir la capacité réelle d'exercer une autorité et un contrôle sur le comportement d'un tiers sans nécessairement exercer une autorité effective au moment du fait préjudiciable (Cass. 16 octobre 1992, Pas. 1993, 16 ; Cass. 11 décembre 2001, De Verz. 2002, 361, note J. VANHOVEN ; Cass. 22 janvier 2007, Arr. Cass. 2007, 136).

Pour que le lien de subordination existe, une convention ou un contrat est conclu entre le « préposé » et la personne morale (ou entité), que ce « préposé » soit payé ou non.

Par conséquent, un « préposé » est de manière générale un membre du personnel ou une personne exécutant un rôle ou une tâche pour une personne morale (ou une entité) qui ne représente pas la personne morale (ou l'entité) de manière permanente vis-à-vis de tiers. Un préposé peut exercer une fonction purement interne.

Les « bénévoles » qui ne sont pas liés par une convention à l'entité donneuse d'ordre ne peuvent par conséquent pas être considérés comme des « préposés » au sens du présent arrêté. Autrement dit, les « bénévoles » qui sont liés par un contrat ou une convention à une entité dans un contexte professionnel sont donc bien considérés comme des « préposés ». Il doit clairement ressortir du contrat que le « bénévole » a pris connaissance des mesures de sécurité prévues dans la loi et le présent arrêté et qu'il s'engage à accomplir son rôle ou sa tâche en respectant les instructions de et sous la responsabilité de l'entité donneuse d'ordre. Les collaborateurs « détachés » auprès d'une autre autorité publique peuvent bien évidemment être aussi considérés comme des « préposés » ;

12° La définition de « personne morale » a été ajoutée à la demande du Conseil d'État. Étant donné que les points 10° et 11° définissent qui sont les organes et les préposés de la personne morale, il était également nécessaire de définir la personne morale.

De definitie werd toegevoegd om duidelijk te maken dat een drager houder moet zijn van een veiligheidsmachtiging. Deze vereiste is verantwoord daar de verzending vaak door dezelfde persoon zal gebeuren. Bovendien is deze persoon in het bezit van geclassificeerde informatie ook al heeft hij geen "need to know".

De vereiste van veiligheidsmachtiging is analoog aan de vereiste om te beschikken over een veiligheidsmachtiging wanneer het gaat over een toegang voor onbepaalde duur van een persoon tot een beveiligde zone, zonder dat betrokkene toegang heeft tot de geclassificeerde informatie zelf.

De vereiste van veiligheidsmachtiging geldt voor alle "draggers" dus ook voor de bodes en de chauffeurs van het Openbaar Ministerie;

10° De definitie van "organen" van de rechtspersoon.

In artikel 1bis, 10°, b) van de wet worden de begrippen "organen" en "aangestelden" gebruikt. In de praktijk van de Nationale Veiligheids-overheid is de noodzaak gegroeid om deze beide begrippen duidelijk te omschrijven en van elkaar te onderscheiden. Op advies van de Raad van State wordt hiermee samenhangend ook de term "rechtspersoon" gedefinieerd in punt 12°.

Met de term "organen" wordt verwezen naar de volgens het Wetboek van Vennootschappen en Verenigingen op verplichte of facultatieve wijze bepaalde personen of colleges van personen die in de structuur van de rechtspersonen een bepaalde taak vervullen en die, voor zover hun rol niet louter intern is, op bestendige wijze de rechtspersoon ten aanzien van derden vertegenwoordigen. Zowel het feitelijk gedrag van het orgaan als de door het orgaan gestelde rechtshandelingen worden rechtstreeks aan de rechtspersoon toegerekend. Ten aanzien van derden vallen het orgaan en de rechtspersoon samen (VAN DEN BRANDEN, S., MARYSSE, S., Focus op de besloten vennootschap, 77-94 (18 p.)).

Hieruit blijkt dat ook "feitelijke bestuurders" inclusief "schaduwbestuurders", die achter de schermen werkelijke bestuurdersbevoegdheid uitoefenen onder de term "organen" vallen.

Het begrip moet duidelijk onderscheiden worden van "aangestelden" dat omschreven wordt in punt 11°;

11° De definitie van "aangestelden". "Aanstellen" wordt begrepen in zijn dagdagelijkse betekenis, met name "in dienst stellen, nemen" (Van Dale Groot Woordenboek) en vereist een band van ondergeschiktheid, dit is de feitelijke mogelijkheid om op het gedrag van een ander gezag en toezicht uit te oefenen, zonder dat er noodzakelijk effectief gezag wordt uitgeoefend op het moment van het schadeverwekkend feit (Cass. 16 oktober 1992, Pas. 1993, 16; Cass. 11 december 2001, De Verz. 2002, 361, noot J. VANHOVEN; Cass. 22 januari 2007, Arr. Cass. 2007, 136).

Opdat de relatie van ondergeschiktheid zou bestaan, moet er een overeenkomst of contract worden gesloten tussen de "aangestelde" en de rechtspersoon (of entiteit), ongeacht of de "aangestelde" al dan niet wordt betaald.

Een "aangestelde" is bijgevolg in het algemeen een personeelslid of een werknemer van een rechtspersoon (of van een entiteit) die niet op bestendige wijze de rechtspersoon (of de entiteit) ten aanzien van derden vertegenwoordigt. Een aangestelde kan een louter interne functie vervullen.

"Vrijwilligers" die niet zijn verbonden door een overeenkomst aan de entiteit die de opdracht geeft, kunnen bijgevolg in het kader van dit besluit niet beschouwd worden als "aangestelden". Anders gezegd, "vrijwilligers" die bijgevolg wel zijn verbonden door een contract of overeenkomst aan de entiteit in een professionele context kunnen wel beschouwd worden als "aangestelden". Uit het contract moet duidelijk blijken dat de "vrijwilliger" kennis heeft genomen van de beveiligingsmaatregelen bepaald in de wet en voorliggend besluit en zich ertoe verbindt om zijn rol of taak uit te voeren met respect voor de instructies van en onder de verantwoordelijkheid van de entiteit die de opdracht geeft. Medewerkers die "gedetacheerd" worden naar een andere overheidsinstantie kunnen uiteraard ook beschouwd worden als een "aangestelde";

12° De definitie van "rechtspersoon" werd toegevoegd op vraag van de Raad van State. Aangezien in de punten 10° en 11° gedefinieerd wordt wie de organen en aangestelden zijn van de rechtspersoon, diende rechtspersoon ook gedefinieerd te worden.

La notion de « personne morale » renvoie, quant au fond, à toute personne morale, quelle que soit sa forme juridique, pour laquelle une habilitation de sécurité est demandée ou qui est titulaire d'une habilitation de sécurité. Dans le cadre du présent arrêté, la notion de personne morale désigne toute personne morale qui n'est pas une entité de droit public belge. Par conséquent, celles-ci doivent suivre la procédure décrite à l'article 1bis, 10°, b) et 15°, b), de la loi et au chapitre 5, section 2 (habilitation de sécurité pour les personnes morales), du présent arrêté. Cette disposition vise à définir quelles personnes morales doivent demander une habilitation de sécurité pour les personnes morales afin de pouvoir prendre connaissance d'informations classifiées. Par conséquent, les personnes morales qui ne relèvent pas de cette définition (= secteur public) sont dispensées de la demande d'habilitation de sécurité pour les personnes morales afin de pouvoir prendre connaissance d'informations classifiées. En revanche, les personnes physiques d'un organisme public doivent bien évidemment être en possession d'une habilitation de sécurité afin de pouvoir prendre connaissance d'informations classifiées ;

13° La définition de « personne de contact pour la sécurité » est nouvelle. Conformément à l'article 1bis, 15°, a) et b), de la loi, toutes les administrations publiques, les organismes d'intérêt public, les entreprises publiques autonomes et les personnes morales qui utilisent des informations classifiées doivent désigner un officier de sécurité. L'officier de sécurité est chargé de veiller au respect des règles de sécurité. L'officier de sécurité doit être titulaire d'une habilitation de sécurité.

Pour les personnes morales, cela implique une lourde obligation. Ainsi, l'officier de sécurité, qui est un collaborateur de la personne morale, ne pourra être habilité qu'après l'habilitation de la personne morale. Cela a des conséquences financières pour les personnes morales.

La loi du 7 avril 2023 portant modification de la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, attestations de sécurité et avis de sécurité a introduit le niveau de classification « RESTREINT ». Contrairement aux trois autres niveaux de classification, il n'est pas nécessaire d'être titulaire d'une habilitation de sécurité pour accéder à des documents classifiés au niveau « RESTREINT » (un briefing de sécurité est cependant obligatoire).

Les auteurs du projet d'arrêté royal ont dès lors estimé qu'il était excessif d'exiger des personnes morales utilisant exclusivement des informations classifiées de niveau « RESTREINT » que celles-ci désignent un officier de sécurité. Cela impliquerait que la personne morale doive être titulaire d'une habilitation de sécurité, étant donné que l'article 1bis, 15°, b), impose à la personne morale d'être titulaire d'une habilitation de sécurité, ce qui entraverait l'attribution rapide et efficace des contrats.

C'est pourquoi la nouvelle fonction de « personne de contact pour la sécurité » a été créée par analogie avec la fonction de « gestionnaire des avis de sécurité » introduite par l'article 3 de la loi du 2 juin 2024 modifiant la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, attestations de sécurité, avis de sécurité et au service public réglementé et la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

Dans son avis (p. 2), le Comité permanent R indique que la loi attribue à l'officier de sécurité la responsabilité du respect des règles de sécurité relatives aux informations classifiées (article 1^{er}octies de la loi). Étant donné que les informations classifiées au niveau « RESTREINT » relèvent également de la définition des informations classifiées (prévue à l'art. 4 de la loi), le Comité permanent R estime que la responsabilité du respect des règles de sécurité pour le niveau « RESTREINT » ne peut pas être déléguée à la personne de contact pour la sécurité.

L'article 7, § 1^{er}, 1°, de la loi relative à la classification précise que le Roi détermine les mesures de protection applicables à la classification et à la gestion des informations classifiées. La désignation d'une « personne de contact pour la sécurité » en ce qui concerne l'utilisation d'informations classifiées au niveau « RESTREINT » est l'une de ces mesures de protection, ce qui signifie que la mission de vérification du respect des règles de sécurité pour le niveau « RESTREINT » peut effectivement être confiée à la « personne de contact pour la sécurité » susmentionnée.

Inhoudelijk verwijst het begrip “rechtspersoon” naar elke rechtspersoon, ongeacht de rechtsvorm, waarvoor een veiligheidsmachtiging wordt aangevraagd of die houder is van een veiligheidsmachtiging. In het kader van voorliggend besluit wordt met rechtspersoon elke rechtspersoon bedoeld die geen Belgische publiekrechtelijke rechtspersoon is. Deze dienen bijgevolg de procedure zoals beschreven in artikel 1bis, 10°, b) en 15°, b) van de wet en hoofdstuk 5, afdeling 2 (de veiligheidsmachtiging voor rechtspersonen) van voorliggend besluit te volgen. De bepaling beoogt te definiëren welke rechtspersonen een veiligheidsmachtiging voor rechtspersonen moeten aanvragen om kennis te kunnen nemen van geclassificeerde informatie. Bijgevolg worden rechtspersonen die niet onder deze definitie (= publieke sector) vallen, vrijgesteld van het aanvragen van een veiligheidsmachtiging voor rechtspersonen om kennis te kunnen nemen van geclassificeerde informatie. Uiteraard moeten de natuurlijke personen van een publiekrechtelijke instantie wel in het bezit zijn van een veiligheidsmachtiging voor natuurlijke personen opdat zij kennis zouden kunnen nemen van geclassificeerde informatie;

13° De definitie van “contactpersoon voor de veiligheid” is nieuw. Overeenkomstig artikel 1bis, 15°, a) en b) van de wet dienen alle openbare besturen, instellingen van openbaar nut, autonome overheidsbedrijven en rechtspersonen die geclassificeerde informatie aanwenden een veiligheidsofficier aan te duiden. De veiligheidsofficier is bevoegd voor de inachtneming van de veiligheidsregels. De veiligheidsofficier moet over een veiligheidsmachtiging beschikken.

Voor rechtspersonen houdt dit een zware verplichting in. Zo zal de veiligheidsofficier, die een medewerker is van de rechtspersoon, slechts gemachtigd kunnen worden nadat de rechtspersoon gemachtigd is. Dit heeft financiële gevolgen voor rechtspersonen.

De wet van 7 april 2023 houdende wijziging van de wet van 11 december 1998, betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen voerde het classificatieniveau “BEPERKT” in. In tegenstelling tot de andere drie classificatieniveaus dient een persoon geen houder te zijn van een veiligheidsmachtiging om toegang te krijgen tot geclassificeerde stukken van het classificatieniveau “BEPERKT” (maar moet wel een veiligheidsbriefing hebben ontvangen).

De opstellers van het ontwerp koninklijk besluit vonden het dan ook buitensporig om voor rechtspersonen die enkel geclassificeerde informatie bij het niveau “BEPERKT” aanwenden te eisen dat zij een veiligheidsofficier zouden moeten aanstellen. Dit zou impliceren dat de rechtspersoon wel houder zou moeten zijn van een veiligheidsmachtiging, gezien in artikel 1bis, 15°, b) de verplichting wordt opgelegd dat de rechtspersoon houder moet zijn van een veiligheidsmachtiging, hetgeen een vlotte en efficiënte toebedeling van contracten in de weg zou staan.

Om deze reden werd de nieuwe functie van “contactpersoon voor de veiligheid” gecreëerd en dit naar analogie van de functie van “beheerder van de veiligheidsadviezen” ingevoerd door artikel 3 van de wet van 2 juni 2024 houdende wijziging van de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, veiligheidsattesten, veiligheidsadviezen en de publiek gereguleerde dienst en de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens.

Het Vast Comité I stelt in zijn advies (op p. 2) dat de zorg voor de inachtneming van de veiligheidsregels inzake geclassificeerde informatie bij wet toegekend wordt aan de veiligheidsofficier (artikel 1octies van de wet). Aangezien geclassificeerde informatie van het classificatieniveau “BEPERKT” ook valt onder de definitie van geclassificeerde informatie (voorzien in art. 4 van de wet) meent het Vast Comité I dat de zorg voor de inachtneming van de veiligheidsregels voor het niveau “BEPERKT” niet gedelegeerd kan worden aan de contactpersoon voor de veiligheid.

Artikel 7, § 1, 1° van de Classificatiewet preciseert dat de Koning de beschermingsmaatregelen bepaalt van toepassing voor de classificatie en het beheer van geclassificeerde informatie. De aanwijzing van een “contactpersoon voor de veiligheid” voor wat betreft de aanwending van geclassificeerde informatie van het classificatieniveau “BEPERKT” betreft één van deze beschermingsmaatregelen, waardoor de zorg voor de inachtneming van de veiligheidsregels voor het niveau “BEPERKT” wel degelijk kan worden toevertrouwd aan voormelde “contactpersoon voor de veiligheid”.

La définition précise que la personne de contact pour la sécurité doit avoir obtenu un avis de sécurité positif. Dans son avis (p. 2), le Comité permanent R indique que l'exigence d'un avis de sécurité positif ne peut être imposée par arrêté royal car cela ne permettrait pas à la personne morale de droit privé ou de droit public concernée de déroger à l'avis.

Les auteurs du projet d'arrêté royal estiment que la possibilité de déroger à l'avis n'est pas retirée à la personne morale de droit privé ou de droit public. Si l'Autorité nationale de Sécurité, visée à l'article 23 de la loi, émet un avis positif, l'autorité administrative compétente peut encore émettre un avis négatif. Dans ce cas, cette personne ne pourra pas exercer la fonction de personne de contact pour la sécurité ;

14° La définition de la notion d'« entité ». Dans son avis, le Conseil d'État recommande, dans un souci de sécurité juridique, de définir la notion d'« entité » dans le projet. La notion d'« entité » doit être comprise dans son acceptation la plus large. Il peut s'agir de personnes morales de droit privé ou de droit public, d'autorités administratives, etc. Elle concerne toutes les instances qui utilisent des informations classifiées ;

15° La définition de l'« autorité fonctionnelle d'un système de communication et d'information » est nouvelle et a été ajoutée pour indiquer qui est responsable de la mise en œuvre de la politique relative aux systèmes de communication et d'information au sein d'un service donné.

L'autorité fonctionnelle peut être non seulement une personne physique, mais aussi une entité (par exemple un réseau financé par plusieurs nations). Lorsqu'il s'agit d'une entité, celle-ci doit toujours désigner une personne habilitée à signer des documents au nom de l'entité. Tout service travaillant avec un système de communication et d'information destiné à traiter des informations classifiées doit ainsi disposer d'une autorité fonctionnelle, y compris le ministère public.

TITRE II. — Rôles et responsabilités

CHAPITRE 1^{er}. — L'officier de sécurité

Article 2

L'article 2 dispose que les membres du gouvernement fédéral et des gouvernements des entités fédérées désignent un officier de sécurité au sein de leur cellule stratégique et au moins un officier de sécurité au sein de chaque administration publique relevant de leur autorité, dans laquelle des informations classifiées de niveau « CONFIDENTIEL » ou supérieur sont utilisées. Cette disposition figurait déjà dans l'arrêté royal du 24 mars 2000 en ce qui concerne le gouvernement fédéral. Les gouvernements des entités fédérées ont été ajoutés pour aligner la réglementation sur la pratique.

En effet, la loi s'applique à toute personne qui utilise ou souhaite utiliser des informations classifiées. Même lorsque ces informations sont utilisées par des entités fédérées, les mesures de protection (telles que la désignation d'un officier de sécurité), définies par la loi et le présent arrêté d'exécution, doivent être respectées.

Le Conseil d'État a confirmé dans son avis qu'il ne pouvait être déduit de l'article 1bis, 15°, a), de la loi du 11 décembre 1998 que la loi ne s'appliquait qu'aux autorités publiques fédérales. La notion d'« administrations publiques », reprise à l'article 1bis, 15°, a), de la loi du 11 décembre 1998, s'entend au sens large pour inclure les entités fédérées ou les instances chargées d'une mission d'intérêt général, dans la mesure où celles-ci utilisent des informations classifiées.

Cependant, le Conseil d'État a souligné qu'à la lumière du principe de l'exercice autonome des compétences, l'article 1bis, 15°, a), de la loi ne pouvait être lu ou interprété comme habilitant le Roi à utiliser cette disposition comme base juridique pour imposer unilatéralement aux entités fédérées des obligations auxquelles ces dernières n'auraient pas consenti volontairement, étant donné que l'instrument juridique requis pour les y contraindre - l'accord de coopération - fait défaut en l'espèce.

Le Conseil d'État estime dès lors que la disposition proposée dans le projet n'est acceptable que si les entités fédérées choisissent volontairement de coopérer, dans un souci de sécurité, à une classification des documents dans les matières pour lesquelles elles sont compétentes. Il y a alors lieu de penser que, lorsqu'une entité constitutive coopère volontairement à une telle classification afin de bénéficier des avantages que celle-ci induit, elle doit automatiquement se soumettre aux conséquences opérationnelles que cette classification implique, lesquelles sont déterminées par l'autorité compétente en la matière, à savoir l'État fédéral, telles que l'obligation prévue à l'article 2, alinéa 1^{er}, du projet

De la définition steldat de contactpersoon voor de veiligheid een positief veiligheidsadvies moet hebben verkregen. Het Vast Comité I stelt in zijn advies (op p. 2) dat de vereiste van een positief veiligheidsadvies niet kan opgelegd worden bij koninklijk besluit omdat dit aan de betrokken private of publieke rechtspersoon niet de mogelijkheid zou toelaten om af te wijken van het advies.

De opstellers van het ontwerp koninklijk besluit menen dat de mogelijkheid om af te wijken van het advies niet ontnomen wordt aan de private of publieke rechtspersoon. Indien de Nationale Veiligheids-overheid, bedoeld in artikel 23 van de wet, een positief advies zou geven, dan kan de bevoegde administratieve overheid nog steeds een negatief advies geven. Enkel zal deze persoon dan de functie van contactpersoon voor de veiligheid niet kunnen uitoefenen;

14° De definitie van "entiteit". De Raad van State adviseert in haar advies, om ter wille van de rechtszekerheid, het begrip "entiteit" te definiëren in het ontwerp. "Entiteit" moet in de meest ruime zin worden opgevat. Dit kunnen zowel publiekrechtelijke als privaatrechtelijke rechtspersonen zijn, administratieve overheden, Het gaat om alle instanties die geclassificeerde informatie aanwenden;

15° De definitie van "functionele autoriteit van een communicatie- en informatiesysteem" is nieuw en werd toegevoegd om aan te duiden wie verantwoordelijk is voor de implementatie van het beleid betreffende de communicatie- en informatiesystemen binnen een bepaalde dienst.

De functionele autoriteit kan een natuurlijk persoon zijn, maar ook een entiteit (bijvoorbeeld een netwerk gefinancierd door meerdere naties). In het geval het gaat om een entiteit, dan moet er altijd iemand worden aangeduid door deze entiteit die gemachtigd is om documenten te ondertekenen in naam van de entiteit. Elke dienst die werkt met een communicatie- en informatiesysteem dat bedoeld is om geclassificeerde informatie te verwerken dient aldus te beschikken over een functionele autoriteit, dus ook het Openbaar Ministerie.

TITEL II. — Rollen en verantwoordelijkheden

HOOFDSTUK 1. — De veiligheidsofficier

Artikel 2

Artikel 2 bepaalt dat de leden van de federale regering en van de deelstatenregeringen een veiligheidsofficier aanduiden binnen hun beleidscel en ten minste één veiligheidsofficier binnen elk openbaar bestuur dat onder hun gezag ressorteert, waarbinnen geclassificeerde informatie met het beschermingsniveau "VERTROUWELIJK" of hoger wordt aangewend. Deze bepaling stond reeds in het koninklijk besluit van 24 maart 2000 voor wat betreft de federale regering. De deelstatenregeringen werden toegevoegd om de regelgeving in overeenstemming met de praktijk te brengen.

De wet is immers van toepassing op éénieder die geclassificeerde informatie aanwendt of wenst aan te wenden. Ook als deze informatie wordt aangewend door de gefedereerde entiteiten, moeten de beschermingsmaatregelen (zoals de aanstelling van een veiligheidsofficier), zoals die door de wet en voorliggend uitvoeringsbesluit worden bepaald, in acht worden genomen.

De Raad van State bevestigde in haar advies dat uit artikel 1bis, 15°, a), van de wet van 11 december 1998 niet kan worden afgeleid dat die wet enkel van toepassing zou zijn op de federale overheidsinstanties. Het begrip "openbare besturen" in artikel 1bis, 15°, a), van de wet van 11 december 1998 wordt ruim opgevat, zodat ook gefedereerde entiteiten of instanties die een taak van algemeen belang uitvoeren, hieronder kunnen vallen, voor zover deze geclassificeerde informatie aanwenden.

De Raad van State benadrukte echter dat in het licht van het beginsel van de autonome bevoegdheidsuitoefening artikel 1bis, 15°, a) van de wet niet kan gelezen of geïnterpreteerd worden als zou daarbij de Koning gemachtigd worden om aan die bepaling rechtsgrond te ontfemen om aan de deeltentiteiten op eenzijdige wijze verplichtingen op te leggen waarmee laatstgenoemden niet vrijwillig ingestemd zouden hebben, aangezien in casu het vereiste juridische instrument om hen daartoe te verplichten - het samenwerkingsakkoord - ontbreekt.

De Raad van State stelt dus dat de voorgestelde bepaling van het ontwerp enkel aanvaardbaar is indien de deeltentiteiten er uit eigen beweging voor kiezen om ter wille van de veiligheid mee te werken aan een classificatie van documenten in de aangelegenheden waarvoor zij bevoegd zijn. Er is dan immers reden om aan te nemen dat, wanneer een deeltentiteit vrijwillig aan een dergelijke classificatie meewerkt om de voordelen die dat met zich meebrengt te genieten, zij zich automatisch moet schikken naar de operationele gevolgen die deze classificatie met zich meebrengt, die worden vastgesteld door de overheid die ter zake bevoegd is, namelijk de federale Staat, zoals de

de nommer un officier de sécurité auprès des organes et services concernés. La désignation de l'officier de sécurité relève de la responsabilité des entités fédérées et non de l'autorité fédérale.

L'article 2, alinéa 1^{er}, du projet est donc légèrement modifié en conséquence.

Article 3

L'article 3 du projet dispose que la fonction d'officier de sécurité ne peut être exercée que par des personnes qui possèdent la nationalité belge.

Les « informations classifiées » sont des informations qui, dans l'intérêt de la sécurité nationale, sont protégées par des mesures de sécurité contre tout accès non autorisé, toute utilisation inappropriée et toute diffusion. En d'autres termes, des intérêts fondamentaux de l'État belge sont en jeu et doivent être protégés, quelle que soit leur forme et leur localisation. Dans le cadre de la gestion des risques, et notamment de l'identification des menaces contre les intérêts fondamentaux de l'État belge, il est logique d'imposer des mesures de sécurité permettant de résister à ces menaces ou de les réduire à un risque acceptable.

L'imposition de la nationalité belge à certaines personnes clés, dont l'officier de sécurité, fait partie de ces mesures de sécurité.

En effet, l'officier de sécurité veille au respect des règles de sécurité belges en matière de protection des informations classifiées (article 1^{er} octies de la loi). L'officier de sécurité doit s'assurer que l'entreprise et son personnel respectent les mesures de protection des informations classifiées. L'officier de sécurité doit également être titulaire d'une habilitation de sécurité pour les personnes physiques démontrant des garanties suffisantes en termes de discrétion, de loyauté et d'intégrité. En raison de cette fonction indépendante de contrôle du respect des règles de sécurité relatives aux informations classifiées qui, comme mentionné précédemment, protègent les intérêts fondamentaux de l'État belge, il importe également que l'officier de sécurité (et la personne de contact pour la sécurité) possède la nationalité belge.

D'autres pays suivent la même logique (Royaume-Uni, Canada et Pays-Bas).

Au sein d'un groupe d'entreprises dont au moins une entreprise a accès à des informations classifiées, ou au sein d'une société holding dont une des filiales a accès à des informations classifiées, un officier de sécurité (ou une personne de contact pour la sécurité) peut être désigné pour veiller à la cohérence entre l'administration du groupe ou du holding et les défis que la protection de ces informations classifiées implique. L'Autorité nationale de Sécurité procède à une évaluation de l'officier de sécurité proposé par le groupe de sociétés ou la société holding afin de déterminer si cette personne sera en mesure d'exercer efficacement sa fonction.

Pour les informations classifiées de l'UE, de l'OTAN ou d'institutions inter- ou supranationales, il suffit que l'officier de sécurité ou la personne de contact pour la sécurité soit un ressortissant d'un État membre de l'une de ces organisations, étant donné qu'il s'agit ici - logiquement - de protéger la « sécurité nationale » de l'UE ou de l'OTAN. Exiger que l'officier de sécurité ou la personne de contact pour la sécurité possède également la nationalité belge serait disproportionné.

Article 4

L'article 4 dispose que l'Autorité nationale de Sécurité fixe les modalités du contrôle de l'exécution des missions de l'officier de sécurité. Étant donné que l'Autorité nationale de Sécurité doit contrôler l'exécution des missions de l'officier de sécurité, elle est également la mieux placée pour élaborer avec expertise ces règles complexes à portée technique.

verplichting waarin artikel 2, eerste lid, van het ontwerp voorziet om een veiligheidsofficier aan te stellen bij de betrokken organen en diensten. Het aanwijzen van de veiligheidsofficier behoort tot de bevoegdheid van de gefedereerde entiteiten en niet van de federale overheid.

Artikel 2, eerste lid van het ontwerp wordt in die zin dan ook licht aangepast.

Artikel 3

Artikel 3 van het ontwerp bepaalt dat de functie van veiligheidsofficier enkel kan worden uitgeoefend door personen die over de Belgische nationaliteit beschikken.

“Geclassificeerde informatie” is informatie die, in het belang van de nationale veiligheid, wordt beschermd door veiligheidsmaatregelen tegen elke niet-geautoriseerde toegang, niet-geëigende aanwending en verspreiding ervan. Er staan met andere woorden fundamentele Belgische staatsbelangen op het spel, die beschermd moeten worden, ongeacht de vorm die deze aannemen en waar deze zich ook bevinden. In het kader van risicomanagement, met name het identificeren van dreigingen tegen de fundamentele Belgische staatsbelangen, is het logisch om beveiligingsmaatregelen op te leggen die kunnen weerstaan aan deze dreigingen of deze tot een aanvaardbaar risico kunnen reduceren.

Het opleggen van de Belgische nationaliteit voor bepaalde sleutelfiguren, waaronder de veiligheidsofficier, behoort tot deze beveiligingsmaatregelen.

De veiligheidsofficier zorgt immers voor de inachtneming van de Belgische veiligheidsregels inzake de bescherming van geclassificeerde informatie (artikel 1^{octies} van de wet). De veiligheidsofficier moet toezien op de naleving van de beschermingsmaatregelen voor geclassificeerde informatie door de onderneming en het personeel dat er werkzaam is. De veiligheidsofficier moet tevens in bezit zijn van een veiligheidsmachtiging voor natuurlijke personen, waaruit blijkt dat hij of zij voldoende garanties biedt inzake geheimhouding, loyaleiteit en integriteit. Omwille van deze onafhankelijke, toezichthoudende functie op de naleving van de veiligheidsvoorschriften inzake geclassificeerde informatie, die, zoals hiervoor reeds aangehaald, fundamentele Belgische staatsbelangen beschermen, is het eveneens vereist dat de veiligheidsofficier (en de contactpersoon voor de veiligheid) over de Belgische nationaliteit beschikt.

Dezelfde logica wordt gevolgd door andere landen (UK, Canada en Nederland).

Binnen een groep ondernemingen waarvan ten minste één onderneming toegang heeft tot geclassificeerde informatie, of binnen een holdingmaatschappij waarvan één van de dochterondernemingen toegang heeft tot geclassificeerde informatie, kan een veiligheidsofficier (of een contactpersoon voor de veiligheid) worden benoemd om te zorgen voor samenhang tussen het bestuur van de groep of de holding en de uitdagingen die de bescherming van deze geclassificeerde informatie met zich meebrengt. De Nationale Veiligheidsoverheid voert een evaluatie uit van de veiligheidsofficier die door de groep ondernemingen of de holding wordt voorgesteld om na te gaan of deze persoon effectief in staat zal zijn om zijn functie uit te oefenen.

Voor de geclassificeerde informatie van de EU, NAVO of inter- of supranationale instellingen volstaat het voor de veiligheidsofficier of de contactpersoon voor de veiligheid om een onderdaan te zijn van een lidstaat van één van deze organisaties, gezien het hier -logischerwijze- gaat om de bescherming van de “nationale veiligheid” van de EU of de NAVO. Het zou onevenredig zijn om hier te vereisen dat de veiligheidsofficier of de contactpersoon voor de veiligheid hier eveneens over de Belgische nationaliteit zou moeten beschikken.

Artikel 4

Artikel 4 bepaalt dat de Nationale Veiligheidsoverheid regels vastlegt met betrekking tot het toezicht op de uitvoering van de opdrachten van de veiligheidsofficier. Gezien de Nationale Veiligheidsoverheid toezicht moet uitoefenen op het uitvoeren van de opdrachten van de veiligheidsofficier, is deze ook het best geplaatst om deze complexe regels met een technische draagwijdte met kennis van zaken uit te werken.

CHAPITRE 2. — *La personne de contact pour la sécurité*

Article 5

L'article 5 décrit les responsabilités de la personne de contact pour la sécurité.

Article 6

L'article 6 définit certaines missions de la personne de contact pour la sécurité relatives à la prise de connaissance des mesures de protection concernant les informations classifiées au niveau « RESTREINT ». Sur avis du Conseil d'État, le point 1° est supprimé car il est redondant. En effet, la définition de la « personne de contact pour la sécurité » figure déjà à l'article 1^{er}, 13°, qui énonce les définitions.

Article 7

A cet égard, il est renvoyé à l'explication de la définition de « personne de contact pour la sécurité ». Si un officier de sécurité a déjà été désigné au sein d'une entité, il n'est évidemment plus nécessaire de désigner une personne de contact pour la sécurité, étant donné que, conformément à l'article 1^{er} octies, § 1^{er}, 1°, de la loi relative à la classification, l'officier de sécurité veille également au respect des règles de sécurité relatives à la protection des informations classifiées, qui incluent dès lors également les informations classifiées au niveau « RESTREINT ».

Article 8

L'article 8 dispose que l'Autorité nationale de Sécurité fixe les modalités du contrôle de l'exécution des missions de la personne de contact pour la sécurité. Étant donné que l'Autorité nationale de Sécurité doit contrôler l'exécution des missions de l'officier de sécurité, elle est également la mieux placée pour élaborer ces règles à portée technique en connaissance de cause. Les missions de la personne de contact pour la sécurité sont analogues à celles de l'officier de sécurité.

CHAPITRE 3. — *L'autorité fonctionnelle d'un système de communication et d'information*

Article 9

L'article 9 définit les missions de l'autorité fonctionnelle d'un système de communication et d'information et n'appelle pas de commentaire supplémentaire.

TITRE III. — *Informations classifiées*CHAPITRE 1^{er}. — *Mesures de protection applicables à la classification et à la gestion d'informations classifiées*Section 1^{re}. — *Disposition générale*

Article 10

Cet article veille à préserver la compétence pour chaque ministre de prescrire des règles complémentaires d'ordre technique en matière de classification, de déclassification et de mesures de protection inhérentes à la classification.

Les règles prévues par le présent arrêté constituent la norme minimale à laquelle les personnes (morales) doivent satisfaire afin de pouvoir traiter des informations classifiées. Toutefois, ces règles ne mettent en lumière qu'une seule dimension de la sécurité militaire. La sécurité opérationnelle en constitue par exemple un autre aspect. La sécurité opérationnelle peut être définie comme suit : "All measures taken to give a military operation or exercise appropriate security, using passive or active means, to deny an adversary knowledge of the essential elements of friendly information or indicators thereof" (NATO Glossary of Terms and definitions, AAP-06).

En vertu de l'article 11, § 1^{er}, 2°, de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, le SGRS a pour mission de « veiller au maintien de la sécurité militaire du personnel relevant du ministre de la Défense nationale, et des installations militaires, armes, munitions, équipements, plans, écrits, documents, systèmes informatiques et de communications ou autres objets militaires ».

Le maintien de la sécurité militaire, par exemple au cours d'une opération à l'étranger, requiert des mesures de sécurité strictes. Chaque opération nécessite des règles différentes et la situation sécuritaire diffère par ailleurs dans chaque pays.

De plus, les règles doivent pouvoir être adaptées en fonction de la menace et des besoins opérationnels. Il est dès lors essentiel que le chef du SGRS puisse, le cas échéant, imposer des règles plus strictes en matière de protection des informations classifiées afin de garantir la sécurité militaire.

HOOFDSTUK 2. — *De contactpersoon voor de veiligheid*

Artikel 5

Artikel 5 omschrijft de verantwoordelijkheden van de contactpersoon voor de veiligheid.

Artikel 6

Artikel 6 omschrijft bepaalde opdrachten van de contactpersoon voor de veiligheid betreffende de kennisname van de beschermingsmaatregelen inzake geclassificeerde informatie met het classificatieniveau "BEPERKT". Op advies van de Raad van State wordt punt 1° geschrapt, omdat dit overbodig is. De definitie van "contactpersoon voor de veiligheid" wordt immers al gegeven in artikel 1, 13° dat de definities bepaalt.

Artikel 7

Hiervoor kan verwezen worden naar de toelichting bij de definitie van "contactpersoon voor de veiligheid". Indien er reeds een veiligheidsofficier is aangewezen in de schoot van een entiteit, moet er uiteraard geen contactpersoon voor de veiligheid meer worden aangesteld, gezien volgens artikel 1octies, § 1, 1° van de Classificatiewet de veiligheidsofficier tevens zorgt voor de inachtneming van de veiligheidsregels inzake de bescherming van geclassificeerde informatie, waaronder dus ook geclassificeerde informatie met het beschermingsniveau "BEPERKT".

Artikel 8

Artikel 8 bepaalt dat de Nationale Veiligheidsoverheid regels vastlegt met betrekking tot het toezicht op de uitvoering van de opdrachten van de contactpersoon voor de veiligheid. Gezien de Nationale Veiligheidsoverheid toezicht moet uitoefenen op het uitvoeren van de opdrachten van de veiligheidsofficier, is deze ook het best geplaatst om deze regels met een technische draagwijdte met kennis van zaken uit te werken. De opdrachten van de contactpersoon voor de veiligheid zijn analoog aan deze van de veiligheidsofficier.

HOOFDSTUK 3. — *De functionele autoriteit van een communicatie- en informatiesysteem*

Artikel 9

Artikel 9 omschrijft de opdrachten van de functionele autoriteit van een communicatie- en informatiesysteem en behoeven geen verder commentaar.

TITEL III. — *Geclassificeerde informatie*HOOFDSTUK 1. — *De beschermingsmaatregelen van toepassing voor de classificatie en het beheer van geclassificeerde informatie*Afdeling 1. — *Algemene bepaling*

Artikel 10

Dit artikel strekt tot het behoud van de mogelijkheid van elke minister om bijkomende regels van technische aard voor te schrijven op het vlak van classificatie, declassificatie en beschermingsmaatregelen verbonden aan classificatie.

De regels voorzien in voorliggend besluit vormen de minimumstandaard waaraan (rechts)personen dienen te voldoen willen zij geclassificeerde informatie verwerken. Deze regels belichten echter slechts één dimensie van de militaire veiligheid. Een ander aspect is bijvoorbeeld de operationele veiligheid. Operationele veiligheid wordt omschreven als "All measures taken to give a military operation or exercise appropriate security, using passive or active means, to deny an adversary knowledge of the essential elements of friendly information or indicators thereof" (NATO Glossary of Terms and definitions, AAP-06).

De ADIV is op grond van artikel 11, § 1, 2° van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten bevoegd voor "het behoud van de militaire veiligheid van het personeel dat onder de Minister van Landsverdediging ressorteert, de militaire installaties, wapens en wapensystemen, munitie, uitrusting, plannen, geschriften, documenten, informatica- en verbindingssystemen of andere militaire voorwerpen".

Het behoud van de militaire veiligheid, bijvoorbeeld tijdens een buitenlandse operatie, vereist strenge beveiligingsmaatregelen. Elke operatie vereist andere regels en de veiligheidssituatie in elk land is ook verschillend.

Verder moeten de regels aangepast kunnen worden in functie van de dreiging en de operationele noodwendigheden. Het is dan ook essentieel dat de Chef van de ADIV, striktere regels inzake de bescherming van geclassificeerde informatie kan opleggen indien nodig om de militaire veiligheid te garanderen.

C'est pourquoi, il est également prévu que, outre le ministre, le chef du SGRS puisse prescrire des règles supplémentaires (plus strictes) de nature technique en ce qui concerne la Défense. Cela n'exclut cependant pas la possibilité pour les fonctionnaires dirigeants d'établir des directives supplémentaires (plus strictes) pour les services qui leur sont subordonnés. Dans ce cas, ces directives n'ont pas de caractère réglementaire, mais elles sont contraignantes pour les services subordonnés.

Section 2. — Personnes et autorités compétentes pour la classification, la modification du niveau de classification et la déclassification

Article 11

L'article 11 définit le champ d'application *ratione personae* en matière de classification, de déclassification et de modification du niveau de classification des informations classifiées. Ces personnes doivent être titulaires d'une habilitation de sécurité de niveau « SECRET » au minimum, même s'il s'agit de classer des informations de niveau « RESTREINT ».

Il permet dès lors de déterminer précisément les personnes compétentes pour classer, modifier le niveau de classification, et déclasser les informations classifiées, ce qui permet ainsi un meilleur contrôle sur le flux de ces informations et une meilleure sécurité vis-à-vis de leur contenu et de leur pertinence.

On peut également se référer à l'explication de la modification de l'article 1bis de la loi (DOC 55 n°2443/003, p. 7) : « [...] car les décisions de déclassification et de modification des niveaux de classification appartiennent exclusivement à un gouvernement public. [...] »

Il est donc clair que les personnes morales privées – avec lesquelles une autorité administrative passe des contrats – ne peuvent être considérées comme une « autorité d'origine », même si elles produisent des pièces classifiées au profit et sous l'autorité d'une autorité administrative.

Le Collège des procureurs généraux a soulevé que le procureur fédéral et les magistrats qu'il désigne devraient également avoir l'autorisation de classer et de déclasser des informations aux niveaux « SECRET », « CONFIDENTIEL » et « RESTREINT », en plus du niveau « TRÈS SECRET ». Ils ont donc été inclus dans cet article.

Article 12

L'article 12 définit le champ d'application *ratione personae* de la compétence de classification, de déclassification et de modification du niveau de classification des informations de niveau « TRÈS SECRET ».

Il précise ainsi les personnes autorisées à classer, modifier ou déclasser des informations classifiées « TRÈS SECRET », ce qui permet un meilleur contrôle sur l'utilisation de ces données et renforce la sécurité quant à leur contenu.

Le procureur fédéral ainsi que les magistrats qu'il désigne sont les personnes qui doivent avoir une habilitation pour effectuer ces actions.

Dans son avis 61.551/2 du 14 juin 2017, le Conseil d'État remet en question la nécessité d'exiger, par le biais de cet article 12, que ces magistrats doivent s'être vu délivrer une habilitation de sécurité au préalable pour user de la compétence de classification, de déclassification et de modification des informations classifiées du niveau « TRÈS SECRET » car l'article 8 de la loi du 11 décembre 1998 n'exige pas que ces mêmes magistrats possèdent une habilitation pour la consultation de pièces classifiées.

Selon le Conseil d'État, cela soulève une incohérence, car il semble contradictoire d'exiger une habilitation pour que ces magistrats puissent remplir leurs fonctions alors que cela n'est pas exigé dans le cadre de l'article 8 de la loi du 11 décembre 1998.

Néanmoins, il est fondamental que le procureur fédéral et les magistrats délégués possèdent une habilitation de sécurité appropriée pour classer, modifier ou déclasser des informations, surtout celles classifiées « TRÈS SECRET ». Cette exigence est essentielle pour garantir la sécurité et la confidentialité des données sensibles, car elle assure que seules des personnes formées et vérifiées puissent activement créer, modifier ou supprimer les niveaux d'habilitation d'informations critiques, contrairement à l'article 8 de la loi du 11 décembre 1998, qui ne concerne qu'un accès passif à ces informations, une simple consultation.

Daarom wordt naast de minister ook voorzien dat de chef van de ADIV bijkomende (strikttere) regels van technische aard kan voorschrijven voor wat betreft Defensie. Dit sluit echter niet uit dat ook leidende ambtenaren, bijkomende (strikttere) richtlijnen kunnen uitvaardigen voor wat betreft de diensten die onder hen ressorteren. Deze hebben dan geen reglementair karakter, maar zijn wel bindend voor de diensten die onder hen ressorteren.

Afdeling 2. — Bevoegde personen en overheden voor het classificeren, de wijziging van het classificatieniveau en het declassificeren

Artikel 11

In artikel 11 wordt het toepassingsgebied *ratione personae* vastgesteld op het gebied van classificatie, declassificatie en wijziging van het classificatieniveau van geclassificeerde informatie. Deze personen moeten houder zijn van een veiligheidsmachtiging van ten minste het niveau « GEHEIM », ook al gaat het om het classificeren van informatie van het niveau « BEPERKT ».

Daardoor kan er op precieze wijze worden bepaald welke personen bevoegd zijn voor het classificeren, het wijzigen van het classificatieniveau of het declassificeren van geclassificeerde informatie, zodat er meer controle is op de verspreiding van deze informatie en meer veiligheid ten aanzien van de inhoud en relevantie ervan.

Er kan ook gewezen worden op de toelichting bij het amendement van artikel 1bis van de wet (DOC 55 2443/003, p. 7): « [...] want beslissingen over declassificatie en beslissingen tot wijzigingen van classificatieniveaus komen uitsluitend toe aan de publieke overheid. [...] »

Het is dus duidelijk dat private rechtspersonen -waarmee een administratieve overheid contracten afsluit- niet kunnen worden beschouwd als een « overheid van oorsprong », ook al stellen ze geclassificeerde stukken op ten behoeve van en onder het gezag van een administratieve overheid.

Het college van procureurs-generaal merkte op dat de federale procureur en de magistraten die hij machtigt ook de toestemming zouden moeten hebben om informatie te classificeren en declassificeren op de niveaus « GEHEIM », « VERTROUWELIJK » en « BEPERKT », naast het niveau « ZEER GEHEIM ». Daarom worden ze in dit artikel opgenomen.

Artikel 12

In artikel 12 wordt het toepassingsgebied *ratione personae* bepaald van de bevoegdheid voor het classificeren, declassificeren of het wijzigen van het classificatieniveau van informatie van het niveau « ZEER GEHEIM ».

Op die manier wordt vastgesteld welke personen gemachtigd zijn om informatie van het niveau « ZEER GEHEIM » te classificeren, te wijzigen of te declassificeren, hetgeen zorgt voor een betere controle op het gebruik van deze gegevens en een verhoogde bescherming van de inhoud ervan.

De personen die een machtiging moeten hebben om deze acties uit te voeren zijn de federale procureur en de magistraten die hij aanduidt.

In zijn advies 61.551/2 van 14 juni 2017 stelt de Raad van State in vraag of het noodzakelijk is om, door middel van dit artikel 12, te eisen dat deze magistraten voorafgaand een veiligheidsmachtiging moeten hebben verkregen om de bevoegdheid uit te oefenen van het classificeren, declassificeren of wijzigen van geclassificeerde informatie van het niveau « ZEER GEHEIM », omdat het voor diezelfde magistraten volgens artikel 8 van de wet van 11 december 1998 niet vereist is om over een machtiging te beschikken om geclassificeerde stukken te raadplegen.

Volgens de Raad van State vormt dit een incoherentie, aangezien het tegenstrijdig lijkt om te eisen dat deze magistraten een machtiging hebben om hun functie kunnen uitoefenen, terwijl dit niet vereist is in het kader van artikel 8 van de wet van 11 december 1998.

Toch is het essentieel dat de federale procureur en de gedelegeerde magistraten over een adequate veiligheidsmachtiging beschikken om informatie te classificeren, te declassificeren of het niveau te wijzigen, vooral voor informatie van het classificatieniveau « ZEER GEHEIM ». Deze vereiste is essentieel om de veiligheid en vertrouwelijkheid van gevoelige gegevens te waarborgen, omdat er zo voor wordt gezorgd dat enkel opgeleide en geverifieerde personen actief de machtingsniveaus voor kritieke informatie kunnen aanmaken, wijzigen of schrappen; artikel 8 van de wet van 11 december 1998 heeft daarentegen enkel betrekking op een passieve toegang tot deze informatie, een eenvoudige raadpleging.

Le Conseil d'État souligne que l'article 8 mentionne que les magistrats n'ont pas besoin d'une habilitation pour consulter des documents classifiés. Cependant, il est important de noter que cette disposition concerne uniquement l'accès à des documents déjà classifiés, et ne concerne aucunement le fait de conférer le pouvoir de classifier, modifier ou déclassifier. Ces deux processus sont fondamentalement distincts : l'un permet simplement la consultation, tandis que l'autre implique une responsabilité active dans la gestion de la sécurité des informations.

Il semble donc difficile de pouvoir transposer la même logique que celle développée pour l'article 8 afin d'établir que le procureur fédéral et les magistrats désignés puissent classifier, modifier ou déclassifier des informations classifiées « TRÈS SECRET » sans une habilitation adéquate.

Par exemple, en ce qui concerne l'article 3 de la loi du 11 décembre 1998, qui traite des témoins protégés, il est crucial que ces magistrats aient la capacité de classifier de nouvelles pièces. Une telle responsabilité requiert une connaissance approfondie des enjeux de sécurité et des procédures de classification, accessible uniquement par le biais d'une habilitation de sécurité adéquate.

Il est donc fondamental de distinguer le rôle passif de consultation des documents classifiés, comme le prévoit l'article 8, d'un rôle actif de classification et de déclassification. Pour garantir la sécurité et l'intégrité des informations, le procureur fédéral et les magistrats doivent être en mesure de prendre des décisions éclairées, ce qui ne peut être assuré qu'en possédant les habilitations nécessaires pour agir de manière responsable sur les informations classifiées « TRÈS SECRET ».

Section 3. — Gestion des informations classifiées

Article 13

Cet article permet à l'Autorité nationale de Sécurité de pouvoir compléter de manière rapide les dispositions du présent arrêté par des mesures administratives et techniques supplémentaires qui permettraient une meilleure gestion des informations classifiées.

Sous-section 1. — Marquages

Article 14

La gestion des informations sensibles est cruciale et nécessite une attention particulière pour éviter toute confusion. Les autorités doivent classifier, modifier ou déclassifier ces informations de manière appropriée, en veillant à ce qu'elles soient clairement identifiées selon leur niveau de confidentialité. La classification n'est pas statique et peut évoluer ; il est donc essentiel de mettre à jour le niveau de classification lorsque cela s'avère nécessaire. Il est également important de déclassifier. Ainsi, les mesures de sécurité rigoureuses qui s'appliquaient à des informations devenues moins sensibles peuvent être levées. Les marquages doivent être clairs et visibles pour garantir une bonne identification. En définitive, une gestion responsable des informations sensibles est essentielle pour les protéger et éviter toute confusion. Les personnes compétentes doivent être conscientes de leur rôle et agir avec prudence.

Articles 15 à 19

Ces articles ne nécessitent pas d'explication particulière, si ce n'est que la traduction en allemand et en anglais des niveaux de classification n'a pas été prévue, étant donné que ces niveaux de classification en allemand et en anglais sont inexistant dans la loi et que, par conséquent, ces documents ne seront pas non plus protégés si le marquage est effectué en allemand ou en anglais. Toutefois, conformément à l'article 16, alinéa 4, du projet d'arrêté royal il est possible de compléter le marquage en néerlandais ou en français par l'équivalent international en langue anglaise repris dans le tableau comparatif de l'annexe 1. Les compatriotes germanophones peuvent toujours opter pour un marquage supplémentaire en allemand, conformément à l'article 18, qui indique clairement le niveau de classification aux destinataires germanophones d'un document classifié, même s'ils préparent déjà des documents classifiés avec une indication du niveau de classification en français ou en néerlandais.

De Raad van State benadrukt dat in artikel 8 vermeld wordt dat magistraten geen machtiging nodig hebben om geclassificeerde documenten te raadplegen. Het is echter belangrijk om op te merken dat deze bepaling enkel betrekking heeft op toegang tot documenten die al geclassificeerd zijn en geenszins op de toekenning van de bevoegdheid om te classificeren, wijzigen of declassificeren. Deze twee procedures zijn fundamenteel verschillend: de ene staat louter de raadpleging toe, terwijl de andere een actieve verantwoordelijkheid in het beheer van de veiligheid van de informatie inhoudt.

Het lijkt dus moeilijk om dezelfde logica te hanteren dan die die gevolgd werd voor artikel 8 om te bepalen dat de federale procureur en de aangeduide magistraten informatie met classificatieniveau "ZEER GEHEIM" zouden kunnen classificeren, wijzigen of declassificeren zonder een adequate veiligheidsmachtiging.

Bijvoorbeeld met betrekking tot artikel 3 van de wet van 11 december 1998, dat betrekking heeft op beschermde getuigen, is het cruciaal dat deze magistraten de mogelijkheid hebben om nieuwe stukken te classificeren. Een dergelijke verantwoordelijkheid vereist een diepgaande kennis van de veiligheidsuitdagingen en de classificatieprocedures, waartoe enkel toegang kan worden verkregen middels een adequate veiligheidsmachtiging.

Het is dus fundamenteel om een onderscheid te maken tussen de passieve rol van het raadplegen van geclassificeerde documenten, zoals voorzien in artikel 8, en de actieve rol van het classificeren en declassificeren. Om de veiligheid en de integriteit van informatie te verzekeren, moeten de federale procureur en de magistraten in staat zijn om weloverwogen beslissingen te kunnen nemen, hetgeen enkel kan worden gegarandeerd indien zij over de nodige machtigingen beschikken om op een verantwoordelijke manier te handelen op basis van informatie met classificatieniveau "ZEER GEHEIM".

Afdeling 3. — Beheer van geclassificeerde informatie

Artikel 13

Dit artikel stelt de Nationale Veiligheidsoverheid in staat om de bepalingen in het besluit in kwestie snel aan te vullen met bijkomende administratieve en technische maatregelen die een beter beheer van geclassificeerde informatie mogelijk maken.

Onderafdeling 1. — Markeringen

Artikel 14

Het beheer van gevoelige informatie is cruciaal en vereist bijzondere aandacht om verwarring te vermijden. De overheden moeten deze informatie classificeren, wijzigen of declassificeren op een adequate manier, door ervoor te zorgen dat de informatie duidelijk wordt geïdentificeerd volgens het vertrouwelijkheidsniveau ervan. De classificatie is niet statisch en kan evolueren; het is dus essentieel om het classificatieniveau wanneer nodig bij te werken. Het is ook belangrijk om te declassificeren. Op die manier kunnen de rigoureuze veiligheidsmaatregelen die van toepassing waren op informatie die ondertussen niet meer zo gevoelig is, worden opgeheven. De markeringen moeten duidelijk en zichtbaar zijn om een goede identificatie te verzekeren. Kortom, een verantwoordelijk beheer van gevoelige informatie is essentieel om deze informatie te beschermen en verwarring te vermijden. Bevoegde personen moeten zich bewust zijn van hun rol en zorgvuldig handelen.

Artikel 15 tot 19

Deze artikelen behoeven geen bijzondere toelichting, buiten het feit dat de vertaling naar het Duits en het Engels van de classificatieniveaus niet werd opgenomen, gezien deze classificatieniveaus in het Duits en het Engels onbestaande zijn in de wet en deze documenten bijgevolg evenmin beschermd zullen worden indien de markering in het Duits of het Engels wordt aangebracht. Wel is het mogelijk om overeenkomstig het artikel 16, vierde lid van het ontwerpbesluit de markering in het Nederlands of in het Frans aan te vullen met het internationaal equivalent in de Engelse taal dat wordt vermeld in de vergelijkende tabel van bijlage 1. Duitstalige landgenoten kunnen er steeds voor opteren om een aanvullende markering overeenkomstig het ontworpen artikel 18 te hanteren in het Duits die het classificatieniveau duidelijk maakt voor de Duitstalige bestemmingen van een geclassificeerd document, niettegenstaande ze nu al geclassificeerde documenten opstellen met een vermelding van het classificatieniveau in het Frans of in het Nederlands.

Sous-section 2. — Déclassification du niveau de classification
« RESTREINT »

Article 20

Cet article n'appelle aucun commentaire.

Sous-section 3. — Classification ou déclassification collective

Article 21

Cet article traite de la possibilité de classification ou de déclassification collectives des documents par l'autorité d'origine. Cela signifie qu'une autorité peut décider d'attribuer un niveau de classification ou de le retirer pour un ensemble de documents, fichiers ou dossiers qui sont identifiables par un sujet commun, sans avoir à examiner chaque document individuellement.

Cette approche vise à simplifier le processus de gestion des informations classifiées, en permettant une action globale plutôt que détaillée.

Cette règle figure déjà dans l'actuel arrêté royal du 24 mars 2000 portant exécution de la loi du 11 décembre relative à la classification, aux habilitations de sécurité, attestations de sécurité et avis de sécurité (article 32) et est parfois appliquée à des fonds d'archives anciens (antérieurs à l'entrée en vigueur de la loi du 11 décembre 1998), pour lesquels il n'est pas opportun de marquer individuellement le document proprement dit en raison de leur vulnérabilité/fragilité, de leur valeur historique, de leur taille ou pour des raisons techniques (documents anciens sur microfiches). Toutefois, une décision écrite de l'autorité d'origine indique toujours que le fonds d'archives doit être considéré comme (dé)classifié dans son intégralité.

Sous-section 4. — Enregistrement

Article 22

Cet article dispose que chaque information classifiée doit être clairement attribuée à un titulaire identifié, garantissant ainsi une traçabilité des données sensibles.

Article 23

Cet article introduit une exception pour les informations classifiées de niveau « RESTREINT » qui ne nécessitent pas d'enregistrement.

Dans ce cas, la responsabilité de la protection des informations incombe au titulaire dès qu'il en prend connaissance, après avoir été informé des restrictions d'utilisation par l'autorité d'origine.

Pour les informations classifiées de niveau « CONFIDENTIEL » ou « SECRET », un enregistrement est obligatoire lors de leur entrée ou sortie de l'organisation.

Les informations de niveau « TRÈS SECRET » doivent également être enregistrées, mais dans un registre distinct.

Par ailleurs, les copies imprimées des documents classifiés de niveau « CONFIDENTIEL » qui restent à l'intérieur de l'organisation ne nécessitent pas d'enregistrement.

Toutefois, les projets de documents de niveau « SECRET » peuvent être exemptés d'enregistrement pendant cinq jours ouvrables, après quoi ils devront être détruits ou enregistrés.

Les registres pour les niveaux « CONFIDENTIEL », « SECRET » et « TRÈS SECRET » peuvent aussi être tenus sous forme électronique, à condition de respecter les normes de sécurité appropriées.

Article 24

Cet article précise que l'utilisation d'informations classifiées dans des systèmes de communication approuvés doit être enregistrée conformément aux processus internes.

Article 25

Cet article souligne que les titulaires des informations classifiées de niveau « SECRET » ou « TRÈS SECRET » doivent toujours connaître leur localisation, garantissant ainsi un contrôle rigoureux sur ces données sensibles.

Sous-section 5. — Reproduction et traduction

Articles 26 à 28

Ces articles établissent des règles concernant la reproduction et la traduction des documents classifiés. Ils disposent que la reproduction ou la traduction d'un document classifié de niveau « TRÈS SECRET » nécessite l'accord écrit de l'autorité d'origine, soulignant ainsi l'importance de la sécurité pour les informations sensibles.

Onderafdeling 2. — Declassificatie van het classificatieniveau
“BEPERKT”

Artikel 20

Dit artikel behoeft geen toelichting.

Onderafdeling 3. — Collectief classificeren of declassificeren

Artikel 21

Dit artikel behandelt de mogelijkheid tot collectieve classificatie of declassificatie van documenten door de overheid van oorsprong. Dit betekent dat een overheid kan beslissen om een classificatieniveau toe te kennen of in te trekken voor een geheel van documenten, bestanden of dossiers die identificeerbaar zijn door een gemeenschappelijk onderwerp, zonder elk document afzonderlijk te moeten onderzoeken.

Deze aanpak strekt ertoe de procedure voor het beheer van geclassificeerde informatie te vereenvoudigen, doordat een globale handeling kan worden gesteld in plaats van een gedetailleerde.

Deze regel staat al in het huidige koninklijk besluit van 24 maart 2000 tot uitvoering van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen (artikel 32) en wordt soms toegepast op oude archief-fondsen (van vóór de inwerkingtreding van de wet van 11 december 1998), waarvoor het niet aangewezen is omwille van hun kwetsbaarheid/fragiliteit, historische waarde, omvang of technische redenen (oude documenten op microfiches) het document zelf individueel te markeren. Daarbij wordt wel altijd via een schriftelijke beslissing van de overheid van oorsprong aangeduid dat het archief-fonds in zijn geheel als ge(de)-classificeerd moet worden beschouwd.

Onderafdeling 4. — Registratie

Artikel 22

Dit artikel bepaalt dat elk stuk geclassificeerde informatie duidelijk moet worden toegewezen aan een geïdentificeerde houder, zodat de traceerbaarheid van gevoelige gegevens kan worden verzekerd.

Artikel 23

Met dit artikel wordt een uitzondering vastgesteld voor geclassificeerde informatie van het niveau “BEPERKT”, waarvoor er geen registratie vereist is.

Hier neemt de houder de verantwoordelijkheid voor de bescherming van de informatie op zich op het moment dat hij er kennis van neemt, nadat hij door de overheid van oorsprong werd geïnformeerd over de beperkingen op de aanwending ervan.

Voor informatie met classificatieniveau “VERTROUWELIJK” of “GEHEIM” is registratie verplicht zodra de informatie bij de organisatie aankomt of deze verlaat.

Informatie van het niveau “ZEER GEHEIM” moet ook worden geregistreerd, maar in een afzonderlijk register.

Afgedrukte kopieën van geclassificeerde documenten van het niveau “VERTROUWELIJK” die binnen de organisatie blijven, moeten overigens niet geregistreerd worden.

Ontwerpdocumenten van het niveau “GEHEIM” kunnen evenwel worden vrijgesteld van registratie gedurende vijf werkdagen. Na die periode moeten ze vernietigd of geregistreerd worden.

De registers voor de niveaus “VERTROUWELIJK”, “GEHEIM” en “ZEER GEHEIM” kunnen bijgehouden worden onder elektronische vorm, op voorwaarde dat de juiste veiligheidsnormen worden nageleefd.

Artikel 24

In dit artikel wordt vastgesteld dat het gebruik van geclassificeerde informatie in goedgekeurde communicatiesystemen geregistreerd moet worden volgens interne processen.

Artikel 25

In dit artikel wordt benadrukt dat houders van geclassificeerde informatie van het niveau “GEHEIM” of “ZEER GEHEIM” steeds de plaats ervan moeten kennen, om een uiterst nauwkeurige controle op deze gevoelige gegevens te waarborgen.

Onderafdeling 5. — Reproductie en vertaling

Artikel 26 tot 28

In deze artikelen worden de regels vastgesteld met betrekking tot de reproductie en vertaling van geclassificeerde documenten. Er wordt in bepaald dat de reproductie of de vertaling van een geclassificeerd document van het niveau “ZEER GEHEIM” het schriftelijk akkoord vereist van de overheid van oorsprong, waardoor het belang van de veiligheid van gevoelige informatie wordt benadrukt.

Pour les documents de niveau « SECRET » ou inférieur, si aucune restriction n'est imposée par l'autorité d'origine, le titulaire peut les reproduire ou les traduire.

En outre, toutes les reproductions et traductions doivent être soumises aux mêmes mesures de protection que celles appliquées à l'original, garantissant ainsi la sécurité continue des informations classifiées. Ces dispositions visent à équilibrer la nécessité de sécurité avec la possibilité d'utiliser les informations de manière efficace.

Sous-section 6. — Transmission et transport

Articles 29 à 32

Les articles 29 à 32 établissent des règles strictes pour la transmission des informations classifiées, en insistant sur la nécessité de prendre des mesures visant à empêcher toute consultation non autorisée.

Les informations doivent être transmises soit par porteur, sous double enveloppe fermée, soit par voie électronique via des systèmes approuvés par l'Autorité nationale de Sécurité, en respectant les mesures de protection appropriées.

Pour les informations classifiées de niveau « RESTREINT », il est également possible de les envoyer par pli recommandé, toujours sous double enveloppe fermée. En cas de circulation interne, les informations de niveau « CONFIDENTIEL » ou supérieur doivent être transportées par porteur (en possession d'une habilitation de sécurité valable d'un niveau au moins équivalent à celle des informations transportées) ou par leur titulaire dans une enveloppe fermée.

Il est impératif que l'organisation où circulent des informations de niveau « RESTREINT » mette en œuvre toutes les mesures de sécurité possibles pour empêcher leur consultation non autorisée, garantissant ainsi la protection de ces informations sensibles.

En outre, les informations classifiées peuvent être transportées au sein de l'installation physique par le titulaire, à condition que toutes les mesures de sécurité nécessaires soient en place pour prévenir toute consultation non autorisée.

Sous-section 7. — Destruction

Article 33

Cet article dispose que les articles de la sous-section s'appliquent sans préjudice des diverses lois existantes qui régissent la classification, la gestion des informations sensibles, l'archivage et la protection des données à caractère personnel.

Cette précision est essentielle car elle garantit que les nouvelles dispositions ne remplacent pas ou ne contredisent pas les règles déjà établies, assurant ainsi une continuité et une cohérence législative.

Par ailleurs, le texte souligne que le titulaire et l'autorité d'origine des informations classifiées doivent régulièrement évaluer l'utilité de ces informations et décider si leur destruction est nécessaire.

Cela reflète une approche proactive et responsable dans la gestion des informations sensibles, visant à éviter la conservation indéfinie de données qui pourraient ne plus être pertinentes ou nécessaires.

Article 34

Cet article établit des règles strictes concernant la gestion des informations classifiées de niveau « TRÈS SECRET ». Il dispose que le titulaire de telles informations ne doit jamais procéder à leur destruction, mais doit les retourner à l'autorité d'origine. Cette mesure vise à garantir la sécurité et l'intégrité des informations sensibles, en évitant qu'elles ne soient perdues ou détruites de manière inappropriée.

L'autorité d'origine est alors responsable de dresser un procès-verbal de la destruction, qui doit inclure des détails sur l'objet détruit et être signé par les personnes ayant effectué la destruction ainsi que par l'officier de sécurité.

Cela crée une traçabilité et une responsabilité claires, essentielles dans le cadre de la gestion des informations classifiées, afin de prévenir toute utilisation abusive ou fuite d'informations.

Documenten van het niveau "GEHEIM" of lager mogen gereproduceerd of vertaald worden door de houder indien er geen beperking werd opgelegd door de overheid van oorsprong.

Bovendien gelden voor alle reproducties en vertalingen dezelfde beschermingsmaatregelen als die die op het origineel werden toegepast, waardoor de voortdurende veiligheid van geclassificeerde informatie verzekerd wordt. Deze bepalingen strekken ertoe een evenwicht te scheppen tussen de veiligheid en de mogelijkheid om informatie op een doeltreffende manier te gebruiken.

Onderafdeling 6. — Verzending en vervoer

Artikel 29 tot 32

De artikelen 29 tot 32 beschrijven strikte regels voor de verzending van geclassificeerde informatie, waarbij de noodzaak wordt benadrukt om maatregelen te nemen om ongeoorloofde raadpleging te voorkomen.

De informatie moet verzonden worden via drager, onder dubbele gesloten omslag of met elektronische middelen via systemen die zijn goedgekeurd door de Nationale Veiligheidsoverheid en met inachtneming van de toepasselijke beschermingsmaatregelen.

Voor geclassificeerde informatie van het niveau "BEPERKT" is het ook mogelijk om deze te verzenden via een ter post aangetekende zending, steeds onder dubbele gesloten omslag. In geval van interne rondzending moet informatie van het niveau "VERTROUWELIJK" of hoger gedragen worden door een drager (in het bezit van een geldige veiligheidsmachtiging van een niveau dat minstens gelijkwaardig is aan de vervoerde informatie) of door de houder ervan en dit onder gesloten omslag.

Het is absoluut noodzakelijk dat een organisatie waarbinnen informatie van het niveau "BEPERKT" circuleert, alle mogelijke veiligheidsmaatregelen neemt om te vermijden dat die informatie ongeoorloofd geraadpleegd wordt, om zo de bescherming van deze gevoelige informatie te verzekeren.

Daarnaast mag geclassificeerde informatie binnen de fysieke entiteit rondgedragen worden door de houder, op voorwaarde dat alle nodige veiligheidsmaatregelen worden genomen om ongeoorloofde raadpleging te voorkomen.

Onderafdeling 7. — Vernietiging

Artikel 33

In dit artikel wordt bepaald dat de artikelen van de onderafdeling van toepassing zijn, onverminderd verschillende bestaande wetten die de classificatie, het beheer van gevoelige informatie, archivering en de bescherming van persoonsgegevens regelen.

Deze beslissing is essentieel, omdat ze garandeert dat de nieuwe bepalingen de reeds vastgestelde regels niet vervangen of tegenspreken, waardoor er een continuïteit en consistentie van wetgeving wordt gewaarborgd.

De tekst benadrukt overigens dat de houder en de overheid van oorsprong van de geclassificeerde informatie regelmatig het nut van die informatie moeten beoordelen en moeten beslissen of deze niet vernietigd moet worden.

Dit weerspiegelt een proactieve en verantwoordelijke benadering van het beheer van gevoelige gegevens, met het doel om te vermijden dat gegevens die mogelijk niet meer pertinent of noodzakelijk zijn, eindeloos worden bewaard.

Artikel 34

In dit artikel worden strikte regels vastgesteld met betrekking tot het beheer van geclassificeerde informatie van het niveau "ZEER GEHEIM". Er wordt bepaald dat de houder van dergelijke informatie nooit mag overgaan tot de vernietiging ervan, maar deze terug dient te bezorgen aan de overheid van oorsprong. Deze maatregel strekt ertoe de veiligheid en integriteit van gevoelige informatie te verzekeren, door te vermijden dat deze niet verloren gaat of op ongeoorloofde wijze vernietigd wordt.

De overheid van oorsprong is daarom verantwoordelijk voor het opstellen van een proces-verbaal voor de vernietiging, waarin het voorwerp van de vernietiging gedetailleerd moet worden beschreven en dat ondertekend moet worden door de personen die de vernietiging uitvoerden, alsook door de veiligheidsofficier.

Dit zorgt voor een duidelijke traceerbaarheid en verantwoordelijkheid, hetgeen essentiële elementen zijn bij het beheer van geclassificeerde informatie om misbruik of een informatielek te voorkomen.

Cet article souligne donc l'importance de la responsabilité et de la traçabilité dans la gestion des informations classifiées, tout en garantissant que les procédures de destruction soient effectuées de manière sécurisée et documentée. Cela contribue à maintenir la confiance dans le système de gestion des informations sensibles et à protéger les intérêts de la sécurité nationale.

Article 35

Cet article traite de la destruction des informations classifiées, spécifiquement celles de niveau « SECRET » ou inférieur.

Il prévoit que cette destruction peut être effectuée par l'autorité d'origine, le titulaire de l'information, ou un officier de sécurité désigné.

Cela inclut également la possibilité pour une personne de contact pour la sécurité de procéder à la destruction des informations classifiées de niveau « RESTREINT ».

Cette procédure est essentielle pour garantir que les informations sensibles ne tombent pas entre de mauvaises mains, ce qui pourrait compromettre la sécurité nationale ou la confidentialité des données.

La nécessité d'enregistrer la destruction des informations classifiées de niveau « CONFIDENTIEL » ou « SECRET » dans un registre souligne l'importance de la traçabilité et de la responsabilité dans la gestion des informations sensibles.

En effet, cette obligation d'enregistrement permet de maintenir un contrôle rigoureux sur les informations classifiées, assurant ainsi que chaque acte de destruction est documenté et justifié. Cela contribue à prévenir les abus et à garantir que seules les personnes autorisées peuvent manipuler ces informations.

Logiquement, cette réglementation s'inscrit dans un cadre plus large de protection des données et de sécurité.

Dans un monde où les cybermenaces et les fuites d'informations sont de plus en plus fréquentes, il est crucial d'établir des protocoles clairs pour la gestion des informations classifiées.

La destruction appropriée de ces informations, accompagnée d'un enregistrement systématique, constitue une mesure préventive contre les risques de divulgation non autorisée.

Cet article établit donc des règles précises pour la destruction des informations classifiées, mettant en avant la responsabilité des autorités et des titulaires d'informations. Cette approche logique et structurée vise à protéger la sécurité des données sensibles tout en assurant une traçabilité nécessaire pour prévenir les abus.

Sous-section 8. — Incidents de sécurité et compromission

Articles 36 à 38

Ces articles disposent qu'en cas d'incident de sécurité impliquant des informations classifiées, l'officier de sécurité ou la personne de contact pour la sécurité doivent être immédiatement informés par écrit.

L'officier de sécurité ou la personne de contact pour la sécurité mène alors une enquête administrative interne et en informe simultanément la direction de l'administration ou de l'organisme concerné, ainsi que l'Autorité nationale de Sécurité. Cela permet à l'Autorité nationale de Sécurité d'exercer ses pouvoirs de contrôle. Si nécessaire, l'Autorité nationale de sécurité informera également l'autorité d'origine des informations classifiées. En effet, selon les réglementations internationales, cela n'est requis que s'il a été constaté que les informations classifiées ont été compromises.

Si une compromission d'informations classifiées de niveau « CONFIDENTIEL » ou supérieur est constatée, l'officier de sécurité doit en faire immédiatement rapport à l'Autorité nationale de Sécurité. Dans ce cas, l'Autorité nationale de Sécurité est tenue d'informer l'autorité d'origine de la compromission et des résultats de l'enquête.

En outre, un résumé des incidents de sécurité et des compromissions survenus au cours de l'année écoulée doit être transmis à l'Autorité nationale de Sécurité par l'officier de sécurité ou, le cas échéant, par la personne de contact pour la sécurité, au plus tard le 15 mars de chaque année.

Ces incidents de sécurité ou compromissions peuvent également concerner des personnes qui ne sont plus en service ou des personnes n'ayant plus besoin d'une habilitation de sécurité.

Dit artikel benadrukt dus het belang van verantwoordelijkheid en van traceerbaarheid bij het beheer van geclassificeerde informatie, door ook te verzekeren dat de vernietigingsprocedures op een beveiligde en gedocumenteerde manier geschieden. Dit helpt om het vertrouwen in het systeem voor het beheer van gevoelige informatie in stand te houden en de belangen van nationale veiligheid te beschermen.

Artikel 35

In dit artikel wordt de vernietiging van geclassificeerde informatie behandeld, meer bepaald die van het niveau "GEHEIM" of lager.

Er wordt bepaald dat deze vernietiging kan worden uitgevoerd door de overheid van oorsprong, door de houder van de informatie of door een aangewezen veiligheidsofficier.

Dit houdt ook de mogelijkheid in dat een contactpersoon voor de veiligheid kan overgaan tot de vernietiging van geclassificeerde informatie van het niveau "BEPERKT".

Deze procedure is essentieel om te waarborgen dat gevoelige informatie niet in slechte handen valt, hetgeen de nationale veiligheid of de vertrouwelijkheid van gegevens zou kunnen compromitteren.

Het feit dat de vernietiging van geclassificeerde informatie van het niveau "VERTROUWELIJK" of "GEHEIM" geregistreerd moet worden in een register, duidt op het belang van traceerbaarheid en van verantwoordelijkheid bij het beheer van gevoelige informatie.

Door middel van deze verplichting tot registratie kan er immers een strikte controle worden gehouden op geclassificeerde informatie, en wordt er verzekerd dat elke handeling van vernietiging gedocumenteerd en gerechtvaardigd wordt. Mede door deze werkwijze wordt misbruik voorkomen en wordt verzekerd dat enkel bevoegde personen informatie kunnen behandelen.

Logischerwijs maken deze regels deel uit van een breder kader inzake gegevensbescherming en veiligheid.

In een wereld waarin cyberdreigingen en informatielekken steeds vaker voorkomen, is het cruciaal om duidelijke protocollen op te stellen voor het beheer van geclassificeerde informatie.

De geëigende vernietiging van deze informatie, samen met systematische registratie, vormt een preventieve maatregel tegen de risico's van ongeoorloofde verspreiding.

In dit artikel worden daarom de precieze regels bepaald voor de vernietiging van geclassificeerde informatie, waarbij de verantwoordelijkheid van de overheden en de houders van informatie wordt benadrukt. Deze logische en gestructureerde aanpak strekt ertoe de veiligheid van gevoelige gegevens te bewaken en de traceerbaarheid te verzekeren die noodzakelijk is om misbruik te voorkomen.

Onderafdeling 8. — Veiligheidsincident en compromittering

Artikel 36 tot 38

In deze artikelen wordt bepaald dat in geval van een veiligheidsincident met betrekking tot geclassificeerde informatie, de veiligheidsofficier of de contactpersoon voor de veiligheid onmiddellijk dienen te worden ingelicht.

De veiligheidsofficier of de contactpersoon voor de veiligheid voeren dan een intern administratief onderzoek uit en lichten tegelijkertijd de directie van het bestuur of de instelling in kwestie in, evenals de Nationale Veiligheidsoverheid. Dit laat de Nationale Veiligheidsoverheid toe om haar bevoegdheden inzake toezicht uit te oefenen. Zo nodig zal de Nationale Veiligheidsoverheid eveneens de overheid van oorsprong van de geclassificeerde informatie informeren. Volgens de internationale regelgeving is dit immers enkel nodig indien werd vastgesteld dat de geclassificeerde informatie gecompromitteerd is.

Indien een compromittering van geclassificeerde informatie van het niveau "VERTROUWELIJK" of hoger wordt vastgesteld, moet de veiligheidsofficier hier van verslag uitbrengen aan de Nationale Veiligheidsoverheid zodra het onderzoek is afgerond. De Nationale Veiligheidsoverheid is in dat geval verplicht om de overheid van oorsprong te informeren van de compromittering en van de resultaten van het onderzoek.

Daarnaast moet er door de veiligheidsofficier of in voorkomend geval door de contactpersoon voor de veiligheid elk jaar, vóór 15 maart, een overzicht van de veiligheidsincidenten en compromitteringen die het afgelopen jaar zijn voorgevallen, worden overgemaakt aan de Nationale Veiligheidsoverheid.

Deze veiligheidsincidenten of compromitteringen kunnen eveneens personen betreffen die niet langer in dienst zijn of die niet meer beschikken over een veiligheidsmachtiging.

CHAPITRE 2. — *Mesures de protection physique*

Le chapitre 2 contient les mesures de protection physique pour l'utilisation d'informations classifiées.

Section 1^{re}. — Dispositions générales

Article 39

L'article 39 dispose que l'Autorité nationale de Sécurité détermine les mesures de protection physique minimales supplémentaires de nature administrative et technique pour l'utilisation d'informations classifiées au sein et en dehors des zones visées à l'article 42. L'Autorité nationale de Sécurité est en effet l'instance qui devra contrôler la conformité des zones visées à l'article 42 avec les mesures de protection exigées par la loi relative à la classification et le présent arrêté. Elle est donc la mieux placée pour élaborer les spécifications techniques.

Article 40

L'article 40 n'appelle aucun commentaire.

Article 41

L'article 41 décrit les informations classifiées pouvant être consultées et les conditions dans lesquelles elles peuvent l'être, respectivement dans la zone administrative et dans la zone sécurisée. Dans son avis, le Conseil d'État demande que l'article 41, alinéas 3 et 4, soit révisé afin de préciser que l'entité est tenue de prendre les mesures permettant d'empêcher toute consultation. Cette disposition a été adaptée en ce sens.

Section 2. — Zones administratives et sécurisées

Tout d'abord, cette section porte sur la mise en place des zones administrative et sécurisée. Elle comprend également les conditions d'accès aux zones administrative et sécurisée, et aborde ensuite la procédure d'approbation d'une zone sécurisée.

Articles 42 et 43

Les articles 42 et 43 n'appellent pas de commentaire supplémentaire.

Article 44

L'article 44 définit les conditions d'accès à une zone sécurisée. À la suite d'une remarque formulée par le Conseil d'État dans son avis et par analogie avec les dispositions de l'article 8, § 2, alinéa 1^{er}, de la loi, il a été précisé à l'article 44, § 1^{er}, 2^o, que les compétences propres des autorités judiciaires n'étaient pas affectées. Cela signifie que les magistrats sont exemptés des exigences de l'article 44, § 1^{er}, 2^o, pendant l'exercice de leurs fonctions judiciaires et qu'ils ont accès à la zone sécurisée sans être escortés.

En réponse à une remarque formulée par le Comité permanent R dans son avis, les précisions nécessaires ont été apportées à l'article 44, § 1^{er}, 3^o, afin de clarifier que le fait d'être titulaire d'une habilitation de sécurité et d'une autorisation spécifique du chef de l'entité s'appliquait cumulativement à l'accès à la zone sécurisée sans être escorté. L'absence de l'une ou de l'autre conduit à ce que l'on ne puisse pénétrer dans la zone sécurisée que sous escorte.

Enfin, le Comité permanent R relève, dans son avis (point 4), que la possibilité prévue à l'article 8, § 2, alinéa 2, de la loi n'était pas développée.

L'article 8, § 2, al. 2 de la loi prévoit que les autorités désignées par le Roi peuvent conditionner l'accès aux locaux, bâtiments ou sites où se trouvent des informations classifiées, notamment à la possession d'une habilitation de sécurité.

Comme indiqué plus haut, l'article 44, § 1^{er}, 2^o du présent arrêté reprend le principe selon lequel l'accès à une zone sécurisée est conditionné à la possession d'une habilitation de sécurité (et à l'autorisation du chef de l'entité). Il est possible de déroger au principe de la possession d'une habilitation de sécurité, si la personne non habilitée est escortée par une personne habilitée pendant son accès à la zone sécurisée (voir article 44, § 1, 3^o du présent arrêté).

Pour répondre à la remarque du Comité permanent R, l'article 44, § 2 du présent arrêté prévoit que ce sont les autorités visées à l'article 12 qui peuvent établir des zones sécurisées, sachant que l'accès à cette zone est conditionné à la possession d'une habilitation de sécurité, comme mentionné ci-dessus (voir article 44, § 1, 2^o du présent arrêté). Pour ces autorités, il est en effet évident qu'elles ont besoin d'une zone sécurisée, qu'elles peuvent donc mettre en place, étant donné qu'elles peuvent classer jusqu'au niveau « TRÈS SECRET ». Bien entendu,

HOOFDSTUK 2. — *De fysieke beschermingsmaatregelen*

Hoofdstuk 2 bevat de fysieke beschermingsmaatregelen voor de aanwending van geclassificeerde informatie.

Afdeling 1. — Algemene bepalingen

Artikel 39

Artikel 39 bepaalt dat de bijkomende minimale fysieke beschermingsmaatregelen van administratieve en technische aard voor de aanwending van geclassificeerde informatie binnen en buiten de zones zoals bedoeld in artikel 42 van voorliggend besluit worden bepaald door de Nationale Veiligheidsoverheid. De Nationale Veiligheidsoverheid is immers de instantie die het toezicht zal moeten uitoefenen op de conformiteit van de in artikel 42 bedoelde zones met de in de Classificatiewet en voorliggend besluit vereiste beschermingsmaatregelen en bijgevolg het best geplaatst om de technische specificiteiten verder uit te werken.

Artikel 40

Artikel 40 vergt geen commentaar.

Artikel 41

Artikel 41 stipuleert welke geclassificeerde informatie onder welke voorwaarden mag geraadpleegd worden in respectievelijk de administratieve en de beveiligde zone. In haar advies vraagt de Raad van State dat artikel 41, derde en vierde lid herzien wordt zodat duidelijker naar voren komt dat de entiteit verplicht is de maatregelen te nemen om het inkijken tegen te gaan. In deze zin is de bepaling aangepast.

Afdeling 2. — Administratieve en beveiligde zones

Eerst en vooral bevat deze afdeling de instelling van de administratieve en de beveiligde zones. Verder bevat deze afdeling de toegangsvoorwaarden voor administratieve en beveiligde zones, om dan in te gaan op de procedure voor de goedkeuring van een beveiligde zone.

Artikelen 42 en 43

Artikelen 42 en 43 vergen geen verdere commentaar.

Artikel 44

Artikel 44 zet de toegangsvoorwaarden uiteen voor een beveiligde zone. Naar aanleiding van een opmerking van de Raad van State in haar advies en naar analogie met het bepaalde in artikel 8, § 2, eerste lid van de wet werd in artikel 44, § 1, 2^o gespecificeerd dat de eigen bevoegdheden van de gerechtelijke overheden onverminderd blijven gelden. Dit betekent dat magistraten gedurende de uitoefening van hun gerechtelijke functie uitgezonderd zijn van de vereisten in artikel 44, § 1, 2^o en zonder begeleiding toegang hebben tot de beveiligde zone.

Naar aanleiding van een opmerking van het Vast Comité I in diens advies werden in artikel 44, § 1, 3^o de nodige preciseringen aangebracht om duidelijk te maken dat het hebben van een veiligheidsmachtiging én een specifieke autorisatie van het hoofd van de entiteit cumulatief gelden voor de toegang tot de beveiligde zone zonder begeleiding. Het ontbreken van één van beiden leidt ertoe dat men de beveiligde zone enkel onder begeleiding kan betreden.

Ten slotte haalt het Vast Comité I in haar advies (punt 4) aan dat er geen uitwerking werd gegeven aan de mogelijkheid voorzien in artikel 8, § 2, tweede lid van de wet.

Artikel 8, § 2, tweede lid van de wet voorziet dat de overheden die de Koning aanwijst de toegang tot lokalen, gebouwen of terreinen die geclassificeerde informatie bevatten aan voorwaarden kan onderwerpen, waaronder het bezit van een veiligheidsmachtiging.

Zoals hoger aangegeven, herneemt artikel 44, § 1, 2^o van voorliggend besluit het principe dat de toegang tot een beveiligde zone enkel mogelijk is mits het bezit van een veiligheidsmachtiging (en de toelating door het hoofd van de entiteit). Van het principe van het bezit van een veiligheidsmachtiging kan worden afgeweken als een niet-gemachtigd persoon tijdens de toegang tot de beveiligde zone wordt begeleid door een gemachtigd persoon (artikel 44, § 1, 3^o van voorliggend besluit).

In antwoord op de opmerking van het Vast Comité I bepaalt artikel 44, § 2 van dit besluit dat het de overheden bedoeld in artikel 12 zijn die beveiligde zones kunnen instellen, wetende dat de toegang tot deze zone afhankelijk is van het bezit van een veiligheidsmachtiging, zoals hiervoor vermeld (artikel 44, § 1, 2^o van voorliggend besluit). Voor deze overheden is het immers evident dat deze een beveiligde zone nodig hebben en dus kunnen instellen, gelet op het feit dat zij tot het niveau "ZEER GEHEIM" kunnen classificeren. Uiteraard moet deze

cette zone de sécurité doit également être homologuée par l'Autorité nationale de Sécurité et elles doivent introduire une demande à cet effet conformément à la procédure décrite dans le présent arrêté. Toutefois, la nécessité d'établir cette zone sécurisée sera déjà présumée en vertu de l'article 44, § 2.

La désignation des autorités visées à l'article 12, à savoir les autorités compétentes pour classer au niveau « TRÈS SECRET » se justifie par le fait que la mesure de sécurité exigée pour la consultation d'informations classifiées au niveau « TRÈS SECRET » correspond à l'exigence de se trouver dans une zone sécurisée (voir article 41 du présent arrêté).

Les autorités autres que celles visées à l'article 12, ou les personnes morales qui ont besoin d'une zone sécurisée parce qu'elles utilisent des informations classifiées, soumettent la demande à cet effet à l'Autorité nationale de Sécurité, conformément à la procédure décrite dans le présent arrêté, qui évaluera la nécessité de cette zone, comme c'est le cas pour une demande d'habilitation de sécurité.

Article 45

Cet article n'appelle aucun commentaire.

Article 46

Cet article traite de la vérification de la déclaration de conformité par l'Autorité nationale de Sécurité. Dans son avis, le Conseil d'État pose la question de savoir si le modèle de déclaration de conformité doit être ajouté en annexe à l'arrêté royal, à l'instar des modèles déjà repris aux annexes 2 à 5.

Cependant, les auteurs soulignent que les évolutions techniques en matière de protection des informations classifiées peuvent entraîner la nécessité de modifier (le modèle de) la déclaration de conformité d'une zone sécurisée. En ce sens, (le modèle de) la déclaration de conformité se distingue fondamentalement des modèles repris aux annexes 2 à 5. C'est pourquoi, et afin d'éviter toute confusion possible due à la diffusion de différents modèles via l'annexe de l'arrêté royal, d'une part, et le site web de l'Autorité nationale de Sécurité, d'autre part, les auteurs ont choisi de ne pas ajouter de modèle de déclaration de conformité en annexe de l'arrêté royal.

Article 47

Cet article n'appelle aucun commentaire.

Article 48

L'article 48 prévoit l'obligation de signaler à l'Autorité nationale de Sécurité toute modification apportée à une installation physique. Le Conseil d'État a relevé dans son avis que les conséquences d'une notification de modification de l'installation physique n'avaient pas été précisées, de sorte que la question se pose de savoir si l'ensemble de la procédure d'approbation doit être à nouveau appliquée. Par conséquent, il est ajouté à la disposition que si la modification concerne une zone sécurisée, l'Autorité nationale de Sécurité peut juger si une nouvelle enquête sur le terrain est nécessaire. La décision d'approbation de cette modification sera notifiée à l'officier de sécurité.

CHAPITRE 3. — Mesures de protection des systèmes de communication et d'information pour les informations classifiées

Le chapitre 3 comporte les mesures de protection des systèmes de communication et d'information pour les informations classifiées.

Article 49

L'article 49 dispose que l'Autorité nationale de Sécurité détermine les mesures de protection minimales supplémentaires de nature administrative et technique des systèmes de communication et d'information pour les informations classifiées. Il s'agit de mesures qui contribuent à la protection de l'information et garantissent les propriétés de confidentialité, d'intégrité, de disponibilité, de non-répudiation et d'authenticité. L'application d'un ensemble de mesures de protection est basée sur la gestion et l'évaluation des risques de sécurité, dans le but d'établir une sécurité proportionnelle avec un équilibre acceptable entre les besoins des utilisateurs, l'investissement requis et le risque de sécurité résiduel. Plus concrètement, il s'agit des mesures de protection techniques des systèmes et réseaux de télécommunication dans lesquels des données classifiées sont utilisées. La directive n'ajoute pas de nouvelles règles juridiques, mais interprète et concrétise l'arrêté d'exécution. En raison de la complexité technique et pour des raisons de sécurité, il convient de partir du principe que l'Autorité nationale de Sécurité, qui doit veiller au respect de ces mesures de protection, est également la mieux placée pour les élaborer en connaissance de cause.

beveiligde zone ook gehomologeerd worden door de Nationale Veiligheidsoverheid en moeten zij hiertoe een aanvraag indienen volgens de procedure beschreven in voorliggend besluit. De noodzaak voor het instellen van deze beveiligde zone zal echter reeds vaststaan op grond van artikel 44, § 2.

De aanwijzing van de in artikel 12 bedoelde overheden, d.w.z. de overheden die bevoegd zijn om gegevens op het niveau "ZEER GEHEIM" te classificeren, wordt gerechtvaardigd door het feit dat de veiligheidsmaatregel die vereist is voor het raadplegen van gegevens die op het niveau "ZEER GEHEIM" geclassificeerd zijn, overeenkomt met de eis dat deze gegevens zich in een beveiligde zone moeten bevinden (zie artikel 41 van voorliggend besluit).

Overheden, die geen overheden zijn waarnaar wordt verwezen in artikel 12, of rechtspersonen die een beveiligde zone behoeven omdat ze geclassificeerde informatie aanwenden, dienen hiertoe de aanvraag in bij de Nationale Veiligheidsoverheid, volgens de procedure beschreven in voorliggend besluit, die de noodzaak hiervan zal beoordelen, net zoals dit het geval is voor een aanvraag voor een veiligheidsmachtiging.

Artikel 45

Dit artikel vergt geen commentaar.

Artikel 46

Dit artikel gaat in op de verificatie van de conformiteitsverklaring door de Nationale Veiligheidsoverheid. De Raad van State stelt in haar advies de vraag of het model van conformiteitsverklaring als bijlage aan het koninklijk besluit dient te worden toegevoegd, naar voorbeeld van de modellen die reeds opgenomen zijn in de bijlagen 2 tot 5.

De opstellers wijzen er echter op dat technische evoluties in de bescherming van geclassificeerde informatie ertoe kunnen leiden dat (het model van) de conformiteitsverklaring voor een beveiligde zone dient gewijzigd te worden. In deze zin verschilt (het model van) de conformiteitsverklaring fundamenteel van de modellen opgenomen in bijlagen 2 tot 5. Gelet hierop, en om mogelijke verwarring te vermijden door de verspreiding van verschillende modellen via enerzijds de bijlage van het koninklijk besluit en anderzijds de website van de Nationale Veiligheidsoverheid, kiezen de opstellers ervoor om geen model van conformiteitsverklaring toe te voegen als bijlage aan het koninklijk besluit.

Artikel 47

Dit artikel vergt geen commentaar.

Artikel 48

Artikel 48 bevat de verplichting om iedere wijziging aan een fysieke installatie te melden aan de Nationale Veiligheidsoverheid. De Raad van State merkte op in haar advies dat er niet werd gepreciseerd wat de gevolgen zijn van een melding van een wijziging aan de fysieke installatie zodat de vraag rijst of de hele goedkeuringsprocedure opnieuw toegepast moet worden. Bijgevolg wordt aan de bepaling toegevoegd dat in geval de wijziging een beveiligde zone betreft, de Nationale Veiligheidsoverheid kan oordelen of er een nieuw terreinonderzoek nodig is. De beslissing inzake de goedkeuring van deze wijziging wordt ter kennis wordt gebracht aan de veiligheidsofficier.

HOOFDSTUK 3. — De beschermingsmaatregelen van communicatie- en informatiesystemen voor geclassificeerde informatie

Hoofdstuk 3 bevat de beschermingsmaatregelen van communicatie- en informatiesystemen voor geclassificeerde informatie.

Artikel 49

Artikel 49 bepaalt dat de bijkomende minimale beschermingsmaatregelen van administratieve en technische aard voor communicatie- en informatiesystemen voor geclassificeerde informatie worden bepaald door de Nationale Veiligheidsoverheid. Het betreft maatregelen die bijdragen tot de informatieborging en het garanderen van de eigenschappen vertrouwelijkheid, integriteit, beschikbaarheid, onweerlegbaarheid en authenticiteit. Het toepassen van een reeks beschermingsmaatregelen gebeurt op basis van het beheer van de beveiligingsrisico's en van een risico-inschatting, met als doel het instellen van een proportionele beveiliging met een aanvaardbaar evenwicht tussen de noden van de gebruikers, de vereiste investering en het resterend veiligheidsrisico. Meer concreet gaat het over de technische beschermingsmaatregelen van telecommunicatiesystemen en -netwerken waarin geclassificeerde gegevens worden aangewend. De richtlijn voegt geen nieuwe rechtsregels toe maar interpreteert en concretiseert het uitvoeringsbesluit. Omwille van de technische complexiteit en omwille van veiligheidsredenen moet ervan uitgegaan worden dat de Nationale Veiligheidsoverheid, die moet toezien op de naleving van deze beschermingsmaatregelen, ook het best geplaatst is om deze met kennis van zaken uit te werken.

Article 50

L'article 50 prévoit l'obligation pour l'officier de sécurité d'évaluer si un système de communication et d'information offre les garanties suffisantes en ce qui concerne la confidentialité, l'intégrité et la disponibilité du système et des informations qu'il contient. L'article aborde ensuite la déclaration de conformité que l'officier de sécurité doit envoyer à l'Autorité nationale de Sécurité.

Dans son avis, le Conseil d'État pose la question de savoir si le modèle de déclaration de conformité doit être ajouté en annexe à l'arrêté royal, à l'instar des modèles déjà repris aux annexes 2 à 5.

Les auteurs soulignent cependant que les évolutions techniques en matière de protection des systèmes de communication et d'information et les informations qu'ils contiennent peuvent entraîner la nécessité de modifier (le modèle de) la déclaration de conformité d'un système de communication et d'information. En ce sens, (le modèle de) la déclaration de conformité se distingue fondamentalement des modèles repris aux annexes 2 à 5. Pour cette raison, et afin d'éviter toute confusion possible due à la diffusion de différents modèles au moyen de l'annexe de l'arrêté royal, d'une part, et du site web de l'Autorité nationale de Sécurité, d'autre part, les auteurs ont choisi de ne pas ajouter de modèle de déclaration de conformité en annexe de l'arrêté royal.

Articles 51 et 52

L'article 51 n'appelle aucun commentaire.

L'article 52 prévoit que, pour les systèmes d'information utilisant des informations classifiées de niveau « RESTREINT », l'Autorité nationale de Sécurité PEUT demander à l'entité de soumettre le système concerné à des tests de sécurité afin de vérifier que les garanties suffisantes sont atteintes en termes de confidentialité, d'authenticité et de non-répudiation de ces systèmes et des informations qu'ils contiennent.

Tant l'OTAN que l'UE autorisent que des entités approuvent par elles-mêmes leur système de communication et d'information jusqu'au niveau « RESTREINT » tout au plus. Les auteurs du présent projet ne sont toutefois pas favorables à ce genre d'auto-homologation ou d'auto-accreditation pour des raisons de sécurité, et préfèrent que l'Autorité nationale de Sécurité examine la documentation fournie en ce qui concerne la sécurité, y compris la gestion des risques et les déclarations sur les risques résiduels, les spécifications des exigences en matière de sécurité liées au système, les documents attestant la mise en œuvre/le déploiement de la sécurité et les procédures de sécurité opérationnelle, ainsi que la garantie que cette documentation est conforme aux règles et aux directives imposées par l'Autorité nationale de Sécurité. L'Autorité nationale de Sécurité effectue un contrôle physique à un stade ultérieur afin d'éviter qu'un certain nombre d'entités belges ne puissent, à défaut d'approbation d'un système de communication et d'information en temps et en heure, prendre part à des projets lancés par l'OTAN ou l'UE.

Article 53

L'article 53 dispose que l'Autorité nationale de Sécurité notifie sa décision concernant l'approbation du système de communication et d'information à l'autorité fonctionnelle du système de communication et d'information et à l'officier de sécurité ou à la personne de contact pour la sécurité. Si l'Autorité nationale de Sécurité prend une décision de refus d'approbation du système de communication et d'information, il s'agit d'une décision administrative contre laquelle un recours peut être introduit devant la section du contentieux administratif du Conseil d'État conformément à l'article 14 des lois coordonnées sur le Conseil d'État, à moins que le législateur ne décide encore à l'avenir de confier cette compétence à une juridiction administrative spécifique créée à cet effet, tel que l'Organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité.

La décision d'approbation du système de communication et d'information a une durée de validité de trois ans au maximum. Ce délai se justifie par l'évolution rapide des technologies. Le même délai a été prévu pour les produits cryptographiques (article 61 du présent arrêté).

Artikel 50

Artikel 50 bepaalt de verplichting voor de veiligheidsofficier om te beoordelen of een communicatie- en informatiesysteem voldoende garanties biedt ten aanzien van de vertrouwelijkheid, de integriteit, en de beschikbaarheid van het systeem en de informatie die het bevat. Het artikel gaat vervolgens in op de conformiteitsverklaring die de veiligheidsofficier dient te versturen naar de Nationale Veiligheids-overheid.

De Raad van State stelt in haar advies de vraag of het model van conformiteitsverklaring als bijlage aan het koninklijk besluit dient te worden toegevoegd, naar voorbeeld van de modellen die reeds opgenomen zijn in de bijlagen 2 tot 5.

De opstellers wijzen er echter op dat technische evoluties in de bescherming van communicatie- en informatiesystemen en de informatie die ze bevatten ertoe kunnen leiden dat (het model van) de conformiteitsverklaring voor een communicatie- en informatiesysteem dient gewijzigd te worden. In deze zin verschilt (het model van) de conformiteitsverklaring fundamenteel van de modellen opgenomen in bijlagen 2 tot 5. Gelet hierop, en om mogelijke verwarring te vermijden door de verspreiding van verschillende modellen via enerzijds de bijlage van het koninklijk besluit en anderzijds de website van de Nationale Veiligheids-overheid, kiezen opstellers ervoor om geen model van conformiteitsverklaring toe te voegen als bijlage aan het koninklijk besluit.

Artikelen 51 en 52

Artikel 51 vergt geen commentaar.

Artikel 52 voorziet dat voor communicatie- en informatiesystemen die geclassificeerde informatie met het classificatieniveau "BEPERKT" aanwenden, de Nationale Veiligheids-overheid de entiteit KAN verzoeken om het desbetreffende systeem te onderwerpen aan beveiligingstests om na te gaan of voldoende garanties zijn bereikt ten aanzien van de vertrouwelijkheid, de authenticiteit en de niet-weerlegbaarheid van deze systemen en de informatie die ze bevatten.

Zowel de NAVO als de EU laten toe dat entiteiten zelf hun communicatie- en informatiesysteem van maximum het niveau "BEPERKT" goedkeuren. De opstellers van voorliggend besluit zijn geen voorstander van dergelijke auto-homologatie of zelf-accrediatie omwille van veiligheidsredenen en geven er de voorkeur aan dat de Nationale Veiligheids-overheid de verstrekte documentatie over de beveiliging bestudeert, met inbegrip van risicobeheer en verklaringen over resterende risico's, systeemgebonden specificaties van beveiligings-eisen, documenten die de beveiligingsimplementatie en de operationele beveiligingsprocedures bewijzen, evenals de garantie dat die documentatie strookt met de regels en richtlijnen die worden opgelegd door de Nationale Veiligheids-overheid. De fysieke controle door de Nationale Veiligheids-overheid gebeurt dan in een latere fase, dit om te vermijden dat heel wat Belgische entiteiten, bij gebrek aan een tijdig goedgekeurd communicatie- en informatiesysteem niet tijdig kunnen meedingen aan projecten gelanceerd door de NAVO of de EU.

Artikel 53

Artikel 53 stipuleert dat de Nationale Veiligheids-overheid zijn beslissing betreffende de goedkeuring van het communicatie- en informatiesysteem ter kennis brengt van de functionele autoriteit van het communicatie- en informatiesysteem en de veiligheidsofficier of de contactpersoon voor de veiligheid. In het geval dat de Nationale Veiligheids-overheid een beslissing neemt tot weigering van de goedkeuring van het communicatie- en informatiesysteem wordt dit beschouwd als een administratieve beslissing, waartegen een beroep open staat bij de afdeling bestuursrechtspraak van de Raad van State overeenkomstig artikel 14 van de gecoördineerde wetten op de Raad van State, tenzij de wetgever in de toekomst nog zal beslissen om dit toe te vertrouwen aan een specifiek daartoe opgericht administratief rechtscollege, zoals het Beroepsorgaan inzake veiligheidsmaatregelen, – attesten of – adviezen.

De beslissing tot goedkeuring van het communicatie- en informatiesysteem heeft een geldigheidsduur van maximum drie jaar. Deze termijn is te verantwoorden omwille van de snelle technologische evolutie. Dezelfde termijn werd voorzien voor cryptografische producten (artikel 61 van het voorliggend besluit).

Une demande de renouvellement de la décision peut être introduite entre le sixième et le septième mois avant la date d'expiration de sa validité, délai considéré comme réaliste par les services. En effet, il ne serait pas souhaitable que la demande soit introduite un jour avant la fin de la période de validité de la décision, et que l'autorité fonctionnelle continue ensuite à utiliser le système de communication et d'information sans approbation. Le délai pour la demande de renouvellement est nouveau et ne figurait pas encore dans l'actuel arrêté royal du 24 mars 2000.

CHAPITRE 4. — *Mesures de protection relatives au matériel cryptographique destiné au traitement d'informations classifiées*

Section 1^{re}. — Généralités

Le chapitre 4 contient les mesures de protection relatives au matériel cryptographique destiné au traitement d'informations classifiées. La section 1 établit les dispositions générales.

Article 54

L'article 54 dispose que l'Autorité nationale de Sécurité fixe les exigences minimales administratives et techniques en termes d'évaluation, d'approbation, d'utilisation, y compris du compte cryptographique, de transport, de partage, de conservation, de gestion, y compris la production des clés cryptographiques, et de destruction du matériel cryptographique destiné au traitement des informations classifiées.

L'Autorité nationale de Sécurité est habilitée à délivrer, modifier, suspendre ou révoquer les approbations des produits cryptographiques. Une approbation signifie que certains produits cryptographiques peuvent être utilisés comme mesure de protection des informations classifiées employées dans les systèmes de communication et d'information. En outre, l'Autorité nationale de Sécurité est également compétente pour gérer le matériel cryptographique destiné à la protection des informations classifiées, y compris les clés cryptographiques, en Belgique. La gestion comprend également le partage de matériel cryptographique national et international pour les utilisateurs. Le matériel cryptographique international est principalement, mais pas exclusivement, celui utilisé dans les contextes de l'UE, de l'OTAN et de l'ESA. L'Autorité nationale de Sécurité garde le contrôle sur les utilisateurs belges de ce matériel sensible, obligation par ailleurs inscrite dans la réglementation internationale.

En raison de la complexité technique et pour des raisons de sécurité, il est souhaitable d'exposer plus en détail les mesures fixées par l'arrêté d'exécution par le biais d'une directive de l'Autorité nationale de Sécurité. Compte tenu de la complexité technique et dans l'intérêt de la sécurité, l'Autorité nationale de Sécurité, qui doit veiller au respect de ces mesures de protection, est également la mieux placée pour les élaborer en connaissance de cause.

Articles 55 et 56

Les articles 55 et 56 n'appellent aucun commentaire.

Section 2. — Procédure d'approbation de produits cryptographiques

La section 2 traite de la procédure d'approbation de produits cryptographiques.

Article 57

L'article 57 n'appelle aucun commentaire.

Article 58

L'article 58 dispose que le produit cryptographique est évalué par l'Autorité nationale de Sécurité. À la demande de l'Autorité nationale de Sécurité, cette évaluation peut également être effectuée par le Service général du Renseignement et de la Sécurité des Forces Armées ou par un autre organisme (tel que l'École Royale Militaire) conformément à la politique de sécurité de l'Autorité nationale de Sécurité, par analogie avec ce qui est prévu en matière de gestion et de partage de matériel cryptographique à l'article 3 de l'arrêté royal du 22 décembre 2023 relatif au fonctionnement et à l'organisation de l'Autorité nationale de Sécurité.

Compte tenu de la remarque formulée par le Conseil d'État au sujet de la nature « réglementaire » des directives du Conseil national de Sécurité, les auteurs du présent projet ont choisi de supprimer la référence à celles-ci. Les dispositions nécessaires seront prises entre les instances compétentes en ce qui concerne cette évaluation, conformément à la politique de sécurité établie par l'Autorité nationale de Sécurité.

Een hernieuwing kan worden aangevraagd tussen de zes en de zeven maanden vóór het einde van de geldigheidsduur van de beslissing, hetgeen door de diensten werd aangewezen als een realistische termijn. Het kan immers niet de bedoeling zijn dat de aanvraag een dag vóór het einde van de geldigheidsduur van de beslissing wordt aangevraagd en de functionele autoriteit vervolgens zonder homologatie verder werkt met het communicatie- en informatiesysteem. De termijn voor de vraag tot hernieuwing is nieuw en stond nog niet in het huidige koninklijk besluit van 24 maart 2000.

HOOFDSTUK 4. — *De beschermingsmaatregelen verbonden aan cryptografisch materiaal voor de behandeling van geclassificeerde informatie*

Afdeling 1. — Algemeen

Hoofdstuk 4 bevat de beschermingsmaatregelen verbonden aan cryptografisch materiaal voor de behandeling van geclassificeerde informatie en afdeling 1 stelt de algemene bepalingen vast.

Artikel 54

Artikel 54 stelt dat de Nationale Veiligheidsoverheid bepaalt wat de minimale administratieve en technische vereisten zijn voor de evaluatie, de goedkeuring, het gebruik, waaronder de cryptografische account, het transport, de verdeling, de bewaring, het beheer, met inbegrip van de productie van cryptografische sleutels, en de vernietiging van cryptografisch materiaal voor de behandeling van geclassificeerde informatie.

De Nationale Veiligheidsoverheid is bevoegd om goedkeuringen van cryptografische producten af te leveren, te wijzigen, te schorsen of in te trekken. Een goedkeuring houdt in dat bepaalde cryptografische producten gebruikt mogen worden als maatregel voor de bescherming van geclassificeerde informatie aangewend in de communicatie- en informatiesystemen. Daarnaast is de Nationale Veiligheidsoverheid ook bevoegd om cryptografisch materiaal voor de bescherming van geclassificeerde informatie, met inbegrip van de cryptografische sleutels, in België te beheren. Het beheer omvat tevens de verdeling van nationaal en internationaal cryptografisch materiaal naar de gebruikers. Het internationaal cryptografisch materiaal is voornamelijk, maar niet uitsluitend, het materiaal gebruikt binnen EU-, NAVO- en ESA-context. Zo behoudt de Nationale Veiligheidsoverheid de controle over Belgische gebruikers van dit gevoelig materiaal, een verplichting die overigens voorkomt in de internationale regelgeving.

Omwille van de technische complexiteit en omwille van veiligheidsredenen is het wenselijk om de maatregelen, die door het uitvoeringsbesluit worden vastgelegd, nader uiteen te zetten via een richtlijn van de Nationale Veiligheidsoverheid. Gelet op de technische complexiteit en ten bate van de veiligheid is de Nationale Veiligheidsoverheid, die moet toezien op de naleving van deze beschermingsmaatregelen, ook het best geplaatst om deze met kennis van zaken uit te werken.

Artikelen 55 en 56

Artikelen 55 en 56 vergen geen commentaar.

Afdeling 2. — Goedkeuringsprocedure voor cryptografische producten

Afdeling 2 bespreekt de goedkeuringsprocedure voor cryptografische producten.

Artikel 57

Artikel 57 vergt geen commentaar.

Artikel 58

Artikel 58 bepaalt dat het cryptografisch product wordt geëvalueerd door de Nationale Veiligheidsoverheid. Op vraag van de Nationale Veiligheidsoverheid kan deze evaluatie ook gebeuren door de Algemene Dienst Inlichting en Veiligheid van de Krijgsmacht of een andere instantie (zoals de Koninklijke Militaire School) overeenkomstig het veiligheidsbeleid van de Nationale Veiligheidsoverheid, naar analogie van hetgeen is bepaald voor wat betreft het beheer en de verdeling van cryptografisch materiaal in artikel 3 van het koninklijk besluit van 22 december 2023 houdende de werking en de organisatie van de Nationale Veiligheidsoverheid.

Gezien de opmerking van de Raad van State met betrekking tot het "verordenende" karakter van de richtlijnen van de Nationale Veiligheidsraad, hebben de opstellers van voorliggend ontwerp ervoor gekozen om richtlijnen te schrappen in dit verband. Tussen de desbetreffende instanties zullen de nodige afspraken worden gemaakt betreffende deze evaluatie overeenkomstig het veiligheidsbeleid van de Nationale Veiligheidsoverheid.

Article 59

À l'article 59, les termes « de niveau « RESTREINT » ou supérieur » sont supprimés car ceux-ci sont redondants, comme également souligné par le Conseil d'État.

Article 60

L'article 60 est modifié conformément à la remarque du Conseil d'État. Les termes « Dans les cas prévus par le Conseil national de sécurité » sont supprimés afin que l'Autorité nationale de Sécurité puisse déterminer par elle-même les cas dans lesquels un autre pays ou une autre instance peut demander une évaluation d'un produit cryptographique, conformément aux compétences confiées à l'Autorité nationale de Sécurité à l'article 1^{quater} de la loi.

Article 61

L'article 61 dispose que l'Autorité nationale de Sécurité notifie sa décision concernant l'approbation d'un produit cryptographique à l'autorité fonctionnelle du système de communication et d'information. Si l'Autorité nationale de Sécurité prend une décision de refus d'approbation d'un produit cryptographique, il s'agit d'une décision administrative contre laquelle un recours peut être introduit devant la section du contentieux administratif du Conseil d'État conformément à l'article 14 des lois coordonnées sur le Conseil d'État, à moins que le législateur ne décide à l'avenir de confier cette compétence à une juridiction administrative spécifique créée à cet effet, tel que l'Organe de recours en matière d'habilitations de sécurité, attestations de sécurité ou avis de sécurité.

Articles 63 et 63

Les articles 62 et 63 n'appellent aucun commentaire.

Section 3. — Gestion et distribution du matériel cryptographique

La section 3 traite de la gestion et de la distribution du matériel cryptographique.

Article 64

L'article 64 impose la possession d'un compte cryptographique, délivrée par l'Autorité nationale de Sécurité, aux instances qui souhaitent utiliser du matériel cryptographique pour les informations classifiées.

Par souci de clarté, la "crypto licence" a été remplacée dans le projet soumis pour avis au Conseil d'Etat par « compte cryptographique ».

La gestion et la distribution du matériel cryptographique relèvent de la compétence de l'Autorité nationale de Sécurité (article 1^{quater}, 8°, de la loi relative à la classification). Afin que l'Autorité nationale de Sécurité puisse distribuer du matériel cryptographique aux instances qui souhaitent l'utiliser pour transmettre des informations classifiées, un compte cryptographique approuvée par l'Autorité nationale de Sécurité est nécessaire. Dans le cas contraire, le fonctionnement de l'Autorité nationale de Sécurité en ce qui concerne la gestion et la distribution du matériel cryptographique serait sérieusement perturbé. Le compte cryptographique montre qu'une entreprise peut utiliser du matériel cryptographique conformément aux exigences de la loi et du présent arrêté, et qu'elle dispose par conséquent d'une infrastructure adéquate (en termes de sécurité physique et de systèmes de communication et d'information), ainsi que d'un personnel formé et titulaire d'une habilitation de sécurité. À l'article 1^{ter} de la loi précitée, le législateur a stipulé que l'Autorité nationale de Sécurité était une autorité de sécurité dont le fonctionnement et l'organisation étaient déterminés par le Roi, par arrêté délibéré en Conseil des Ministres. L'article 64 de l'arrêté s'y rapporte. L'article 1^{ter} de la loi précitée est également mentionné dans les fondements juridiques énumérés dans le préambule de l'arrêté.

En outre, l'article 7, § 1^{er}, de la loi précitée prévoit que le Roi, par arrêté délibéré en Conseil des Ministres, détermine les modalités de la protection et de la déclassification des informations classifiées. La possession d'un compte cryptographique approuvée par l'Autorité nationale de Sécurité est requise pour que du matériel cryptographique puisse être distribué à son possesseur en vue de l'utilisation d'informations classifiées.

Artikel 59

In artikel 59 worden de bewoordingen "met het classificatieniveau "BEPERKT" of hoger" weggelaten, gezien deze overbodig zijn, zoals ook de Raad van State opmerkte.

Artikel 60

Artikel 60 wordt aangepast overeenkomstig de opmerking van de Raad van State. De bewoordingen "In de gevallen bepaald door de Nationale Veiligheidsraad" worden geschrapt, zodat de Nationale Veiligheidsoverheid zelf kan bepalen in welke gevallen een ander land of een andere instantie kan verzoeken om een evaluatie uit te voeren van een cryptografisch product, overeenkomstig de bevoegdheden die aan de Nationale Veiligheidsoverheid werden toevertrouwd in artikel 1^{quater} van de wet.

Artikel 61

Artikel 61 stipuleert dat de Nationale Veiligheidsoverheid zijn beslissing betreffende de goedkeuring van een cryptografisch product ter kennis brengt van de functionele autoriteit van het communicatie- en informatiesysteem. In het geval dat de Nationale Veiligheidsoverheid een beslissing neemt tot weigering van de goedkeuring van een cryptografisch product wordt dit beschouwd als een administratieve beslissing, waartegen een beroep open staat bij de afdeling bestuursrechtsspraak van de Raad van State overeenkomstig artikel 14 van de gecoördineerde wetten op de Raad van State, tenzij de wetgever in de toekomst nog zal beslissen om dit toe te vertrouwen aan een specifiek daartoe opgericht administratief rechtcollege, zoals het Beroepsorgaan inzake veiligheidsmachtingen, – attesten of – adviezen.

Artikelen 63 en 63

De artikelen 62 en 63 vergen geen commentaar.

Afdeling 3. — Beheer en verdeling van cryptografisch materiaal

Afdeling 3 bevat het beheer en verdeling van cryptografisch materiaal.

Artikel 64

Artikel 64 legt het bezit van een cryptografische account op, afgegeven door de Nationale Veiligheidsoverheid, voor instanties die cryptografisch materiaal wensen te gebruiken voor geclassificeerde informatie.

Omwille van de duidelijkheid werd "cryptolicensie" uit het ontwerp voorgelegd voor advies aan de Raad van State vervangen door "cryptografische account".

Het beheer en de verdeling van cryptografisch materiaal is een bevoegdheid van de Nationale Veiligheidsoverheid (artikel 1^{quater}, 8° van de Classificatiewet). Opdat de Nationale Veiligheidsoverheid cryptografisch materiaal kan verdelen aan instanties die dit materiaal wensen te gebruiken voor het versturen van geclassificeerde informatie, is een door de Nationale Veiligheidsoverheid goedgekeurde cryptografische account nodig. Zo niet zou de werking van de Nationale Veiligheidsoverheid met betrekking tot het beheer en de verdeling van het cryptografisch materiaal ernstig verstoord worden. De cryptografische account toont aan dat een bedrijf cryptografisch materiaal kan gebruiken overeenkomstig de voorschriften van de wet en voorliggend besluit en bijgevolg over een adequate infrastructuur beschikt (op het vlak van fysieke veiligheid en de communicatie- en informatiesystemen), evenals opgeleide personeel in het bezit van een veiligheidsmachting. De wetgever heeft in artikel 1^{ter} van voormelde wet bepaald dat de Nationale Veiligheidsoverheid een veiligheidssoverheid is waarvan de werking en de organisatie bepaald worden door de Koning, bij een besluit vastgesteld in overleg in de Ministerraad. Artikel 64 van het besluit heeft hierop betrekking. Artikel 1^{ter} van voormelde wet wordt ook vermeld in de rechtsgronden die worden opgesomd in de aanhef van het besluit.

Verder stelt artikel 7, § 1 van voormelde wet dat de Koning, bij een besluit vastgesteld na overleg in de Ministerraad, de nadere regels bepaalt van de bescherming en de declassificatie van geclassificeerde informatie. Het bezit van een door de Nationale Veiligheidsoverheid goedgekeurde cryptografische account is vereist alvorens cryptografisch materiaal aan de bezitter ervan kan worden verdeeld voor het gebruik van geclassificeerde informatie.

Articles 65 et 66

Les articles 65 et 66 n'appellent aucun commentaire.

Section 4. — Situations d'urgence

La section 4 définit les situations d'urgence.

Articles 67 et 68

Les articles 67 et 68 ont été adaptés sur avis du Conseil d'État pour préciser que les informations classifiées du niveau de classification « RESTREINT » ou « CONFIDENTIEL » pouvaient être transmises au moyen d'un produit cryptographique approuvé pour un niveau de classification inférieur ou sans cryptage, lorsque toutes les conditions étaient remplies (article 67, (a) ET (b)). Ces conditions représentent une liste exhaustive.

Les informations classifiées du niveau de classification « RESTREINT » ou « CONFIDENTIEL » ne permettront que rarement de « neutraliser la menace ». Il s'agit, par conséquent, de circonstances très exceptionnelles. Si les conditions ne sont pas remplies, il peut s'agir d'un incident de sécurité ou d'une compromission.

Contrairement à ce que suggère le Conseil d'État, l'article 68 ne devrait pas faire référence aux « circonstances exceptionnelles visées à l'article 67 », car il s'agit d'une situation différente, dans laquelle des informations ayant le niveau de classification « RESTREINT » peuvent, dans les circonstances décrites à l'article 68, être transmises sans avoir été cryptées.

Article 69

L'article 69 n'appelle aucun commentaire.

CHAPITRE 5. — *Mesures de protection relatives aux personnes physiques et morales*Section 1^{re}. — Habilitation de sécurité pour les personnes physiquesSous-section 1^{re}. — Généralités

Le chapitre 5 contient les mesures de protection relatives aux personnes physiques et morales et la section 1 traite de l'habilitation de sécurité pour les personnes physiques.

Article 70

L'article 70 définit la manière dont l'Autorité nationale de Sécurité doit traiter les demandes d'habilitation de sécurité pour les personnes physiques. Il s'agit de l'accès aux informations classifiées à partir du niveau « CONFIDENTIEL », étant donné qu'aucune habilitation de sécurité n'est requise pour les informations classifiées au niveau « RESTREINT ».

Le paragraphe 1^{er} décrit la situation des personnes de nationalité belge. Si ces personnes ont besoin d'accéder à des informations classifiées dans les strictes limites du besoin d'en connaître, elles peuvent se voir octroyer une habilitation de sécurité par les autorités compétentes, aux conditions prévues par la loi et le présent arrêté. Il convient de tenir compte à cet égard de la directive du Conseil national de Sécurité définissant l'ampleur de l'enquête de sécurité visée à l'article 18, alinéa 5, de la loi. Cette directive n'est communiquée qu'aux agents et membres des services de renseignement et de sécurité, à l'autorité de sécurité, ainsi qu'au Comité permanent R, conformément à l'article 18, alinéa 6, de la loi.

Le paragraphe 2 indique que les personnes de nationalité étrangère (y compris les ressortissants d'un pays non membre de l'UE) peuvent également se voir octroyer une habilitation de sécurité à condition d'être ressortissantes d'un pays avec lequel la Belgique a conclu un accord en matière d'échange et de protection mutuelle des informations classifiées. Une enquête devrait dès lors pouvoir être menée par le service de renseignement et de sécurité belge compétent, conformément à la directive du Conseil national de Sécurité susmentionnée. L'habilitation de sécurité étrangère peut également être reconnue par les autorités compétentes.

Le paragraphe 3 prévoit qu'un tel accord en matière d'échange et de protection mutuelle des informations classifiées n'est pas requis pour les ressortissants d'un État membre de l'Espace économique européen ou de la Confédération suisse. Pour les pays qui ne font pas partie de l'Espace économique européen ou de la Confédération suisse, un tel accord est nécessaire afin d'instaurer un cadre juridique objectif pour l'échange bilatéral et la protection mutuelle d'informations classifiées et disposer d'une vue d'ensemble de la teneur de l'assistance fournie par le pays étranger concerné, le cas échéant.

Artikelen 65 en 66

De artikelen 65 en 66 vergen geen commentaar.

Afdeling 4. — Noodsituaties

Afdeling 4 legt de noodsituaties vast.

Artikelen 67 en 68

De artikelen 67 en 68 werden op advies van de Raad van State aangepast om te verduidelijken dat geclassificeerde informatie met het classificatieniveau "BEPERKT" of "VERTROUWELIJK" door middel van een voor een lager classificatieniveau goedgekeurd cryptografisch product of zonder versleuteling kan worden doorgestuurd wanneer alle voorwaarden samen zijn vervuld (artikel 67, (a) EN (b)). De voorwaarden maken een exhaustieve opsomming uit.

Geclassificeerde informatie met het classificatieniveau "BEPERKT" of "VERTROUWELIJK" zal zelden in staat zijn "om de dreiging te neutraliseren", het gaat bijgevolg om zeer uitzonderlijke omstandigheden. Indien de voorwaarden niet zijn vervuld, kan er sprake zijn van een veiligheidsincident of compromittering.

In tegenstelling tot hetgeen de Raad van State suggereert, moet in artikel 68 niet verwezen worden naar de "in artikel 67 bedoelde uitzonderlijke omstandigheden", gezien dit om een andere situatie gaat, waarin informatie met het classificatieniveau "BEPERKT" onversleuteld verstuurd kan worden in de in artikel 68 beschreven omstandigheden.

Artikel 69

Artikel 69 vergt geen commentaar.

HOOFDSTUK 5. — *De beschermingsmaatregelen gerelateerd aan natuurlijke personen en rechtspersonen*

Afdeling 1. — De veiligheidsmachtiging voor natuurlijke personen

Onderafdeling 1. — Algemeen

Hoofdstuk 5 bevat de beschermingsmaatregelen gerelateerd aan natuurlijke personen en rechtspersonen en afdeling 1 betreft de veiligheidsmachtiging voor natuurlijke personen.

Artikel 70

Artikel 70 bepaalt hoe de aanvragen voor veiligheidsmachtigingen voor natuurlijke personen moeten behandeld worden door de Nationale Veiligheidsoverheid. Het gaat om toegang tot geclassificeerde informatie vanaf het niveau "VERTROUWELIJK", gezien voor informatie met het classificatieniveau "BEPERKT" geen veiligheidsmachtiging is vereist.

Paragraaf 1 omschrijft de situatie voor personen met de Belgische nationaliteit. Indien deze binnen de strikte grenzen van een noodzaak tot kennisname toegang nodig hebben tot geclassificeerde informatie, kunnen zij een veiligheidsmachtiging verkrijgen van de bevoegde autoriteiten volgens de voorwaarden bepaald in de wet en in het voorliggend besluit. Hierbij moet er rekening worden gehouden met de richtlijn van de Nationale Veiligheidsraad die de omvang van het veiligheidsonderzoek bepaalt, zoals vermeld in artikel 18, vijfde lid van de wet. Deze richtlijn wordt overeenkomstig artikel 18, zesde lid van de wet enkel meegedeeld aan de aangeen en leden van de inlichtingen- en veiligheidsdiensten, aan de veiligheidsoverheid, alsook aan het Vast Comité I.

Paragraaf 2 geeft aan dat personen met een buitenlandse nationaliteit (met inbegrip van onderdanen van een niet-EU land) eveneens een veiligheidsmachtiging kunnen verkrijgen op voorwaarde zij onderdaan zijn van een land waarmee België een overeenkomst inzake de uitwisseling en de wederzijdse bescherming van geclassificeerde informatie heeft afgesloten. Dit houdt tevens in dat er een onderzoek mogelijk moet zijn door de bevoegde Belgische inlichtingen- en veiligheidsdienst volgens voormelde richtlijn van de Nationale Veiligheidsraad. De buitenlandse veiligheidsmachtiging kan ook worden erkend door de bevoegde autoriteiten.

Paragraaf 3 bepaalt dat dergelijke overeenkomst inzake de uitwisseling en de wederzijdse bescherming van geclassificeerde informatie niet vereist is voor onderdanen van een lidstaat van de Europese Economische Ruimte of de Zwitserse Bondsstaat. Voor landen buiten de Europese Economische Ruimte of de Zwitserse Bondsstaat wordt dergelijke overeenkomst wel vereist, zodat er een objectief, juridisch kader aanwezig is voor de bilaterale uitwisseling en de wederzijdse bescherming van geclassificeerde informatie en er zicht is op de inhoud van de bijstand die in voorkomend geval door het desbetreffende vreemde land wordt gegeven.

Par conséquent, le paragraphe 3 est une exception au paragraphe 2 et a été adapté à la suite de la remarque formulée par le Conseil d'État à ce sujet.

Par ailleurs, les auteurs du projet ne sont pas d'accord avec la remarque formulée par le Comité permanent R (point 6) selon laquelle, sauf accord de sécurité, la possibilité d'être titulaire d'une habilitation de sécurité belge en vertu de la loi relative à la classification est réservée aux seules personnes de nationalité belge. Ni la loi relative à la classification ni l'arrêté royal du 24 mars 2000 ne limitent la possibilité d'octroyer une habilitation de sécurité belge aux personnes de nationalité belge (le Comité R ne l'explique pas non plus dans son avis). L'article 1bis, 10°, a), de la loi cite les habilitations de sécurité accordées à des « personnes physiques », sans les limiter aux personnes physiques belges. Cela n'exclut évidemment pas la possibilité laissée à « l'autorité d'origine » de restreindre l'accès aux seules personnes titulaires de la nationalité belge, pour des raisons légitimes liées à la protection des informations, mais il s'agit là d'une décision de « l'autorité d'origine » concernée et non de l'Autorité nationale de Sécurité. L'existence d'un accord en matière d'échange et de protection mutuelle des informations classifiées n'est pas non plus une condition nécessaire pour délivrer une habilitation de sécurité à un ressortissant étranger, conformément à la loi relative à la classification. Cet accord est toutefois nécessaire pour fournir une assistance lors d'une enquête de sécurité visant à octroyer une habilitation de sécurité à un résident d'un État étranger, par les autorités compétentes de cet État (article 19, dernier alinéa de la loi). Un tel accord n'est pas nécessaire pour demander l'assistance d'un État étranger dans le cadre d'une enquête de sécurité (article 18, alinéa 2, de la loi).

Sous-section 2. — Procédure de demande

Articles 71 à 73

Ces articles traitent de la procédure à suivre pour introduire une demande d'habilitation de sécurité.

Il est d'abord stipulé qu'une demande doit être dûment motivée. En d'autres termes, la demande doit préciser concrètement les raisons pour lesquelles la personne concernée a besoin d'une habilitation de sécurité et les informations classifiées auxquelles elle doit avoir accès. Ces informations permettent à l'Autorité nationale de Sécurité d'évaluer la recevabilité de la demande. Dans son avis, le Conseil d'État a noté que le mot « précisément » devait être omis, dans la mesure où sa portée ne pouvait être précisée. Le mot « précisément » est tiré de l'article 24, § 1^{er}, de l'arrêté royal du 24 mars 2000. Les auteurs du présent projet préfèrent remplacer le mot « précisément » par « dûment » afin d'éviter l'introduction de demandes d'habilitation de sécurité sans aucune raison ou pour des raisons très vagues.

L'article énumère ensuite les personnes qui signent et introduisent la demande d'habilitation de sécurité par l'intermédiaire de l'officier de sécurité. Cette disposition a été largement reprise de l'arrêté royal du 24 mars 2000, avec quelques modifications. Ainsi, le paragraphe 4 est abrogé. Historiquement, cette disposition spécifique pour les membres du personnel de la police intégrée reposait sur le constat que les fonctionnaires de police ne devaient pas avoir connaissance d'informations classifiées, étant donné que la procédure stricte de gestion et de traitement des « informations classifiées » entravait la diffusion et l'utilisation de ces informations dans le cadre de leurs missions.

À l'heure actuelle, les échanges d'informations classifiées entre les services de police et les services de renseignement et de sécurité, mais aussi avec d'autres services partenaires, augmentent de manière significative, notamment dans le cadre de dossiers judiciaires relevant de leur compétence. Par ailleurs, le fait d'obliger la police intégrée à établir une liste des fonctions nécessitant une habilitation de sécurité, liste que le Conseil national de sécurité doit valider, n'offre pas la souplesse nécessaire pour répondre aux évolutions de la structure de la police (changement des noms de services, nouvelles directions, nouvelles missions, etc.), à sa complexité, et aux évolutions auxquelles les services de police sont confrontés.

Il convient donc de supprimer ce régime particulier uniquement applicable à la police intégrée et d'appliquer le régime général des paragraphes 1 à 3, en vertu duquel un supérieur hiérarchique déterminé valide et signe la demande d'habilitation de sécurité. Ce supérieur se doit de vérifier le besoin d'en connaître de la personne qui

Paragraaf 3 vormt bijgevolg een uitzondering op paragraaf 2 en werd aangepast ten gevolge van de opmerking van de Raad van State in dit verband.

De opstellers van het ontwerp zijn het overigens niet eens met de opmerking van het Vast Comité I (randnummer 6) dat, behoudens een veiligheidsakkoord, de mogelijkheid om te beschikken over een Belgische veiligheidsmachtiging ingevolge de Classificatiewet enkel voorbehouden is aan personen die over de Belgische nationaliteit beschikken. De Classificatiewet noch het koninklijk besluit van 24 maart 2000 beperken de mogelijkheid tot het toekennen van een Belgische veiligheidsmachtiging aan personen die over de Belgische nationaliteit beschikken (het Comité I legt dit ook niet uit in haar advies). Artikel 1bis, 10°, a) van de wet heeft het over veiligheidsmachtigingen toegekend aan “natuurlijke personen”, zonder dat dit beperkt wordt tot Belgische natuurlijke personen. Dit sluit uiteraard niet uit dat de “overheid van oorsprong” omwille van geconcreteerde redenen die met de bescherming van de informatie te maken hebben de toegang wel kan beperken tot personen die over de Belgische nationaliteit beschikken, maar dat vormt een beslissing van de desbetreffende “overheid van oorsprong” en niet van de Nationale Veiligheidszorg. Ook het bestaan van een overeenkomst inzake de uitwisseling en de wederzijdse bescherming van geclassificeerde informatie vormt volgens de Classificatiewet geen noodzakelijke voorwaarde voor het afleveren van een veiligheidsmachtiging aan een buitenlandse onderdaan. Deze overeenkomst is wel noodzakelijk voor het leveren van bijstand aan een veiligheidsonderzoek dat tot doel heeft het verlenen van een veiligheidsmachtiging aan een ingezetene van een vreemde Staat, door de bevoegde overheden van die Staat (artikel 19, laatste lid van de wet). Voor het vragen van bijstand aan een vreemde Staat in het kader van een veiligheidsonderzoek (artikel 18, tweede lid van de wet) is dergelijke overeenkomst niet vereist.

Onderafdeling 2. — Aanvraagprocedure

Artikelen 71 tot en met 73

Deze artikelen gaan over de procedure die moet gevolgd worden voor het indienen van een aanvraag voor een veiligheidsmachtiging.

In de eerste plaats wordt er bepaald dat een aanvraag met redenen gemotiveerd moet zijn. Dit wil zeggen dat de aanvraag concreet moet preciseren om welke redenen de desbetreffende persoon een veiligheidsmachtiging behoeft en voor welke geclassificeerde informatie de desbetreffende betrokkene de toegang behoeft. Dit laat de Nationale Veiligheidszorg toe om de ontvankelijkheid van de aanvraag te evalueren. De Raad van State merkte in haar advies op dat het woord “nauwkeurig” moet weggelaten worden, aangezien de strekking ervan niet verduidelijkt kan worden. Het woord “nauwkeurig” werd overgenomen van het artikel 24, § 1 van het koninklijk besluit van 24 maart 2000. De opstellers van voorliggend ontwerp geven er de voorkeur aan om het woord “nauwkeurig” te vervangen door “met redenen” om te vermijden dat aanvragen voor veiligheidsmachtigingen zonder enige of erg vage redenen worden ingediend.

Vervolgens worden de personen opgesomd die de aanvraag voor de veiligheidsmachtiging ondertekenen en indienen via de veiligheidsfunctionarissen. Deze bepaling werd grotendeels overgenomen van het koninklijk besluit van 24 maart 2000 met enige wijzigingen. Zo wordt paragraaf 4 opgeheven. Historisch gezien berustte deze specifieke bepaling voor de leden van de geïntegreerde politie op de vaststelling dat politieambtenaren geen kennis moesten hebben van geclassificeerde informatie, aangezien de strikte procedure voor het beheer en de verwerking van ‘geclassificeerde informatie’ de verspreiding en het gebruik van die informatie in het raam van hun opdrachten belemmerde.

Momenteel is er een sterke toename van uitgewisselde geclassificeerde informatie tussen de politiediensten en de inlichtingen- en veiligheidsdiensten alsook met andere partnerdiensten, in het bijzonder in het raam van gerechtelijke dossiers die onder hun bevoegdheid vallen. Daarnaast biedt het verplichten van de geïntegreerde politie om een lijst op te stellen van de functies waarvoor een veiligheidsmachtiging vereist is - een lijst die de Nationale Veiligheidsraad moet valideren - niet de nodige flexibiliteit om in te spelen op veranderingen van de politiestructuur (wijziging van namen van diensten, nieuwe directies, nieuwe opdrachten enz.) alsook op haar complexiteit en de veranderende realiteit waarmee de politiediensten te maken krijgen.

Deze bijzondere regeling die enkel van toepassing is op de geïntegreerde politie moet daarom worden afgeschaft, zodat de algemene regeling uit de paragrafen 1 tot 3 van toepassing kan worden, met name dat een hiërarchische overste de aanvraag voor een veiligheidsmachtiging geldig verklaart en ondertekent. Deze overste moet de noodzaak

demande cette habilitation de sécurité, ce qui permettra aussi de limiter les demandes d'habilitation qui seraient uniquement fondées sur l'appartenance à un service.

Les demandes d'habilitation de sécurité introduites par des indépendants ayant ou non la personnalité juridique (respectivement la société unipersonnelle et l'entreprise unipersonnelle) peuvent être signées par le donneur d'ordre, à savoir le fonctionnaire dirigeant d'une administration publique, d'un organisme d'intérêt public ou d'une entreprise publique autonome pour laquelle l'indépendant travaille exclusivement, ou la ou les personnes qui assure(nt) la gestion de la personne morale dûment habilitée pour laquelle l'indépendant travaille exclusivement, sans qu'il soit question d'exercer une autorité d'employeur sur ces personnes. Ces indépendants peuvent également choisir d'introduire (et de financer) eux-mêmes la demande d'habilitation de sécurité. Cette disposition vise à éviter que les entreprises individuelles ou les sociétés unipersonnelles qui travaillent exclusivement pour un seul donneur d'ordre doivent demander et payer des habilitations de sécurité pour des personnes morales et, par conséquent, à simplifier et rendre plus efficace l'attribution des contrats. Le donneur d'ordre parraine et aide l'indépendant à demander une habilitation de sécurité, étant donné que l'indépendant travaille exclusivement pour ce donneur d'ordre. En d'autres termes, le donneur d'ordre collecte les données nécessaires auprès de l'indépendant pour pouvoir soumettre cette demande et aide l'indépendant à respecter ses obligations contractuelles. Par conséquent, ce parrainage entraîne une responsabilité accrue pour le donneur d'ordre : d'une part, au niveau de la collecte de données (fiables) auprès de l'indépendant et, d'autre part, au niveau du suivi et de la prévention des incidents de sécurité dans le chef de l'indépendant. Pour cette raison, il est explicitement prévu qu'il doit s'agir d'indépendants travaillant au lieu du siège d'exploitation ou du siège réel du donneur d'ordre (le siège d'exploitation peut être le siège social, mais le siège social n'est pas nécessairement le siège d'exploitation). Il est recommandé que le donneur d'ordre n'utilise cette disposition que si peu de sous-traitants travaillent pour l'entité, afin de permettre un suivi efficace. Des informations classifiées ne peuvent en aucun cas être utilisées au siège ou à l'adresse où l'indépendant est établi. Cette disposition est également mentionnée dans le contrat conclu avec l'indépendant. En cas de recours à ce « parrainage », le donneur d'ordre, et plus particulièrement l'officier de sécurité du donneur d'ordre, est responsable de l'indépendant en ce qui concerne les briefings de sécurité, le suivi des incidents de sécurité, la demande de renouvellement des habilitations de sécurité, le débriefing de sécurité..., de la même manière que pour les membres du personnel régulier du donneur d'ordre.

Si l'indépendant avec ou sans personnalité juridique travaille pour plusieurs donneurs d'ordre dans le cadre de marchés publics classifiés, il est tenu de suivre la procédure décrite au chapitre 5, section 2 (habilitation de sécurité pour les personnes morales) et de signer lui-même l'habilitation de sécurité, le cas échéant, comme prévu à l'alinéa 7 du paragraphe 2.

En réponse à une observation formulée par le Comité permanent R, il a été examiné à chaque fois si l'ajout « ou les autorités de sécurité visées à l'article 1quinquies de la loi » était indiqué.

Sous-section 3. — Appréciation de la recevabilité de la demande

Article 74

L'article 74 a été adapté à la suite d'une observation du Comité permanent R dans le sens où une demande peut être irrecevable non seulement parce que certaines formalités n'ont pas été respectées, mais également parce que les motifs de la demande ne sont pas corrects ou convaincants (par exemple une demande émanant d'une personne morale qui ne doit pas utiliser des informations classifiées).

En outre, il est précisé que cet article ne prévoit pas de délai spécifique pour le contrôle de la demande par l'Autorité nationale de Sécurité. Le texte utilise les termes « sans délai », soit le plus rapidement possible. La décision est prise en même temps que l'envoi du dossier aux services de renseignement et de sécurité (la facture pour le paiement de la rétribution est également envoyée automatiquement). Dans la pratique, la procédure est assez rapide étant donné qu'elle s'effectue généralement par voie numérique (plateforme HABIL+). Cependant, la possibilité demeure de passer par une procédure manuelle, par exemple en cas de panne de la plateforme HABIL+.

tot kennisname controleren van de persoon die deze veiligheidsmachtiging vraagt, waardoor de aanvragen voor machtigingen die enkel gestoeld zijn op het feit dat men deel uitmaakt van een dienst, ook beperkt zullen worden.

Aanvragen voor veiligheidsmachtigingen van zelfstandigen met of zonder rechtspersoonlijkheid (respectievelijk de éénpersoonsvennootschap en de éénmanszaak) kunnen worden ondertekend door de opdrachtgever, zijnde hetzij de leidend ambtenaar van een openbaar bestuur, instelling van openbaar nut of autonoom overheidsbedrijf waar de zelfstandige exclusief werkzaam voor is, hetzij de persoon of de personen die het bestuur van de naar behoren gemachtigde rechtspersoon verzekeren waar de zelfstandige exclusief werkzaam voor is en dit zonder dat er sprake van kan zijn dat er een werkgeversgezag wordt uitgeoefend over deze personen. Deze zelfstandigen kunnen er ook voor opteren om de aanvraag voor de veiligheidsmachtiging zelf in te dienen (en te financieren). Deze bepaling heeft als doel te vermijden dat de eenmanszaak of de éénpersoonsvennootschap, die exclusief werkzaam is voor één opdrachtgever, een veiligheidsmachtiging voor rechtspersonen moet aanvragen en bekosten en heeft bijgevolg een eenvoudiger en efficiëntere manier in het toekennen van contracten op het oog. De opdrachtgever sponsort en staat de zelfstandige bij in het aanvragen van een veiligheidsmachtiging, gezien deze zelfstandige exclusief voor die opdrachtgever werkzaam is. Dit houdt in dat de opdrachtgever de nodige gegevens verzamelt bij deze zelfstandige om deze aanvraag te kunnen indienen en de zelfstandige ondersteunt om aan zijn contractuele verplichtingen te voldoen. Deze sponsoring houdt bijgevolg een verhoogde verantwoordelijkheid in voor de opdrachtgever: enerzijds in het verzamelen van (betrouwbare) gegevens bij deze zelfstandige en anderzijds in het opvolgen en voorkomen van veiligheidsincidenten in hoofde van deze zelfstandige. Om deze reden wordt er uitdrukkelijk bepaald dat het moet gaan om zelfstandigen die op de plaats van de uitbatingsetel of werkelijke zetel (de uitbatingsetel kan de statutaire zetel zijn, maar de statutaire zetel is niet noodzakelijk de uitbatingsetel) van de opdrachtgever werkzaam zijn. Het is aangewezen dat de opdrachtgever enkel gebruikt maakt van deze bepaling indien er slechts een klein aantal onderaannemers voor de entiteit werkzaam zijn, zodat een efficiënte opvolging mogelijk blijft. In geen enkel geval kan er geëvalueerde informatie worden aangewend op de zetel of het adres waar de zelfstandige is gevestigd. Dit wordt ook vermeld in het contract met de zelfstandige. De opdrachtgever, en meer bepaald de veiligheidsofficier van de opdrachtgever, wordt -in het geval dat van deze "sponsoring" wordt gebruik gemaakt- verantwoordelijk voor deze zelfstandige op het vlak van veiligheidsbriefings, opvolgen van veiligheidsincidenten, aanvraag hernieuwen van veiligheidsmachtigingen, veiligheidsdebriefing, ... net zoals dit het geval is voor de gewone personeelsleden van de opdrachtgever.

Indien deze zelfstandige zonder of met rechtspersoonlijkheid werkzaam is voor meerdere opdrachtgevers in het kader van geëvalueerde overheidsopdrachten, dan dient deze de procedure zoals beschreven in hoofdstuk 5, afdeling 2 (de veiligheidsmachtiging voor rechtspersonen) alsnog te volgen en in voorkomend geval de veiligheidsmachtiging zelf te ondertekenen zoals bepaald in het zevende lid van paragraaf 2.

Naar aanleiding van een opmerking van het Vast Comité I werd er telkens nagegaan of het aangewezen is om "of de in artikel 1quinquies van de wet bedoelde veiligheidsoverheden" toe te voegen.

Onderafdeling 3. — Beoordeling van de ontvankelijkheid van de aanvraag

Artikel 74

Artikel 74 werd aangepast ten gevolge van een opmerking van het Vast Comité I in die zin dat een aanvraag niet alleen onontvankelijk kan zijn omdat bepaalde formaliteiten niet vervuld zijn maar ook omdat de motieven in de aanvraag niet correct of overtuigend zijn (bijv. een aanvraag door een rechtspersoon die geen geëvalueerde informatie moet aanwenden).

Daarnaast wordt verduidelijkt dat in dit artikel niet werd voorzien in een specifieke termijn voor de controle van de aanvraag door de Nationale Veiligheidsoverheid. De tekst spreekt van 'onverwijld', dit wil zeggen zo snel mogelijk. De beslissing gebeurt gelijktijdig met de verzending van het dossier naar de inlichtingen- en veiligheidsdiensten (de factuur voor de betaling van de retributie wordt dan ook automatisch verzonden). In de praktijk verloopt dit vrij snel, gezien dit normaliter digitaal gebeurt (via het platform HABIL+). De mogelijkheid wordt echter behouden om, bijvoorbeeld bij een panne van HABIL+, de verzending manueel te laten verlopen.

Article 75

L'article 75 n'appelle aucun commentaire.

Sous-section 4. — Enquête de sécurité

La sous-section 4 décrit l'enquête de sécurité.

Article 76

L'article 76 fixe les délais dans lesquels les services de renseignement et de sécurité doivent clôturer l'enquête de sécurité.

Il est précisé que la procédure de demande prévoit que l'officier de sécurité dispose de 15 jours pour transmettre les documents à l'ANS. L'ANS dispose d'environ un mois (« immédiatement ») pour les transmettre aux services de renseignement et de sécurité. Les services de renseignement et de sécurité disposent de 2, 3 ou 6 mois pour clôturer leur enquête. Dès que l'Autorité nationale de Sécurité reçoit les résultats de l'enquête de sécurité, elle dispose d'un mois pour statuer sur la demande d'habilitation de sécurité et transmettre sa décision à l'officier de sécurité.

L'intéressé devra donc attendre environ 5 mois pour une habilitation de sécurité de niveau « CONFIDENTIEL », 6 mois pour le niveau « SECRET » et 9 mois pour le niveau « TRÈS SECRET ». La note explicative, annexée au présent arrêté, a pour objet d'expliquer à l'intéressé la procédure de demande d'une habilitation de sécurité. Les délais indiqués dans la note explicative visent à informer l'intéressé du délai d'attente global probable.

Articles 77 et 78

Les articles 77 et 78 n'appellent aucun commentaire.

Sous-section 5 — Décision concernant l'habilitation de sécurité

La sous-section 5 concerne la décision relative à l'habilitation de sécurité.

Articles 79 et 80

Les articles 79 et 80 n'appellent aucun commentaire.

Sous-section 6. — Durée de validité de l'habilitation de sécurité

Article 81

La sous-section 6 traite de la durée de validité de l'habilitation de sécurité et contient l'article 81, qui n'appelle pas de commentaire supplémentaire.

Sous-section 7. — Enquête de sécurité complémentaire

Article 82

La sous-section 7 aborde les enquêtes de sécurité complémentaires et contient le seul article 82. Dans son avis, le Comité permanent R s'interroge sur la légalité de l'obligation (par ailleurs vague) de l'employeur de « signaler à l'officier de sécurité tout élément troublant dans le comportement de la personne concernée qui est inconciliable avec les garanties de discrétion, de loyauté et d'intégrité ». Vu l'article 22 de la Constitution, le Comité permanent R estime qu'il appartient au législateur de déterminer les informations sur la base desquelles une enquête de sécurité peut être menée (comme régi par la loi pour l'officier de sécurité, par exemple).

Les auteurs soulignent qu'il n'est pas demandé à l'employeur de mener une enquête de sécurité, mais tout au plus d'être attentif aux signaux graves indiquant que la personne concernée pourrait ne plus répondre aux conditions requises pour traiter des informations classifiées et les transmettre à l'officier de sécurité.

Section 2. — Habilitation de sécurité pour les personnes morales

Sous-section 1. — Généralités

Article 83

L'article 83 du projet d'arrêté royal prévoit que « toute personne morale peut être autorisée à accéder à des informations classifiées pour autant que le besoin d'en connaître soit reconnu par l'autorité et que cette personne morale dispose d'une habilitation de sécurité pour les personnes morales ».

L'article 83 a été conçu comme une disposition introductive qui, par analogie avec l'article 8 de la loi, définit les conditions de base auxquelles une personne morale peut accéder à des informations classifiées. Par analogie avec les règles applicables aux personnes physiques, les personnes morales ne peuvent accéder aux informations classifiées que si elles disposent d'une habilitation de sécurité correspondante pour les personnes morales et si elles ont le besoin d'en connaître. Sur avis du Conseil d'Etat (p. 25), il est précisé que, conformément à l'article 8 § 2 de la loi, l'habilitation de sécurité n'est

Artikel 75

Artikel 75 vergt geen commentaar.

Onderafdeling 4. — Het veiligheidsonderzoek

Onderafdeling 4 beschrijft het veiligheidsonderzoek.

Artikel 76

Artikel 76 legt de termijnen vast waarbinnen de inlichtingen- en veiligheidsdienst het veiligheidsonderzoek dient af te werken.

Hierbij wordt verduidelijkt dat de aanvraagprocedure voorziet dat de veiligheidsofficier over 15 dagen beschikt om de documenten aan de NVO over te zenden. De NVO heeft ongeveer een maand ("onverwijld") om deze over te zenden naar de inlichtingen- en veiligheidsdiensten. De inlichtingen- en veiligheidsdiensten beschikken over 2, 3 of 6 maanden om hun onderzoek af te ronden. Zodra de Nationale Veiligheidsoverheid de resultaten van het veiligheidsonderzoek heeft ontvangen, heeft ze één maand de tijd om zich over de aanvraag om een veiligheidsmachtiging uit te spreken en haar beslissing aan de veiligheidsofficier over te zenden.

De betrokkene zal dus ongeveer 5 maanden moeten wachten voor een veiligheidsmachtiging van het niveau "VERTROUWELIJK", 6 maanden voor het niveau "GEHEIM" en 9 maanden voor het niveau "ZEER GEHEIM". Het doel van de verklarende nota, die in bijlage aan dit besluit werd toegevoegd, is aan de betrokkene uitleg te geven over de aanvraagprocedure inzake de veiligheidsmachtigingen. De termijnen in de verklarende nota willen betrokkene informeren over de totale vermoedelijke wachttijd.

Artikelen 77 en 78

Artikelen 77 en 78 vergen geen commentaar.

Onderafdeling 5. — De beslissing betreffende de veiligheidsmachtiging

Onderafdeling 5 bevat de beslissing betreffende de veiligheidsmachtiging.

Artikelen 79 en 80

Artikelen 79 en 80 vergen geen commentaar.

Onderafdeling 6. — Geldigheidsduur van de veiligheidsmachtiging

Artikel 81

Onderafdeling 6 behandelt de geldigheidsduur van de veiligheidsmachtiging en bevat het artikel 81 dat geen verdere toelichting vereist.

Onderafdeling 7. — Tussentijds veiligheidsonderzoek

Artikel 82

Onderafdeling 7 betreft de tussentijdse veiligheidsonderzoeken en bevat het enige artikel 82. Het Vast Comité I stelt zich in haar advies vragen bij de wettigheid van de (overigens vage) verplichting van de werkgever om 'aan de veiligheidsofficier elk verontrustend element (te) signaleren betreffende het gedrag van de betrokkene dat onverzoenbaar is met de garanties inzake geheimhouding, loyauteit en integriteit'. Gelet op artikel 22 van de Grondwet komt het volgens het Vast Comité I aan de wetgever toe om te bepalen op basis van welke informatie een veiligheidsonderzoek kan gevoerd worden (zoals dat bijvoorbeeld wettelijk geregeld is voor de veiligheidsofficier).

De opstellers wijzen erop dat aan de werkgever niet wordt gevraagd om een veiligheidsonderzoek te voeren, maar hooguit om aandachtig te zijn voor ernstige signalen die erop wijzen dat de betrokkene mogelijk niet meer voldoet aan de voorwaarden om met geclassificeerde informatie om te gaan en deze door te geven aan de veiligheidsofficier.

Afdeling 2. — De veiligheidsmachtiging voor rechtspersonen

Onderafdeling 1. — Algemeen

Artikel 83

Artikel 83 van het ontwerp koninklijk besluit bepaalde "Iedere rechtspersoon kan toegang krijgen tot geclassificeerde informatie, indien de noodzaak tot kennisname wordt erkend door de overheid en deze rechtspersoon beschikt over een veiligheidsmachtiging voor rechtspersonen".

Artikel 83 is opgevat als een inleidende bepaling die naar analogie van artikel 8 van de wet de basisvoorwaarden uiteenzet op grond waarvan een rechtspersoon toegang kan verkrijgen tot geclassificeerde informatie. Analoot aan de regels voor fysieke personen, kunnen rechtspersonen enkel toegang krijgen tot geclassificeerde informatie indien deze beschikken over een overeenstemmende veiligheidsmachtiging voor rechtspersonen en over de nodige noodzaak tot kennisname beschikken. Op advies van de Raad van State (p. 54) wordt er gepreciseerd dat er in overeenstemming met artikel 8, § 2 van de wet

pas requise pour les informations classifiées de niveau « RESTREINT ». Les personnes physiques sont soumises à l'exigence supplémentaire de recevoir un briefing de sécurité. Étant donné qu'une personne morale ne peut pas recevoir de briefing, cette troisième condition n'a pas été retenue pour les personnes morales.

Le Comité permanent R a indiqué dans son avis (p. 5, § 9) qu'il n'était pas possible de déterminer si le terme « autorité » se référait au pouvoir adjudicateur ou à l'autorité de sécurité. Afin de préciser qu'il s'agit ici de l'autorité de sécurité, le texte du projet d'arrêté royal a été adapté en conséquence.

En outre, le Conseil d'État a indiqué dans son avis qu'une exception devrait être prévue pour le niveau RESTREINT (p. 25). Il convient ici de se référer au commentaire relatif à l'article 84, alinéa 2, du présent arrêté.

Article 84

L'article 84, alinéa 1^{er}, du projet d'arrêté royal prévoit que seules les personnes morales ayant leur siège en Belgique peuvent obtenir une habilitation de sécurité.

Les auteurs du projet d'arrêté estiment que l'exigence d'avoir le siège social en Belgique pour être éligible aux marchés publics classifiés ne s'oppose pas à la libre circulation des services car elle se justifie pour des raisons d'intérêt public, à savoir la sécurité nationale, et du fait que la mesure est proportionnée à l'objectif poursuivi.

En l'occurrence, il ne s'agit pas d'une exigence de nationalité. Les personnes morales étrangères peuvent également soumissionner à de tels marchés si elles ont leur siège social ou une unité d'établissement en Belgique. Les personnes morales titulaires d'une habilitation de sécurité étrangère reconnue par l'Autorité nationale de Sécurité en application d'un accord international peuvent également soumissionner à ces marchés.

Dans son avis (p. 8), le Conseil d'État considère que la possibilité de faire valoir une habilitation de sécurité délivrée à l'étranger ne s'applique qu'aux marchés publics dans le domaine de la défense et de la sécurité, et donc pas dans les domaines relevant en principe de la loi du 17 juin 2016.

Cela aurait pour conséquence que les personnes morales n'ayant pas de siège social en Belgique, mais qui satisfont à toutes les exigences de sécurité sur la base d'une attestation délivrée par une autorité étrangère et reconnue par l'Autorité nationale de Sécurité en vertu d'un accord international, ne pourraient pas soumissionner à des marchés publics. Le Conseil d'État estime que cette exclusion n'est pas proportionnée.

La loi du 13 août 2011 relative aux marchés publics dans les domaines de la défense et de la sécurité restera d'application lorsque l'utilisation d'informations classifiées s'avère nécessaire. Cela découle de la définition des équipements sensibles. Les équipements sensibles sont définis comme les « équipements, travaux et services destinés à des fins de sécurité qui font intervenir, nécessitent et/ou comportent des informations classifiées » (art. 3, 17°, de la loi précitée).

La situation décrite par le Conseil d'État ne peut pas se produire dans la réalité car les entreprises n'invoqueront les habilitations de sécurité étrangères que lorsqu'il s'agit d'informations classifiées et, par définition, la loi du 13 août 2011 est dès lors d'application.

Sur la base de ce qui précède, les auteurs estiment que la disposition du projet d'arrêté royal est conforme au droit européen.

À la demande du Comité permanent R (point 10 de l'avis), la possibilité de déroger à l'exigence de nationalité par un traité ou un accord de sécurité a été explicitement prévue dans un souci de clarté. Cette disposition est prévue à l'alinéa 2 du présent arrêté.

L'article 84, alinéa 3, du projet d'arrêté prévoit qu'en ce qui concerne les marchés publics impliquant des informations classifiées, l'administrateur ICT doit être titulaire d'une habilitation de sécurité du niveau fixé conformément à la politique de sécurité de l'Autorité nationale de Sécurité.

Le Conseil d'État (p. 25) et le Comité R (p. 6) ont noté dans leur avis que cette disposition serait incompatible avec l'art. 8, § 2, de la loi, qui dispose qu'une personne ne doit pas être titulaire d'une habilitation de sécurité pour accéder à des informations classifiées de niveau « RESTREINT » et, par conséquent, que cette disposition devait être révisée.

geen veiligheidsmachtiging nodig is voor geclassificeerde informatie van het niveau "BEPERKT". Voor fysieke personen geldt nog de bijkomende vereiste van het ontvangen van een veiligheidsbriefing. Aangezien een rechtspersoon geen briefing kan ontvangen werd deze derde voorwaarde niet weerhouden voor rechtspersonen.

Het Vast Comité I stelde in haar advies (op p. 5 § 9) dat het onduidelijk was of de term overheid verwees naar de aanbestedende overheid of naar de veiligheids-overheid. Om duidelijk te maken dat het hier gaat over de veiligheids-overheid werd de tekst van het ontwerp koninklijk besluit overeenkomstig aangepast.

Verder stelde de Raad van State in haar advies dat er een uitzondering zou voorzien moeten worden voor het niveau BEPERKT (p. 54). Hier kan verwezen worden naar de commentaar bij artikel 84 tweede lid van dit besluit.

Artikel 84

Het eerste lid van artikel 84 van het ontwerp koninklijk besluit stelt dat enkel rechtspersonen waarvan de statutaire zetel in België gevestigd is een veiligheidsmachtiging zouden kunnen verkrijgen.

De opstellers van het ontwerpbesluit menen dat de vereiste van het vestigen van de statutaire zetel in België om in aanmerking te kunnen komen voor geclassificeerde overheidsopdrachten niet strijdig is met het vrij verkeer van diensten omdat het gerechtvaardigd is om redenen van algemeen belang, met name de nationale veiligheid, en omdat de maatregel proportioneel is aan het nagestreefde doel.

Het betreft hier geen nationaliteitsvereiste. Buitenlandse rechtspersonen kunnen zich immers ook inschrijven op dergelijke opdrachten als ze in België hun statutaire zetel of een vestigingseenheid hebben. Ook rechtspersonen die beschikken over een met toepassing van een internationale overeenkomst door de Nationale Veiligheids-overheid erkende buitenlandse veiligheidsmachtiging kunnen zich inschrijven op dergelijke opdrachten.

De Raad van State meent in haar advies (op. 36) dat de mogelijkheid om zich te beroepen op een in het buitenland afgegeven veiligheidsmachtiging enkel geldt voor overheidsopdrachten in het domein van defensie en veiligheid en dus niet in de domeinen waarvoor in principe de wet van 17 juni 2016 van toepassing is.

Dit zou tot gevolg hebben dat rechtspersonen die geen statutaire zetel hebben in België maar wel beantwoorden aan alle veiligheidsvereisten op grond van een attest afgegeven door een buitenlandse overheid en erkend door de Nationale Veiligheids-overheid krachtens een internationale overeenkomst niet kunnen inschrijven op overheidsopdrachten. Dergelijke uitsluiting is volgens de Raad van State niet evenredig.

De wet van 13 augustus 2011 inzake de overheidsopdrachten op defensie- en veiligheidsgebied zal steeds van toepassing zijn wanneer de Anwendung van geclassificeerde informatie vereist is. Dit volgt uit de definitie van gevoelig materiaal. Gevoelig materiaal wordt omschreven als "materiaal, werken en diensten voor veiligheidsdoeleinden die betrekking hebben op geclassificeerde informatie of die geclassificeerde informatie noodzakelijk maken en/of bevatten" (art. 3, 17° voormelde wet).

De situatie zoals beschreven door de Raad van State kan zich in de realiteit niet voordoen daar ondernemingen zich enkel zullen beroepen op buitenlandse veiligheidsmachtigingen wanneer er geclassificeerde informatie aangewend wordt en dus per definitie de wet van 13 augustus 2011 van toepassing is.

Op grond van het voorgaande menen de opstellers dat de bepaling in het ontwerp koninklijk besluit in overeenstemming is met het Europees Recht.

Op vraag van het Vast Comité I (punt 10 van het advies) werd uitdrukkelijk en voor de duidelijkheid de mogelijkheid voorzien om af te wijken van de nationaliteitsvereiste bij verdrag of veiligheidsakkoord. Dit is voorzien in het tweede lid van voorliggend besluit.

Het derde lid van artikel 84 van het ontwerp besluit stelt dat voor wat betreft overheidsopdrachten die betrekking hebben op geclassificeerde informatie de ICT-beheerder in het bezit moet zijn van een veiligheidsmachtiging waarvan het niveau wordt bepaald overeenkomstig het veiligheidsbeleid van de Nationale Veiligheids-overheid.

Zowel de Raad van State (p. 54) als het Comité I (p. 6) merkten op in hun advies dat deze bepaling niet in overeenstemming zou zijn met art. 8, § 2 van de wet dat stelt dat een persoon geen houder dient te zijn van een veiligheidsmachtiging om toegang te hebben tot geclassificeerde informatie van het niveau "BEPERKT" en bijgevolg deze bepaling diende te worden herzien.

Pour ce qui concerne les marchés publics qui impliquent, nécessitent et/ou contiennent des informations classifiées de niveau « RESTREINT », l'Autorité nationale de Sécurité détermine la nécessité d'une habilitation de sécurité pour l'administrateur ICT et, le cas échéant, son niveau. Ainsi, une habilitation de sécurité peut être considérée comme nécessaire pour le niveau « RESTREINT » pour un administrateur ICT.

Les auteurs du projet d'arrêté royal sont d'avis que cette disposition est bel et bien conforme à l'article 8 de la loi. Les règles selon lesquelles une personne n'a pas besoin d'une habilitation de sécurité ne s'appliquent qu'à l'accès aux informations classifiées stricto sensu, c'est-à-dire au contenu d'un document. Il ne s'agit pas de l'accès privilégié au système de communication et d'information dans lequel les informations classifiées sont utilisées. Il s'agit ici de la protection de l'ICT.

L'obligation éventuelle imposée à l'administrateur ICT d'être titulaire d'une habilitation de sécurité supérieure au niveau de classification dans lequel l'ICT est utilisé découle des réglementations de l'UE et de l'OTAN. Si l'OTAN ou l'UE lançaient une adjudication publique du niveau « UE/OTAN RESTREINT », l'UE et l'OTAN prévoieraient des règles stipulant que l'administrateur ICT doit être titulaire d'une habilitation de sécurité supérieure au niveau « UE/OTAN RESTREINT », c'est-à-dire EU ou OTAN « CONFIDENTIEL ». L'équivalent au niveau « UE/OTAN CONFIDENTIEL » à l'échelle nationale est le niveau « CONFIDENTIEL ». Si cette règle n'est pas respectée, les entreprises ne peuvent pas soumissionner à de tels marchés publics.

Cette mesure trouve son origine dans la distinction entre l'accès à des informations classifiées dont dispose un utilisateur et l'accès privilégié dont dispose un administrateur ICT. L'accès des utilisateurs sera toujours limité sur la base du principe du « besoin d'en connaître ». Par conséquent, un utilisateur n'a pas besoin d'une habilitation de sécurité pour accéder à des documents classifiés du niveau « RESTREINT ».

Toutefois, un administrateur ICT a accès à toutes les informations déployées au sein du réseau, ainsi qu'aux produits cryptographiques. Ses tâches comprennent la gestion (technique), l'exploitation et la configuration de l'environnement ICT. En d'autres termes, il a un accès total et peut avoir un impact sur l'intégrité du système.

En outre, souvent le caractère sensible ou classifié apparaît du fait que différents éléments d'informations sont réunis.

Dès lors, la possession par l'administrateur ICT d'une habilitation de sécurité du niveau fixé par l'ANS est justifiée, y compris en ce qui concerne les marchés publics contenant des informations classifiées de niveau « RESTREINT ».

Le niveau de classification le plus élevé est « TRÈS SECRET ». Par conséquent, le gestionnaire du système ICT devra avoir une habilitation de sécurité « TRÈS SECRET » lorsque la personne morale détient une habilitation de sécurité de niveau « TRÈS SECRET ». Dans ce cas seulement, la personne concernée ne peut pas avoir une habilitation de sécurité plus élevée.

Sous-section 2. — Procédure de demande

Article 85

L'article 85 du projet d'arrêté définit la procédure de demande d'habilitation de sécurité pour les personnes morales.

L'objectif était de créer une procédure qui soit, dans la mesure du possible, similaire à la procédure de demande d'habilitation de sécurité pour les personnes physiques.

L'article 85, § 1^{er}, du projet d'arrêté énumère les éléments à remettre à l'autorité de sécurité compétente. Le dossier d'habilitation comprend notamment le questionnaire de base complété par l'ensemble des personnes physiques appartenant aux organes de la personne morale.

Toutes les personnes physiques appartenant aux organes de la personne morale doivent soumettre une demande d'habilitation, ce qui ne signifie pas que ces personnes doivent toutes faire l'objet d'une enquête de sécurité. Sur la base du questionnaire de base, l'Autorité nationale de Sécurité détermine le nombre de personnes physiques appartenant aux organes de la personne morale devant être titulaires d'une habilitation de sécurité, étant entendu qu'au moins la moitié d'entre elles doivent en disposer.

Suite à l'avis du Comité permanent R (p.6), la disposition selon laquelle l'Autorité nationale de Sécurité détermine quelles personnes physiques appartenant aux organes de la personne morale doivent être titulaires d'une habilitation de sécurité a été supprimée.

Bijgevolg wordt er nu gepreciseerd dat voor wat betreft overheidsoptdrachten die betrekking hebben op geclassificeerde informatie van het niveau "BEPERKT", de Nationale Veiligheidsoverheid de noodzaak van een veiligheidsmachtiging voor de ICT-beheerder en desgevallend het niveau ervan bepaalt. Een veiligheidsmachtiging kan dus wel noodzakelijk geacht worden voor het niveau "BEPERKT" voor een ICT-beheerder.

De opstellers van het ontwerp koninklijk besluit menen dat deze bepaling wel in overeenstemming is met artikel 8 van de wet. De regels dat een persoon geen veiligheidsmachtiging nodig heeft geldt enkel voor de toegang tot geclassificeerde informatie sensu stricto, i.e. de inhoud van een document. Dit gaat niet over de bevoorrechte toegang tot het communicatie en informatiesysteem waarbinnen geclassificeerde informatie aangewend wordt. Hier betreft het de bescherming van de ICT.

De eventuele verplichting dat de ICT beheerder een veiligheidsmachtiging moet hebben die hoger is dan het classificatieniveau waarbinnen de ICT gehanteerd wordt, vloeit voort uit de EU en de NAVO reglementering. Indien de NAVO of de EU een openbare aanbesteding zouden uitschrijven van het niveau EU/NAVO BEPERKT, dan voorzien de EU en NAVO regels dat de ICT beheerder een hogere veiligheidsmachtiging moet hebben dan het niveau EU/NAVO BEPERKT i.e. EU of NAVO VERTROUWELIJK. Het equivalent op nationaal niveau van EU/ NAVO VERTROUWELIJK is "VERTROUWELIJK". Indien niet aan deze regel voldaan is, zullen ondernemingen niet kunnen inschrijven op dergelijke overheidsopdrachten.

Deze maatregel vindt haar oorsprong in het onderscheid tussen de toegang tot geclassificeerde informatie die een gebruiker heeft en de bevoorrechte toegang van een ICT beheerder. De toegang die gebruikers hebben zal steeds beperkt zijn op grond van het beginsel van "need to know". Een gebruiker heeft dan ook geen veiligheidsmachtiging nodig om toegang te hebben tot geclassificeerde documenten van het niveau BEPERKT.

Een ICT beheerder heeft echter toegang tot alle informatie die aangewend wordt binnen het netwerk alsook tot de cryptografische producten. Zijn taken omvatten onder andere het (technische) beheer, de uitbating en de configuratie van de ICT. Hij heeft met andere woorden een volledige toegang en kan de integriteit van het systeem beïnvloeden.

Bovendien is het vaak zo dat het gevoelig of geclassificeerde karakter ontstaat wanneer verschillende stukken informatie samengelegd worden.

Bijgevolg is het bezit van een veiligheidsmachtiging voor, waarvan het niveau wordt bepaald door de NVO, voor de ICT-beheerder gerechtvaardigd, met inbegrip van overheidsopdrachten die geclassificeerde informatie van het niveau "BEPERKT" bevatten.

Het hoogste classificatieniveau is "ZEER GEHEIM". Als gevolg zal de beheerder van het ICT systeem over een veiligheidsmachtiging ZEER GEHEIM moeten beschikken wanneer de rechtspersoon houder is van een veiligheidsmachtiging van het niveau "ZEER GEHEIM". In dit geval kan betrokkene niet beschikken over een hogere veiligheidsmachtiging.

Onderafdeling 2. — Aanvraagprocedure

Artikel 85

Artikel 85 van het ontwerpbesluit beschrijft de aanvraagprocedure voor veiligheidsmachtigingen voor rechtspersonen.

Er werd gestreefd naar een procedure die in de mate van het mogelijke gelijklopend is aan de aanvraagprocedure voor veiligheidsmachtigingen van natuurlijke personen.

Artikel 85, § 1 van het ontwerpbesluit somt de elementen op die overgemaakt moeten worden aan de bevoegde veiligheidsautoriteit. Het habilitatiedossier omvat onder andere de door alle fysieke personen die tot de organen van de rechtspersoon behoren ingevulde basisvragenlijst.

Alle fysieke personen die tot de organen van de rechtspersoon behoren, dienen een aanvraag tot machtiging in te dienen, dit wil niet zeggen dat al deze personen een veiligheidsonderzoek dienen te ondergaan. De Nationale Veiligheidsoverheid bepaalt op grond van de basisvragenlijst hoeveel fysieke personen die tot de organen behoren houder moeten zijn van een veiligheidsmachtiging, waarbij minstens de helft er één moet bezitten.

Ten gevolge van het advies van het Comité I (p. 6) werd de bepaling geschrapt die stelde dat de Nationale Veiligheidsoverheid bepaalt welke fysieke personen die tot de organen van de rechtspersoon behoren over een veiligheidsmachtiging dienen te beschikken.

Pour les informations classifiées de l'UE ou de l'OTAN, l'exigence de nationalité belge pour l'un des membres de l'organe d'administration n'est pas imposée. Pour ce faire, il suffit d'être ressortissant d'un Etat membre de l'une de ces organisations vu qu'en l'occurrence, il s'agit – logiquement – de la protection de la « sécurité nationale » de l'UE ou de l'OTAN. Il serait disproportionné d'exiger qu'au moins un des membres de l'organe d'administration possède également la nationalité belge.

Cette disposition garantit que la procédure de demande d'habilitation de sécurité pour les personnes morales ne soit pas bloquée inutilement par l'exigence de nationalité belge pour l'un des membres de l'organe d'administration et que les informations classifiées bénéficient toujours de la protection nécessaire.

L'article 85, § 3, de l'arrêté prévoit que la personne chargée de la gestion journalière de la personne morale doit résider et être domiciliée en Belgique. En outre, cette personne doit pouvoir se soumettre à une enquête de sécurité menée par l'un des services de renseignement et de sécurité, conformément à la loi, au présent arrêté et à la directive du Conseil national de Sécurité, comme prévu à l'article 18, alinéa 5, de la loi.

Dans son rapport, le Comité R estime que cette disposition ajoute une condition à la loi et qu'elle devrait donc être supprimée (p. 7). Les auteurs du projet d'arrêté estiment en revanche qu'il ne s'agit pas d'une condition supplémentaire.

La loi dispose qu'une habilitation de sécurité ne peut être délivrée qu'après réalisation d'une enquête de sécurité (articles 16 et suivants de la loi). L'enquête doit être menée conformément aux règles énoncées dans la loi relative à la classification. Si l'enquête ne peut être menée conformément à ces règles, l'habilitation de sécurité ne peut être délivrée. Toute autre conclusion serait contra legem et saperait le système de sécurité. De plus, la Belgique est tenue, en vertu d'accords de sécurité, de s'assurer que les personnes titulaires d'une habilitation de sécurité sont correctement habilitées. Si tel n'était pas le cas, la coopération internationale serait mise en péril.

Si une personne ne réside pas en Belgique pendant une certaine période, l'enquête de sécurité ne peut être menée conformément aux règles susmentionnées, faute d'informations suffisantes.

Sous-section 3. — Appréciation de la recevabilité de la demande

Article 86

L'article 86 dispose que l'Autorité nationale de Sécurité vérifie que toutes les données mentionnées à l'article 85, § 1^{er}, ont été envoyées. Le Comité précise que le SGRS et la VSSE doivent également être ajoutés à cette disposition (p. 7). Les auteurs du projet d'arrêté royal estiment que cela n'est pas absolument nécessaire dans cette disposition vu que l'Autorité nationale de Sécurité est le point de contact pour les personnes morales. Le SGRS et la VSSE sont uniquement compétents pour mener l'enquête de sécurité. Dans un souci d'exhaustivité, les autorités visées à l'article 1^{er}quinquies ont été ajoutées.

Article 87

Cet article n'appelle pas de commentaire supplémentaire.

Sous-section 4. — Enquête de sécurité

Article 88

L'article 88 du projet d'arrêté royal stipulait que les articles 76 à 78 s'appliquaient aux demandes d'habilitation de sécurité des personnes morales.

L'article 77 du projet d'arrêté fait référence à des annexes qui s'appliquent uniquement à la procédure de demande d'habilitation de sécurité pour les personnes physiques. Pour cette raison, la référence à l'article 77 a été supprimée de cet article.

Sous-section 5. — Décision concernant l'habilitation de sécurité

Article 89

Cet article n'appelle pas de commentaire supplémentaire.

Article 90

L'article 90 de l'arrêté prévoit que l'officier de sécurité dispose d'un délai de quinze jours pour notifier aux organes de la personne morale les décisions relatives aux habilitations de sécurité.

Il s'agit, en l'espèce, de la notification de la décision d'habilitation de sécurité de la personne morale et non de l'habilitation de sécurité des administrateurs.

Voor de geclassificeerde informatie van de EU of NAVO wordt de vereiste van de Belgische nationaliteit voor één van de leden van het bestuursorgaan niet opgelegd. Hiervoor volstaat het om een onderdaan te zijn van een lidstaat van één van deze organisaties, gezien het hier -logischerwijze- gaat om de bescherming van de "nationale veiligheid" van de EU of de NAVO. Het zou onevenredig zijn om hier te vereisen dat minstens één van de leden van het bestuursorgaan hier eveneens over de Belgische nationaliteit zou moeten beschikken.

Deze bepaling zorgt ervoor dat de aanvraagprocedure voor de veiligheidsmachtiging voor rechtspersonen niet nodeloos geblokkeerd wordt door de vereiste dat minstens één van de leden van het bestuursorgaan hier eveneens over de Belgische nationaliteit moet beschikken en de geclassificeerde informatie toch de nodige bescherming krijgt.

Artikel 85, § 3 van het besluit stelt dat de persoon aan wie het dagelijks bestuur van de rechtspersoon werd opgedragen in België moet verblijven en er gedomicilieerd zijn. Deze persoon moet tevens kunnen onderworpen worden aan een veiligheidsonderzoek uitgevoerd door één van de inlichtingen- en veiligheidsdiensten overeenkomstig de wet, het voorliggend besluit en de richtlijn van de Nationale Veiligheidsraad, zoals vermeld in artikel 18, vijfde lid van de wet.

Het Comité I meent in zijn verslag dat deze bepaling een voorwaarde toevoegt aan de wet en deze dus dient te vervallen (p. 7). De opstellers van het ontwerpbesluit menen echter dat het hier geen bijkomende voorwaarde betreft.

De wet bepaalt dat een veiligheidsmachtiging enkel kan afgeleverd worden nadat een veiligheidsonderzoek is gevoerd (artikel 16 ev. van de wet). Het onderzoek moet gevoerd worden volgens de regels vervat in de Classificatiewet. Indien het onderzoek niet gevoerd kan worden overeenkomstig deze regels dan kan er geen veiligheidsmachtiging afgeleverd worden. Een andere conclusie zou contra legem zijn en het veiligheidssysteem ondermijnen. Bovendien is België op grond van veiligheidsakkoorden verplicht ervoor te zorgen dat personen die een veiligheidsmachtiging hebben op een correcte manier gehabiteerd zijn. Wanneer zou blijken dat dit niet het geval zou zijn, dan brengt dit de internationale samenwerking in het gedrang.

Indien een persoon niet in België verblijft gedurende een bepaalde periode kan er geen veiligheidsonderzoek gevoerd worden overeenkomstig de voormelde regels wegens een gebrek aan voldoende informatie.

Onderafdeling 3. — Beoordeling van de ontvankelijkheid van de aanvraag

Artikel 86

Artikel 86 stelt dat de Nationale Veiligheidsoverheid zal nagaan of alle in artikel 85, paragraaf 1 vermelde gegevens werden toegestuurd. Het Comité stelde dat in deze bepaling ook de ADIV en de VSSE diende toegevoegd te worden (p.7). De opstellers van het ontwerp koninklijk besluit menen dat dat in deze bepaling niet absoluut noodzakelijk is daar de Nationale Veiligheidsoverheid het aanspreekpunt is voor rechtspersonen. De ADIV en de VSSE zijn enkel bevoegd voor het voeren van het veiligheidsonderzoek. Voor de volledigheid werden de in artikel 1^{er}quinquies bedoelde overheden toch toegevoegd.

Artikel 87

Dit artikel behoeft geen verdere commentaar.

Onderafdeling 4. — Het veiligheidsonderzoek

Artikel 88

Artikel 88 van het ontwerp koninklijk besluit stelde dat de artikelen 76 tot en met 78 van toepassing zijn op de aanvragen van veiligheidsmachtigingen van rechtspersonen.

Artikel 77 van het ontwerpbesluit verwijst naar bijlagen die enkel van toepassing zijn op de aanvraagprocedure van veiligheidsmachtigingen voor natuurlijke personen. Om deze reden werd de verwijzing naar artikel 77 uit dit artikel geschrapt.

Onderafdeling 5. — De beslissing betreffende de veiligheidsmachtiging

Artikel 89

Dit artikel behoeft geen verdere commentaar.

Artikel 90

Artikel 90 van het besluit stelt dat de veiligheidsofficier vijftien dagen de tijd heeft om de beslissingen aangaande de veiligheidsmachtigingen ter kennis te brengen aan de organen van de rechtspersoon.

Hier gaat het over de kennisgeving van de beslissing inzake de veiligheidsmachtiging van de rechtspersoon en niet over de veiligheidsmachtiging van de bestuurders.

La notification doit être motivée. Elle indiquera si la personne morale satisfait aux conditions de discrétion, de loyauté et d'intégrité. Les données à caractère personnel d'un administrateur ne seront jamais partagées avec d'autres personnes.

Lorsque l'Autorité nationale de Sécurité traite des données à caractère personnel en exécution de la loi relative à la classification, elle est liée par les règles visées au titre 3, sous-titre 3, de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel. Les données des sociétés ne constituent pas des données à caractère personnel. Aucune donnée relative à la vie privée des personnes physiques appartenant aux organes de la personne morale n'est communiquée dans la décision concernant l'habilitation de sécurité de la personne morale. Il s'agit d'une décision distincte.

Sous-section 6. — Durée de validité de l'habilitation de sécurité

Article 91

Cet article n'appelle pas de commentaire supplémentaire.

Sous-section 7. — Autres tâches de l'officier de sécurité dans le cadre de la présente section

Article 92

L'article 92 impose à l'officier de sécurité l'obligation de communiquer par écrit à l'Autorité nationale de Sécurité certaines informations concernant la personne morale.

Le Comité R a indiqué dans son avis que cette obligation incombait non pas à l'officier de sécurité mais bien à la personne morale. Le texte du projet d'arrêté a été modifié en ce sens.

En outre, le Conseil d'État a déclaré dans son avis (p. 27) qu'il serait souhaitable que le texte soit aligné sur le régime des habilitations de sécurité pour les personnes physiques en ce qui concerne les enquêtes de sécurité complémentaires. Les alinéas 4 et 5 ont été insérés pour répondre à cette remarque.

Section 3. — Habilitations de sécurité en vue d'un accès à l'étranger

Articles 93 et 94

Les articles 93 et 94 actualisent les articles 27 et 28 de l'arrêté royal du 24 mars 2000. Ces articles n'appellent pas de commentaire supplémentaire.

CHAPITRE 6. — Mesures de protection liées aux marchés publics qui impliquent, nécessitent et/ou contiennent des informations classifiées

Article 95

Étant donné que l'Autorité nationale de Sécurité vérifie que toutes les mesures de protection nécessaires liées aux marchés publics ont été prises pour protéger les informations classifiées pendant la phase de prospection, la procédure d'attribution ainsi que lors de l'exécution d'un marché classifié, elle est également la mieux placée pour élaborer des règles supplémentaires de nature technique et administrative en connaissance de cause.

Articles 96 et 97

Le chapitre 6 définit les mesures de protection liées aux marchés publics qui impliquent ou nécessitent des informations classifiées. Les dispositions de ce chapitre complètent les règles énoncées dans la loi du 13 août 2011 relative aux marchés publics et à certains marchés de travaux, de fournitures et de services dans les domaines de la défense et de la sécurité ; elles ne portent pas préjudice à ces dispositions.

Les marchés impliquant ou nécessitant des informations classifiées relèvent toujours du champ d'application de la loi du 13 août 2011.

Article 98

Cet article n'appelle aucun commentaire.

Article 99

Cet article n'appelle aucun commentaire.

De kennisgeving dient gemotiveerd te zijn. De kennisgeving zal aangeven of de rechtspersoon voldoet aan de voorwaarden geheimhouding, loyaliteit en integriteit. Nooit zullen persoonsgegevens van een bepaalde bestuurder gedeeld worden met andere personen.

Wanneer de Nationale Veiligheidsoverheid persoonsgegevens verwerkt in de uitvoering van de Classificatiewet is zij gebonden aan de regels vervat in titel 3, ondertitel 3 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens. De gegevens van vennootschappen maken geen persoonsgegevens uit. Er worden geen gegevens betreffende het privéleven van de fysieke personen die deel uitmaken van de organen van de rechtspersoon meegedeeld in de beslissing betreffende de veiligheidsmachtiging van de rechtspersoon. Dit vormt een aparte beslissing.

Onderafdeling 6. — Geldigheidsduur van de veiligheidsmachtiging

Artikel 91

Dit artikel behoeft geen verdere commentaar.

Onderafdeling 7. — Overige taken van de veiligheidsofficier in het kader van deze afdeling

Artikel 92

Artikel 92 legt aan de veiligheidsofficier de verplichting op om bepaalde informatie inzake de rechtspersoon schriftelijk mee te delen aan de Nationale Veiligheidsoverheid.

Het Comité I stelde in zijn advies dat deze verplichting niet toekomt aan de veiligheidsofficier maar wel aan de rechtspersoon. De tekst van het ontwerpbesluit werd hieraan aangepast.

Verder stelde de Raad van State in zijn advies (op p. 56) dat het wenselijk zou zijn dat de tekst afgelijnd wordt met de regeling voor veiligheidsmachtigingen voor natuurlijke personen voor wat betreft de tussentijdse veiligheidsonderzoeken. Om tegemoet te komen aan deze opmerking werd een vierde en een vijfde lid toegevoegd.

Afdeling 3. — Veiligheidsmachtigingen met het oog op toegang in het buitenland

Artikelen 93 en 94

Artikelen 93 en 94 zijn een actualisatie van de artikelen 27 en 28 van het koninklijk besluit van 24 maart van 2000. Deze artikelen behoeven geen verdere commentaar.

HOOFDSTUK 6. — De beschermingsmaatregelen verbonden aan overheidsopdrachten die betrekking hebben op geclassificeerde informatie of deze noodzakelijk maken en/of bevatten

Artikel 95

Gezien de Nationale Veiligheidsoverheid verifieert dat alle beschermingsmaatregelen verbonden aan overheidsopdrachten werden genomen nodig voor de bescherming van geclassificeerde informatie tijdens de prospectiefase, de gunningsprocedure en de uitvoering van een geclassificeerde opdracht, is deze ook het best geplaatst om bijkomende regels van technische en administratieve aard met kennis van zaken uit te werken.

Artikelen 96 en 97

Hoofdstuk 6 bepaalt de beschermingsmaatregelen die verbonden zijn aan overheidsopdrachten die betrekking hebben op geclassificeerde informatie of deze noodzakelijk maken. De bepalingen in dit hoofdstuk zijn een aanvulling op de regels vervat in de wet van 13 augustus 2011 inzake overheidsopdrachten en bepaalde opdrachten voor werken, levering en diensten op defensie- en veiligheidsgebied; zij doen geen afbreuk aan deze bepalingen.

Opdrachten die betrekking hebben op geclassificeerde informatie of deze noodzakelijk maken vallen steeds onder het toepassingsgebied van de wet van 13 augustus 2011.

Artikel 98

Dit artikel behoeft geen commentaar.

Artikel 99

Dit artikel behoeft geen commentaar.

Article 100

L'article 100, 1°, du présent projet dispose que l'Autorité nationale de Sécurité vérifie que « les adjudicataires enregistrés sur le territoire qui participent à des marchés publics impliquant, nécessitant et/ou contenant des informations classifiées de niveau « CONFIDENTIEL » ou supérieur ou aux contrats de sous-traitance y afférents pendant l'exécution des marchés ou au stade précontractuel, disposent d'une habilitation de sécurité pour les personnes morales octroyée au niveau de classification correspondant ».

Le Conseil d'État en déduit qu'il ne peut s'agir que d'un « adjudicataire établi sur le territoire, ce qui exclut tous les adjudicataires potentiels non enregistrés » (rapport p. 9).

Les auteurs renvoient au commentaire de l'article 84 du présent arrêté. Seules les personnes morales dont le siège social se situe en Belgique peuvent être habilitées par l'Autorité nationale de Sécurité dans le cadre d'un marché public belge classifié. L'Autorité nationale de Sécurité n'a pas de compétences (de supervision, notamment) concernant les entreprises à l'étranger. Les informations à examiner en ce qui concerne une personne morale enregistrée à l'étranger ne sont pas non plus accessibles aux services d'enquête belges. Toutefois, les entreprises enregistrées sur le territoire (= inscrites au registre belge des entreprises, la Banque-Carrefour des Entreprises (BCE)) ne sont pas exclues en soi de la participation aux appels d'offres publics classifiés.

Pour répondre à la remarque du Conseil d'État selon laquelle l'exclusion des personnes morales n'ayant pas de siège social en Belgique, alors que celles-ci peuvent satisfaire à toutes les exigences de sécurité sur la base d'une attestation délivrée par une autorité étrangère et reconnue par l'Autorité nationale de Sécurité en vertu d'un accord international, est disproportionnée, une disposition a été ajoutée au point 5° de l'article 100. Il en ressort que l'Autorité nationale de Sécurité vérifie que les personnes morales qui ne sont pas immatriculées sur le territoire disposent d'une habilitation de sécurité pour personnes morales valide, délivrée par les autorités compétentes du pays tiers et reconnue par l'Autorité nationale de Sécurité sur la base des accords et traités internationaux liant la Belgique en la matière, par analogie aux dispositions de l'article 84, alinéa 2, du présent arrêté.

Article 101

Cet article n'appelle aucun commentaire.

Article 102

Le projet d'arrêté prévoyait que les candidats ou soumissionnaires non retenus devaient restituer au pouvoir adjudicateur les informations classifiées en leur possession dans un délai de 15 jours ouvrables à compter de la notification de leur non-sélection. Ils ne sont pas non plus autorisés à conserver des copies de ces informations. Cette disposition résulte du fait que des personnes morales ne peuvent jamais être l'autorité d'origine.

Dans son avis (p. 28), le Conseil d'État pose la question de savoir si le fait que les candidats non sélectionnés n'ont pas le droit de conserver les pièces classifiées dans le cadre de la procédure de recours qu'ils engagent est compatible avec le droit effectif au recours garanti par l'article 13 de la CEDH.

Si des candidats se voient accorder l'accès à des informations classifiées, cet accès n'est exigé qu'en vue de l'exécution du marché public.

Conformément à l'article 8 de la loi, nul ne peut avoir accès à des informations classifiées s'il n'est pas titulaire d'une habilitation de sécurité correspondante, s'il n'a pas reçu un briefing de sécurité sur ses obligations et dans la mesure où la prise de connaissance et l'accès sont nécessaires à l'exercice de ses fonctions ou de son marché.

Cependant, une personne ne doit pas être titulaire d'une habilitation de sécurité pour accéder à des informations classifiées de niveau « RESTREINT ».

Les autorités judiciaires telles que les juges et les magistrats, y compris les membres de l'Organe de recours visé dans la loi du 11 décembre 1998 portant création d'un organe de recours en matière d'habilitations de sécurité, d'attestations de sécurité et d'avis de sécurité, peuvent toutefois prendre connaissance d'informations classifiées sans disposer de l'habilitation de sécurité requise dans le cadre de l'exercice de leurs fonctions judiciaires.

Si la personne morale n'a pas été sélectionnée pour le marché public, elle n'a pas de besoin d'en connaître pour prendre connaissance des informations classifiées et ne remplit plus les conditions de l'article 8 de la loi.

Artikel 100

Artikel 100, 1° van voorliggend ontwerp stelt dat de Nationale veiligheidsoverheid nagaat of de "op het grondgebied geregistreerde opdrachtnemers die deelnemen aan overheidsopdrachten die betrekking hebben op geclassificeerde informatie van het niveau "VERTROUWELIJK" of hoger of deze noodzakelijk maken en/of bevatten, of deze in onderaanneming tijdens de uitvoering van de opdrachten of in de precontractuele fase beschikken over een veiligheidsmachtiging voor rechtspersonen in overeenstemming met het overeenkomstige classificatieniveau".

De Raad van State leidt hieruit af dat het enkel kan gaan over "een op het grondgebied gevestigde opdrachtnemer wat alle potentiële niet geregistreerde opdrachtnemers uitsluit" (verslag p. 37).

De opstellers verwijzen naar de commentaar bij artikel 84 van het voorliggend besluit. Enkel rechtspersonen waarvan de statutaire zetel in België is gevestigd, kunnen door de Nationale Veiligheidsoverheid gemachtigd worden in het kader van een Belgische geclassificeerde overheidsopdracht. De Nationale Veiligheidsoverheid heeft geen bevoegdheden (oa. van toezicht) ten aanzien van ondernemingen in het buitenland. De te onderzoeken inlichtingen van een in het buitenland geregistreerde rechtspersoon zijn ook niet toegankelijk voor de Belgische onderzoeksdiensten. Maar op het grondgebied geregistreerde (= geregistreerd in het Belgische ondernemingsregister, de Kruispuntbank van Ondernemingen (KBO)) ondernemingen zijn op zich niet uitgesloten om deel te nemen aan geclassificeerde openbare aanbestedingen.

Om de opmerking van de Raad van State te beantwoorden dat de uitsluiting van rechtspersonen die geen statutaire zetel hebben in België, terwijl ze wel kunnen beantwoorden aan alle veiligheidsvereisten op grond van een attest afgegeven door een buitenlandse overheid en erkend door de Nationale Veiligheidsoverheid krachtens een internationale overeenkomst, onevenredig is, werd in een punt 5° van artikel 100 een bepaling toegevoegd. Hieruit blijkt dat de Nationale Veiligheidsoverheid verifieert dat rechtspersonen die niet zijn geregistreerd op het grondgebied beschikken over een geldige veiligheidsmachtiging voor rechtspersonen, afgeleverd door de bevoegde autoriteiten van het derde land en erkend door de Nationale Veiligheidsoverheid op grond van de internationale overeenkomsten en verdragen die België ter zake binden, naar analogie met de bepalingen van artikel 84, tweede lid van voorliggend besluit.

Artikel 101

Dit artikel behoeft geen commentaar.

Artikel 102

Het ontwerp besluit voorzag dat kandidaten of inschrijvers die niet geselecteerd werden de geclassificeerde informatie die in hun bezit is, terug dienden te sturen naar de aanbestedende overheid binnen de vijftien werkdagen na betekening van hun niet-selectie. Ze mogen ook geen kopieën bijhouden van deze informatie. Deze bepaling is een gevolg van het feit dat rechtspersonen nooit de overheid van oorsprong kunnen zijn.

De Raad van State stelt in haar advies (op p. 57) de vraag of het feit dat niet-geselecteerde kandidaten niet het recht hebben om de geclassificeerde stukken bij te houden in het kader van de beroepsprocedure die zij instellen verzoenbaar is met het recht op daadwerkelijke rechtshulp gegarandeerd op grond van artikel 13 EVRM.

Indien kandidaten toegang wordt verleend tot geclassificeerde informatie, dan is deze toegang enkel vereist om de overheidsopdracht te kunnen uitvoeren.

Overeenkomstig artikel 8 van de wet heeft niemand toegang tot geclassificeerde informatie, tenzij hij houder is van een overeenstemmende veiligheidsmachtiging, een veiligheidsbriefing heeft ontvangen over zijn verplichtingen en voor zover de kennisname en de toegang noodzakelijk zijn voor de uitoefening van zijn functie of zijn opdracht.

Een persoon dient echter geen houder te zijn van een veiligheidsmachtiging om toegang te hebben tot geclassificeerde informatie van het niveau BEPERKT.

Gerechtigde overheden zoals rechters en magistraten, inclusief de leden van het Beroepsorgaan bedoeld in de wet van 11 december 1998 tot oprichting van een beroepsorgaan inzake veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen kunnen echter kennisnemen van geclassificeerde informatie zonder te beschikken over de vereiste veiligheidsmachtiging in het kader van de uitoefening van hun gerechtelijke functie.

Indien de rechtspersoon niet geselecteerd werd voor de overheidsopdracht, dan beschikt zij niet over de vereiste need to know om kennis te kunnen nemen van de geclassificeerde informatie en voldoet zij niet meer aan de voorwaarden van artikel 8 van de wet.

Cette disposition n'empêche cependant pas la personne morale d'introduire un recours contre la décision de non-sélection.

La personne morale dispose d'un délai de 60 jours pour introduire un recours contre la décision de non-sélection devant le Conseil d'État. Afin de permettre à la personne morale concernée de prouver le bien-fondé de son recours, la date limite à laquelle les documents classifiés doivent être renvoyés à l'autorité d'origine est modifiée comme suit : « après la fin de la période du recours ».

Le délai d'introduction du recours est le délai maximum. Si la personne morale n'a pas l'intention de contester la décision, les informations classifiées doivent être renvoyées à l'autorité d'origine dans un délai de 15 jours. En outre, les informations classifiées ne doivent être utilisées que si le bien-fondé du recours ne peut être démontré sur la base d'autres informations non classifiées.

Lorsque la fin de la période de recours est atteinte, les informations classifiées doivent être renvoyées à l'autorité d'origine. C'est d'ailleurs l'autorité d'origine qui prendra les mesures nécessaires pour que les juges aient accès aux informations classifiées pour leur appréciation.

Les droits dont bénéficie la personne morale non sélectionnée pour introduire un recours sont ainsi suffisamment garantis.

CHAPITRE 7. — *Contrôle*

Le chapitre 7 traite du contrôle.

Articles 103 à 111

Les articles 103 à 111 n'appellent aucun commentaire, si ce n'est pour préciser que le délai de 15 jours ouvrables mentionné à l'article 109 est un délai d'ordre.

TITRE V. — *Dispositions transitoires et finales*

Article 112

L'article 112, alinéa 1^{er}, est une disposition déjà mentionnée dans l'arrêté royal du 24 mars 2000. Cette disposition est nécessaire pour conférer la protection nécessaire aux documents d'archives, qui n'étaient pas classifiés conformément aux dispositions de la loi relative à la classification lors de son entrée en vigueur le 1^{er} juin 2000. Cette disposition n'exclut pas que les documents qui ne sont pas classifiés, mais qui contiennent des éléments classifiés au niveau du contenu (par exemple en ce qui concerne les sources), puissent encore être classifiés conformément aux dispositions de la loi relative à la classification et du présent arrêté d'exécution (éventuellement en application de l'article 21 du présent arrêté). En effet, avant l'entrée en vigueur de la loi relative à la classification, le 1^{er} juin 2000, il n'existait pas de règles univoques relatives à la classification des documents, mais il pouvait s'agir de documents « sensibles », dont l'utilisation non appropriée pouvait porter atteinte à l'un des intérêts énumérés à l'article 3, § 1^{er} de la loi.

L'article 112, alinéa 2, dispose que les pièces classifiées après l'entrée en vigueur de la loi relative à la classification le 1^{er} juin 2000, mais avant l'entrée en vigueur du présent arrêté, revêtus de la mention « TRÈS SECRET », « SECRET » ou « CONFIDENTIEL » et d'une référence à la loi qui ne respecte pas pleinement les exigences de forme énoncées à l'article 16, alinéa 2 ou 3, sont réputées porter le degré de classification correspondant prévu à l'article 4 de la loi. L'objectif est d'éviter que ces pièces ne soient considérées comme « non classifiées » conformément à l'article 16, alinéa 6, du présent arrêté.

Article 113

L'article 113 concerne une disposition transitoire pour les documents portant la mention « DIFFUSION RESTREINTE », conformément à l'article 20 de l'arrêté royal du 24 mars 2000.

Afin d'établir une distinction claire avec les informations classifiées de niveau « RESTREINT » (et de protéger ces informations), le projet prévoit expressément que les documents revêtus de la mention « DIFFUSION RESTREINTE » (AR 24.03.2000) avant l'entrée en vigueur du présent arrêté continueront à porter cette mention, mais ne pourront en aucun cas être assimilés au niveau de classification « RESTREINT ».

Deze regeling weerhoudt echter de rechtspersoon niet om een beroep in te stellen tot vernietiging van de beslissing tot niet-selectie.

De rechtspersoon beschikt over een termijn van 60 dagen om een beroep tot vernietiging van de beslissing om hem niet te weerhouden in te stellen bij de Raad van State. Om de betrokken rechtspersoon de mogelijkheid te geven om de gegrondheid van zijn beroep aan te tonen wordt de termijn waarbinnen de geclassificeerde documenten moeten worden terugbezorgd aan de overheid van oorsprong veranderd in "na afloop van de beroepstermijn".

De termijn voor het instellen van het beroep geldt als maximumtermijn. Indien de rechtspersoon niet van plan is om de beslissing aan te vechten, dan dient de geclassificeerde informatie binnen de 15 dagen terugbezorgd te worden aan overheid van oorsprong. Verder mag de geclassificeerde informatie enkel gebruikt worden indien de gegrondheid van het beroep onmogelijk kan aangetoond worden op grond van andere niet geclassificeerde informatie.

Wanneer de beroepstermijn is verstreken moet de geclassificeerde informatie terugbezorgd worden aan de overheid van oorsprong. Het is overigens de overheid van oorsprong die de nodige maatregelen zal nemen opdat de rechters inzage zullen krijgen in de geclassificeerde informatie voor hun beoordeling.

Op deze manier worden de rechten van de niet-geselecteerde rechtspersoon om beroep aan te tekenen tegen de beslissing voldoende gegarandeerd.

HOOFDSTUK 7. — *Toezicht*

Hoofdstuk 7 behandelt het toezicht.

Artikelen 103 tot 111

Artikelen 103 tot 111 vergen geen specifieke commentaar, buiten de precisering dat de termijn van vijftien werkdagen vermeld in artikel 109 een termijn van orde is.

TITEL IV. — *Overgangs- en slotbepalingen*

Artikel 112

Artikel 112, eerste lid is een bepaling die reeds werd vermeld in het koninklijk besluit van 24 maart 2000. Deze bepaling is nodig om archiefstukken, die niet waren geclassificeerd overeenkomstig de bepalingen van de Classificatiewet op het moment van de inwerking-treding van de Classificatiewet op 1 juni 2000, toch nog de nodige bescherming te geven. Deze bepaling sluit overigens niet uit dat archiefstukken, die geen classificatie dragen, maar inhoudelijk wel degelijk geclassificeerde elementen bevatten (bijvoorbeeld met betrekking tot bronnen) alsnog geclassificeerd worden overeenkomstig de voorschriften van de Classificatiewet en voorliggend uitvoeringsbesluit (eventueel in toepassing van artikel 21 van voorliggend besluit). Vóór de inwerkingtreding van de Classificatiewet op 1 juni 2000 waren er immers geen eenduidige regels betreffende het classificeren van documenten, maar kunnen het wel "gevoelige" documenten betreffen waarvan de niet-geëigende aanwending schade kan toebrengen aan één van de in artikel 3, § 1 van de wet opgesomde belangen.

In artikel 112, tweede lid, wordt bepaald dat de stukken geclassificeerd na de inwerkingtreding van de Classificatiewet op 1 juni 2000 maar voor de inwerkingtreding van onderhavig besluit gemerkt met de vermelding "ZEER GEHEIM", "GEHEIM", of "VERTROUWELIJK" en een verwijzing naar de wet die niet volledig overeenstemt met de formele vereisten vermeld in artikel 2, tweede of derde lid worden geacht gemerkt te zijn met het overeenstemmend classificatieniveau voorzien in artikel 4 van de wet. Dit om te vermijden dat deze stukken als "niet-geclassificeerd" worden beschouwd overeenkomstig artikel 16, zesde lid van voorliggend besluit.

Artikel 113

Artikel 113 betreft een overgangsbepaling voor de documenten die overeenkomstig artikel 20 van het koninklijk besluit van 24 maart 2000 gemerkt worden met de vermelding "Beperkte verspreiding".

Om een duidelijk onderscheid te maken met geclassificeerde informatie met het classificatieniveau "BEPERKT" (en ter bescherming van deze informatie) wordt uitdrukkelijk in het ontwerp bepaald dat documenten, vóór de inwerkingtreding van voorliggend besluit, voorzien van de vermelding "BEPERKTE VERSPREIDING" (KB 24.03.2000) deze vermelding blijven behouden, maar deze op geen enkele manier kunnen worden gelijkgesteld met het classificatieniveau "BEPERKT".

En revanche, les nouveaux documents créés à partir de l'entrée en vigueur du présent arrêté et dont l'autorité d'origine souhaite restreindre la diffusion aux personnes autorisées à en prendre connaissance porteront non plus la mention « DIFFUSION RESTREINTE », mais bien la mention « SENSIBLE NON CLASSIFIÉ » et ce, sans préjudice d'autres dispositions légales ou réglementaires spécifiques concernant les informations non classifiées. Cela signifie que la présente disposition n'affecte pas la validité d'autres dispositions légales ou réglementaires spécifiques. Les deux dispositions sont donc au même niveau et peuvent s'appliquer simultanément.

Cette disposition permet d'éviter toute confusion entre les niveaux de classification « DIFFUSION RESTREINTE » et « RESTREINT » dans l'objectif de protéger le niveau de classification « RESTREINT ». Les documents portant la mention « SENSIBLE NON CLASSIFIÉ » (ou l'ancienne mention « DIFFUSION RESTREINTE ») sont protégés par des règles de secret professionnel dont la violation expose à des poursuites pénales et, éventuellement, à des sanctions disciplinaires.

Articles 114 à 116

Les articles 114 à 116 n'appellent aucun commentaire.

J'ai l'honneur d'être,

Sire,
de Votre Majesté,
le très respectueux
et très fidèle serviteur,
Le Ministre de la Justice,
P. VAN TIGCHELT
La Ministre de la Défense,
L. DEDONDER
La Ministre de l'Intérieur,
A. VERLINDEN

Conseil d'Etat, section de législation

Avis 76.465/2 du 9 juillet 2024 sur un projet d'arrêté royal 'portant exécution de la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, attestations de sécurité, avis de sécurité et au service public réglementé'

Le 8 mai 2024, le Conseil d'Etat, section de législation, a été invité par le Vice-Premier Ministre et Ministre de la Justice et de la Mer du Nord à communiquer un avis dans un délai de trente jours prorogé de trente jours *, sur un projet d'arrêté royal 'portant exécution de la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, attestations de sécurité, avis de sécurité et au service public réglementé'.

Le projet a été examiné par la deuxième chambre le 1^{er} juillet 2024. La chambre était composée de Patrick RONVAUX, président de chambre, Christine HOREVOETS et Pierre-Olivier DE BROUX, conseillers d'Etat, Christian BEHRENDT et Jacques ENGLEBERT, assesseurs, et Béatrice DRAPIER, greffier.

Le rapport a été présenté par Stéphane TELLIER, premier auditeur.

La concordance entre la version française et la version néerlandaise a été vérifiée sous le contrôle de Pierre-Olivier DE BROUX.

L'avis, dont le texte suit, a été donné le 9 juillet 2024.

Comme la demande d'avis est introduite sur la base de l'article 84, § 1^{er}, alinéa 1^{er}, 2°, des lois 'sur le Conseil d'Etat', coordonnées le 12 janvier 1973, la section de législation limite son examen au fondement juridique du projet, à la compétence de l'auteur de l'acte ainsi qu'à l'accomplissement des formalités préalables, conformément à l'article 84, § 3, des lois coordonnées précitées.

Sur ces trois points, le projet appelle les observations suivantes.

Anderzijds krijgen nieuwe documenten, die worden gecreëerd vanaf de inwerkingtreding van voorliggend besluit en waarvan de overheid van oorsprong de verspreiding wil beperken tot de personen die bevoegd zijn om er kennis van te nemen, niet langer de vermelding "BEPERKTE VERSPREIDING" maar de vermelding "GEVOELIG NIET-GECLASSIFICEERD" en dit onverminderd andere specifieke wettelijke of reglementaire bepalingen betreffende niet-geclassificeerde informatie. Dit laatste houdt in dat voorliggende bepaling geen gevolgen heeft voor de gelding van eventuele andere bepalingen in andere specifieke wettelijke of reglementaire bepalingen. Beide bepalingen staan dus op hetzelfde niveau en ze kunnen tegelijk van toepassing zijn.

Hiermee wordt elke verwarring tussen het classificatieniveau "BEPERKTE VERSPREIDING" en "BEPERKT" uitgesloten, hetgeen tot doel heeft om het classificatieniveau "BEPERKT" te beschermen. Documenten met de vermelding "GEVOELIG NIET-GECLASSIFICEERD" (of de vroegere vermelding "BEPERKTE VERSPREIDING") worden beschermd door de regels betreffende het beroepsgeheim, waarvan de schending blootstelt aan strafrechtelijke vervolging en, eventueel aan disciplinaire sancties.

Artikelen 114 tot 116

De artikelen 114 tot en met 116 behoeven geen commentaar.

Ik heb de eer te zijn,

Sire,
van Uwe Majesteit,
de zeer eerbiedige
en zeer getrouwe dienaar,
De Minister van Justitie
P. VAN TIGCHELT
De Minister van Defensie,
L. DEDONDER
De Minister van Binnenlandse Zaken,
A. VERLINDEN

Raad van State, afdeling Wetgeving

Advies 76.465/2 van 9 juli 2024 over een ontwerp van koninklijk besluit 'tot uitvoering van de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, veiligheidsattesten, veiligheidsadviezen en de publiek gereguleerde dienst'

Op 8 mei 2024 is de Raad van State, afdeling Wetgeving, door de Vice-eersteminister en Minister van Justitie en Noordzee verzocht binnen een termijn van dertig dagen verlengd met dertig dagen* een advies te verstrekken over een ontwerp van koninklijk besluit 'tot uitvoering van de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, veiligheidsadviezen en de publiek gereguleerde dienst'.

Het ontwerp is door de tweede kamer onderzocht op 1 juli 2024. De kamer was samengesteld uit Patrick RONVAUX, kamervoorzitter, Christine HOREVOETS en Pierre Olivier DE BROUX, staatsraden, Christian BEHRENDT en Jacques ENGLEBERT, assessoren, en Béatrice DRAPIER, griffier.

Het verslag is uitgebracht door Stéphane TELLIER, eerste auditeur.

De overeenstemming tussen de Franse en de Nederlandse tekst van het advies is nagzien onder toezicht van Pierre-Olivier DE BROUX.

Het advies, waarvan de tekst hierna volgt, is gegeven op 9 juli 2024.

Aangezien de adviesaanvraag ingediend is op basis van artikel 84, § 1, eerste lid, 2°, van de wetten 'op de Raad van State', gecoördineerd op 12 januari 1973, beperkt de afdeling Wetgeving overeenkomstig artikel 84, § 3, van de voornoemde gecoördineerde wetten haar onderzoek tot de rechtsgrond van het ontwerp, de bevoegdheid van de steller van de handeling en de te vervullen voorafgaande vormvereisten.

Wat die drie punten betreft, geeft het ontwerp aanleiding tot de volgende opmerkingen.

OBSERVATIONS PRÉALABLES

1. Compte tenu du moment où le présent avis est donné, la section de législation attire l'attention du demandeur d'avis sur le fait que la dissolution des Chambres législatives emporte que, depuis cette date et jusqu'à ce que, à la suite de l'élection des membres de la Chambre des représentants, le Roi nomme un nouveau Gouvernement, le Gouvernement ne dispose plus de la plénitude de ses compétences. Le présent avis est toutefois donné sans qu'il soit examiné si le projet relève bien des compétences ainsi limitées, la section de législation n'ayant pas connaissance de l'ensemble des éléments de fait que le Gouvernement peut prendre en considération lorsqu'il doit apprécier la nécessité d'arrêter ou de modifier des dispositions réglementaires.

2. Dans un souci de sécurité juridique et compte tenu de la matière sensible réglée par le projet, la publication au *Moniteur belge* de l'arrêté qui en résultera gagnerait à être accompagnée d'un rapport au Roi permettant d'en expliciter les dispositions.

FORMALITÉS PRÉALABLES

La déléguée du Ministre a indiqué ce qui suit, s'agissant de l'accomplissement des formalités préalables :

« De afschriften van de adviesvragen aan het Comité I¹, het COC en het College van Procureurs-Generaal worden u nagestuurd ».

Si l'accomplissement de ces formalités devait encore donner lieu à des modifications du texte soumis au Conseil d'État sur des points autres que de pure forme et ne résultant pas également des suites réservées au présent avis, les dispositions modifiées ou ajoutées devraient être soumises à nouveau à l'avis de la section de législation, conformément à l'article 3, § 1^{er}, alinéa 1^{er}, des lois coordonnées 'sur le Conseil d'État'.

OBSERVATIONS GÉNÉRALES

I. La réglementation envisagée au regard du droit de l'Union européenne

1. La réglementation en projet prévoit, de manière générale et sauf exceptions, que toute personne physique ou morale qui souhaite accéder à des informations classifiées doit disposer d'une habilitation de sécurité.

S'agissant des personnes morales, l'article 84, alinéa 1^{er}, du projet prévoit que

« [s]eules les personnes morales dont le siège social se situe en Belgique peuvent être habilitées dans le cadre des marchés publics qui impliquent, nécessitent et/ou contiennent des informations classifiées de niveau 'CONFIDENTIEL' ou supérieur ».

Cette disposition implique que, lorsqu'un marché public nécessite l'accès à des informations classifiées de niveau « CONFIDENTIEL » ou supérieur, seules des personnes morales qui ont leur siège social en Belgique pourront y soumissionner dès lors qu'elles seules pourront disposer d'une habilitation de sécurité pour ce faire.

Cette disposition apparaît contraire aux principes de libre circulation des marchandises, des services et de liberté d'établissement au sens des articles 34, 49 et 56 du Traité sur le Fonctionnement de l'Union européenne (TFUE). En effet, la passation de marchés conclus dans les États membres par les entités adjudicatrices doit respecter les principes du traité, notamment la libre circulation des marchandises, la liberté d'établissement et la libre prestation de services, ainsi que les principes qui en découlent, comme l'égalité de traitement, la non-discrimination, la reconnaissance mutuelle, la proportionnalité et la transparence.

Toutefois, l'article 346, paragraphe 1, du TFUE dispose ce qui suit :

« 1. Les dispositions des traités ne font pas obstacle aux règles ci-après :

a) aucun État membre n'est tenu de fournir des renseignements dont il estimerait la divulgation contraire aux intérêts essentiels de sa sécurité,

b) tout État membre peut prendre les mesures qu'il estime nécessaires à la protection des intérêts essentiels de sa sécurité et qui se rapportent à la production ou au commerce d'armes, de munitions et de matériel de guerre ; ces mesures ne doivent pas altérer les conditions de la concurrence dans le marché intérieur en ce qui concerne les produits non destinés à des fins spécifiquement militaires ».

VOORAFGAANDE OPMERKINGEN

1. Rekening houdend met het ogenblik waarop dit advies gegeven wordt, vestigt de afdeling Wetgeving de aandacht van de adviesaanvrager erop dat de ontbinding van de wetgevende kamers tot gevolg heeft dat de regering sedert die datum en totdat, na de verkiezing van de leden van de Kamer van volksvertegenwoordigers, een nieuwe regering is benoemd door de Koning, niet meer over de volheid van haar bevoegdheid beschikt. Dit advies wordt evenwel gegeven zonder dat wordt nagegaan of dit ontwerp in die beperkte bevoegdheid kan worden ingepast, aangezien de afdeling Wetgeving geen kennis heeft van het geheel van de feitelijke gegevens die de regering in aanmerking kan nemen als ze te oordelen heeft of het vaststellen of het wijzigen van verordeningen noodzakelijk is.

2. Ter wille van de rechtszekerheid en rekening houdend met de gevoelige aangelegenheid die bij het ontwerp geregeld wordt, verdient het aanbeveling het besluit, in het vooruitzicht van de bekendmaking ervan in het *Belgisch Staatsblad*, te voorzien van een verslag aan de Koning waarin de bepalingen toegelicht worden.

VOORAFGAANDE VORMVEREISTEN

De gemachtigde van de minister heeft het volgende aangegeven in verband met de vervulling van de voorafgaande vormvereisten:

“De afschriften van de adviesvragen aan het Comité I,¹ het COC en het College van Procureurs—Generaal worden u nagestuurd.”

Indien de aan de Raad van State voorgelegde tekst naar aanleiding van het vervullen van die vormvereisten nog wijzigingen zou ondergaan die niet louter vormelijk zijn en die tevens niet voortvloeien uit het gevolg dat aan dit advies gegeven wordt, zouden de gewijzigde of toegevoegde bepalingen op hun beurt om advies aan de afdeling Wetgeving moeten worden voorgelegd overeenkomstig artikel 3, § 1, eerste lid, van de gecoördineerde wetten 'op de Raad van State'.

ALGEMENE OPMERKINGEN

I. De beoogde regelgeving ten aanzien van het recht van de Europese Unie

1. De ontworpen regelgeving bepaalt dat, in het algemeen en behoudens uitzonderingen, elke natuurlijke of rechtspersoon die toegang wenst tot de geclassificeerde gegevens, moet beschikken over een veiligheidsmachtiging.

Wat de rechtspersonen betreft, bepaalt artikel 84, eerste lid, van het ontwerp:

“Enkel rechtspersonen waarvan de statutaire zetel in België is gevestigd, kunnen gemachtigd worden in het kader van overheidsopdrachten die betrekking hebben op geclassificeerde informatie van het niveau 'VERTROUWELIJK' of hoger of deze noodzakelijk maken en/of bevatten.”

Deze bepaling houdt in dat, wanneer voor een overheidsopdracht de toegang vereist is tot geclassificeerde informatie van het niveau "VERTROUWELIJK" of hoger, enkel rechtspersonen waarvan de statutaire zetel in België gevestigd is, daarop zullen kunnen inschrijven aangezien alleen zij over een veiligheidsmachtiging daartoe zullen kunnen beschikken.

Die bepaling blijkt strijdig met de beginselen inzake het vrij verkeer van goederen en diensten en de vrijheid van vestiging in de zin van de artikelen 34, 49 en 56 van het Verdrag betreffende de werking van de Europese Unie (VWEU). Het plaatsen van door de aanbestedende instanties in de lidstaten gesloten opdrachten dient immers te gebeuren met naleving van de beginselen vervat in het Verdrag, inzonderheid het vrij verkeer van goederen, de vrijheid van vestiging en het vrij verrichten van diensten, alsook van de beginselen die daaruit voortvloeien zoals gelijke behandeling, niet—discriminatie, wederzijdse erkenning, evenredigheid en transparantie.

Artikel 346, lid 1, van het VWEU bepaalt evenwel het volgende:

“1. De bepalingen van de Verdragen vormen geen beletsel voor de volgende regels:

a) geen enkele lidstaat is gehouden inlichtingen te verstrekken waarvan de verbreiding naar zijn mening strijdig zou zijn met de wezenlijke belangen van zijn veiligheid;

b) elke lidstaat kan de maatregelen nemen die hij noodzakelijk acht voor de bescherming van de wezenlijke belangen van zijn veiligheid en die betrekking hebben op de productie van of de handel in wapenen, munitie en oorlogsmateriaal; die maatregelen mogen de mededingingsverhoudingen op de interne markt niet wijzigen voor producten die niet bestemd zijn voor specifiek militaire doeleinden.”

Des restrictions à ces libertés peuvent dès lors être prévues par les États membres de l'Union européenne lorsqu'elles sont nécessaires et proportionnées à la sauvegarde des intérêts reconnus comme légitimes par les dispositions du traité.

Le législateur européen a lui-même adopté des dispositions permettant ces restrictions, dans le domaine spécifique des marchés publics en matière de défense et de sécurité, par l'adoption de la directive 2009/81/CE du Parlement européen et du Conseil du 13 juillet 2009 'relative à la coordination des procédures de passation de certains marchés de travaux, de fournitures et de services par des pouvoirs adjudicateurs ou entités adjudicatrices dans les domaines de la défense et de la sécurité, et modifiant les directives 2004/17/CE et 2004/18/CE', transposée en droit belge par la loi du 13 août 2011 'relative aux marchés publics et à certains marchés de travaux, de fournitures et de services dans les domaines de la défense et de la sécurité'.

Cette directive, par des règles d'exemption, laisse par ailleurs aux États membres la possibilité d'adopter des mesures plus restrictives que celles prévues dans la directive².

Le titre 3/1 de la loi du 13 août 2011, inséré par la loi du 17 juin 2016 'relative aux marchés publics', intitulé « Marchés exclus sur base d'intérêts de sécurité essentiels ou sur base de l'article 346 du Traité relatif au fonctionnement de l'Union européenne », contient un article 43/1 qui dispose comme suit :

« Le Roi peut rendre applicables des règles de passation, de contrôle et d'exécution spécifiques aux marchés publics visés à l'article 15, alinéa 2 ».

L'article 15, alinéa 2, de la même loi, dispose ce qui suit :

« Dans les cas visés ci-dessous, seul le titre 3/1 est d'application :

1° si et dans la mesure où la protection des intérêts essentiels de la sécurité du Royaume ne peut être garantie par des mesures moins intrusives, par exemple en imposant des conditions en vue de protéger la confidentialité des informations que le pouvoir adjudicateur met à disposition conformément aux titre 2 et 3 de la présente loi ;

2° si et dans la mesure où l'application des dispositions du titre 2 et 3 de la présente loi obligerait le Royaume à fournir des informations dont il estimerait la divulgation contraire aux intérêts essentiels de sa sécurité ;

3° lorsque la passation et l'exécution du marché public sont déclarés secrets ou doivent s'accompagner de mesures particulières de sécurité, conformément aux dispositions législatives, réglementaires ou administratives en vigueur dans le Royaume, pour autant qu'il est établi que la protection des intérêts essentiels concernés ne peut être garantie par des mesures moins intrusives, telles que celles visées au 1° ;

4° lorsque l'article 346 du Traité relatif au fonctionnement de l'Union européenne est d'application ».

Il peut également être fait référence à l'article 33 de la loi du 17 juin 2016, qui dispose comme suit :

« § 1^{er}. La présente loi s'applique aux marchés publics dans les domaines de la défense et de la sécurité, hormis :

1° les marchés relevant de la loi défense et sécurité ;

2° les marchés visés à l'article 18 de la loi défense et sécurité.

§ 2. La présente loi ne s'applique pas aux marchés publics qui ne sont pas par ailleurs exclus en vertu du paragraphe 1^{er} dans la mesure où la protection des intérêts essentiels de la sécurité du Royaume ne peut être garantie par des mesures moins intrusives, par exemple en imposant des conditions en vue de protéger la confidentialité des informations que le pouvoir adjudicateur met à disposition dans le cadre d'une procédure de passation prévue par la présente loi.

En outre, et en conformité avec l'article 346, paragraphe 1^{er}, a), du Traité sur le fonctionnement de l'Union européenne, la présente loi ne s'applique pas aux marchés publics qui ne sont pas par ailleurs exclus en vertu du paragraphe 1^{er} du présent article, dans la mesure où l'application de la présente loi obligerait le Royaume à fournir des informations dont il estimerait la divulgation contraire aux intérêts essentiels de sa sécurité.

De lidstaten van de Europese Unie kunnen dan ook voorzien in beperkingen van die vrijheden wanneer die noodzakelijk zijn voor en evenredig met het vrijwaren van de bij de bepalingen van het Verdrag als legitiem erkende belangen.

De Europese wetgever heeft zelf bepalingen vastgesteld die zulke beperkingen mogelijk maken in het specifieke gebied van de overheidsopdrachten inzake defensie en veiligheid middels de vaststelling van richtlijn 2009/81/EG van het Europees Parlement en de Raad van 13 juli 2009 'betreffende de coördinatie van de procedures voor het plaatsen door aanbestedende diensten van bepaalde opdrachten voor werken, leveringen en diensten op defensie- en veiligheidsgebied, en tot wijziging van Richtlijnen 2004/17/EG en 2004/18/EG', omgezet in Belgisch recht bij de wet van 13 augustus 2011 'inzake overheidsopdrachten en bepaalde opdrachten voor werken, leveringen en diensten op defensie- en veiligheidsgebied'.

Bij die richtlijn hebben de lidstaten, bij wijze van vrijstellingsregels, de mogelijkheid om maatregelen vast te stellen die restrictiever zijn dan die waarin voorzien is in de richtlijn².

Titel 3/1 van de wet van 13 augustus 2011, ingevoegd bij de wet van 17 juni 2016 'inzake overheidsopdrachten', met als opschrift "Op grond van essentiële veiligheidsbelangen of van artikel 346 van het Verdrag betreffende de werking van de Europese Unie uitgesloten opdrachten", bevat een artikel 43/1, dat luidt:

"De Koning kan specifieke plaatsingsregels, controle- en uitvoeringsmodaliteiten van toepassing maken op de in artikel 15, tweede lid, bedoelde overheidsopdrachten."

Artikel 15, tweede lid, van dezelfde wet bepaalt:

"In onderstaande gevallen is echter uitsluitend titel 3/1 van toepassing:

1° indien en voor zover de bescherming van de essentiële veiligheidsbelangen van het Rijk niet kan worden gewaarborgd door minder ingrijpende maatregelen, bijvoorbeeld door eisen te stellen ter bescherming van het vertrouwelijke karakter van de informatie die de aanbestedende overheid overeenkomstig de bepalingen van titel 2 en 3 van deze wet beschikbaar stelt;

2° indien en voor zover de toepassing van de bepalingen van titel 2 en 3 van deze wet het Rijk ertoe zou verplichten informatie ter beschikking te stellen waarvan hij de openbaarmaking in strijd acht met zijn essentiële veiligheidsbelangen;

3° wanneer het plaatsen en de uitvoering van de overheidsopdracht geheim zijn verklaard of overeenkomstig de in het Rijk geldende wettelijke of bestuursrechtelijke bepalingen gepaard moeten gaan met bijzondere veiligheidsmaatregelen, voor zover vastgesteld werd dat de essentiële belangen niet kunnen worden gewaarborgd met minder ingrijpende maatregelen, zoals die bedoeld in de bepaling onder 1°;

4° indien artikel 346 van het Verdrag betreffende de werking van de Europese Unie van toepassing is."

Er kan eveneens verwezen worden naar artikel 33 van de wet van 17 juni 2016, dat het volgende bepaalt:

"§ 1. Deze wet is van toepassing op de overheidsopdrachten op defensie- en veiligheidsgebied, met uitzondering van:

1° de opdrachten waarop de wet defensie en veiligheid van toepassing is;

2° de in artikel 18 van de wet defensie en veiligheid bedoelde opdrachten.

§ 2. Deze wet is niet van toepassing op overheidsopdrachten die niet anderszins op grond van paragraaf 1 zijn uitgesloten, voor zover de bescherming van de essentiële veiligheidsbelangen van het Rijk niet kan worden gewaarborgd door minder ingrijpende maatregelen, bijvoorbeeld door eisen te stellen ter bescherming van het vertrouwelijke karakter van de informatie die de aanbestedende overheid in een plaatsingsprocedure overeenkomstig deze wet beschikbaar stelt.

Voorts is deze wet, overeenkomstig artikel 346, lid 1, a), van het Verdrag betreffende de werking van de Europese Unie, niet van toepassing op overheidsopdrachten die niet anderszins op grond van paragraaf 1 van dit artikel zijn uitgesloten, voor zover de toepassing van deze wet het Rijk ertoe zou verplichten informatie ter beschikking te stellen waarvan hij de openbaarmaking in strijd acht met zijn essentiële veiligheidsbelangen.

§ 3. Lorsque la passation et l'exécution du marché public sont déclarés secrets ou doivent s'accompagner de mesures particulières de sécurité, conformément aux dispositions législatives, réglementaires ou administratives en vigueur dans le Royaume, la présente loi ne s'applique pas, pour autant qu'il est établi que la protection des intérêts essentiels concernés ne peut être garantie par des mesures moins intrusives, telles que celles visées au paragraphe 2, alinéa 1^{er} ».

Ces dispositions légales sont de nature à appuyer l'admissibilité de la restriction prévue par le Roi à l'article 84, alinéa 1^{er}, du projet.

Toutefois, il est rappelé que pour que puissent être admises des restrictions aux libertés et principes protégés par le droit primaire de l'Union, en ce compris au principe de transparence, celles-ci doivent :

– soit trouver leur justification dans des raisons impérieuses d'intérêt général, ces restrictions devant être propres à garantir la réalisation de l'objectif qu'elles poursuivent et ne pouvant pas aller au-delà de ce qui est nécessaire pour l'atteindre³ ;

– soit se fonder sur l'un des motifs d'exception prévus par le TFUE, parmi lesquels son article 346, paragraphe 1, a).

Invitée à justifier la mesure envisagée au regard des principes ainsi rappelés, la déléguée du Ministre a indiqué ce qui suit :

« De opstellers van het ontwerpbesluit menen dat de vereiste van het vestigen van de statutaire zetel in België om in aanmerking te kunnen komen voor geclassificeerde overheidsopdrachten niet strijdig is met vrij verkeer van diensten omdat het gerechtvaardigd is om redenen van algemeen belang, met name de nationale veiligheid, en omdat de maatregel proportioneel is aan het nagestreefde doel.

'Geclassificeerde informatie' is informatie die, in het belang van de nationale veiligheid, wordt beschermd door veiligheidsmaatregelen tegen elke niet-geautoriseerde toegang, niet-geëigende aanwending en verspreiding⁴ ervan. Er staan met andere woorden fundamentele Belgische staatsbelangen⁵ op het spel, die beschermd moeten worden, ongeacht de vorm die deze aannemen en waar deze zich ook bevinden.

Bedrijven, waarvan de maatschappelijke zetel in België is gevestigd, die werken op een geclassificeerde opdracht⁶, moeten in het bezit zijn van een veiligheidsmachtiging voor rechtspersonen. Hiermee wordt na een veiligheidsonderzoek vastgesteld dat de rechtspersoon voldoende garanties biedt inzake geheimhouding, loyaliteit en integriteit van zijn organen en aangestelden die in aanmerking komen om toegang te hebben tot geclassificeerde informatie⁷.

In het kader van risicomanagement, met name het identificeren van dreigingen tegen de fundamentele Belgische staatsbelangen en het wetenschappelijk en economisch potentieel van België, is het logisch en gerechtvaardigd om beveiligingsmaatregelen op te leggen die kunnen weerstaan aan deze dreigingen (zoals buitenlandse beïnvloeding) of deze tot een aanvaardbaar risico kunnen reduceren.

De maatregel, met name de vereiste van het vestigen van de statutaire zetel in België, is bijgevolg gerechtvaardigd omwille van de nationale veiligheid. Het betreft hier een afweging van de belangen. De NVO kan onmogelijk het vereiste veiligheidsonderzoek voeren en het toezicht uitoefenen op het respecteren van de beschermingsmaatregelen indien de vennootschap niet gevestigd is in België. De te onderzoeken inlichtingen van een in het buitenland geregistreerde rechtspersoon zijn niet toegankelijk voor Belgische onderzoeksdiensten. Het onderzoek dient bijgevolg logischerwijze uitgevoerd te worden door de onderzoeksdienst van het thuisland. De resultaten van dit onderzoek, en de eventuele veiligheidsmachtiging die hieruit volgt, zijn te gebruiken in de Belgische procedures (voor zover een bilateraal veiligheidsakkoord hierin voorziet).

De bescherming van geclassificeerde informatie primeert in dit geval op de keuze van statutaire zetel.

De proportionaliteit blijkt duidelijk uit het feit dat dat buitenlandse vennootschappen in de regel niet uitgesloten worden van een geclassificeerde openbare aanbesteding. Indien zij hun statutaire zetel in België vestigen (of een vestigingseenheid in België hebben) kunnen zij wel in aanmerking genomen worden voor een toekenning van een veiligheidsmachtiging (of indien ze beschikken over een buitenlandse veiligheidsmachtiging die wordt erkend door de Nationale Veiligheids-overheid op basis van een veiligheidsakkoord). Verder verwijzen we naar (...) bepalingen⁸ die (...) geven heel duidelijk aan dat ondernemingen die aan deze voorwaarden voldoen, kunnen deelnemen aan openbare aanbestedingen.

Verder bestaat een analoge maatregel in andere EU lidstaten zoals Frankrijk ».

§ 3. Wanneer de plaatsing en de uitvoering van de overheidsopdracht geheim zijn verklaard of, overeenkomstig de in het Rijk geldende wettelijke, reglementaire of administratieve bepalingen, gepaard moeten gaan met bijzondere veiligheidsmaatregelen, is deze wet, niet van toepassing, voor zover vastgesteld werd dat de bescherming van de essentiële belangen niet kan worden gewaarborgd door minder ingrijpende maatregelen, zoals deze bedoeld in paragraaf 2, eerste lid."

Die wettelijke bepalingen kunnen dienen als ondersteuning van de toelaatbaarheid van de beperking waarin de Koning voorziet in artikel 84, eerste lid, van het ontwerp.

Er wordt evenwel aan herinnerd dat opdat beperkingen van de door het primair Unierecht beschermde vrijheden en beginselen, met inbegrip van het transparantiebeginsel, kunnen worden aanvaard, zij:

– ofwel hun rechtvaardiging moeten vinden in dwingende redenen van algemeen belang, waarbij die beperkingen geschikt moeten zijn om de verwezenlijking van het nagestreefde doel te waarborgen en niet verder mogen gaan dan ter bereiking van dat doel noodzakelijk is;³

– ofwel moeten steunen op een van de uitzonderingsgronden in het VWEU, waaronder artikel 346, lid 1, a).

Op de vraag de beoogde maatregel te verantwoorden ten aanzien van de aldus in herinnering gebrachte beginselen, heeft de gemachtigde van de minister op het volgende gewezen:

"De opstellers van het ontwerpbesluit menen dat de vereiste van het vestigen van de statutaire zetel in België om in aanmerking te kunnen komen voor geclassificeerde overheidsopdrachten niet strijdig is met vrij verkeer van diensten omdat het gerechtvaardigd is om redenen van algemeen belang, met name de nationale veiligheid, en omdat de maatregel proportioneel is aan het nagestreefde doel.

'Geclassificeerde informatie' is informatie die, in het belang van de nationale veiligheid, wordt beschermd door veiligheidsmaatregelen tegen elke niet-geautoriseerde toegang, niet-geëigende aanwending en verspreiding⁴ ervan. Er staan met andere woorden fundamentele Belgische staatsbelangen⁵ op het spel, die beschermd moeten worden, ongeacht de vorm die deze aannemen en waar deze zich ook bevinden.

Bedrijven, waarvan de maatschappelijke zetel in België is gevestigd, die werken op een geclassificeerde opdracht⁶, moeten in het bezit zijn van een veiligheidsmachtiging voor rechtspersonen. Hiermee wordt na een veiligheidsonderzoek vastgesteld dat de rechtspersoon voldoende garanties biedt inzake geheimhouding, loyaliteit en integriteit van zijn organen en aangestelden die in aanmerking komen om toegang te hebben tot geclassificeerde informatie⁷.

In het kader van risicomanagement, met name het identificeren van dreigingen tegen de fundamentele Belgische staatsbelangen en het wetenschappelijk en economisch potentieel van België, is het logisch en gerechtvaardigd om beveiligingsmaatregelen op te leggen die kunnen weerstaan aan deze dreigingen (zoals buitenlandse beïnvloeding) of deze tot een aanvaardbaar risico kunnen reduceren.

De maatregel, met name de vereiste van het vestigen van de statutaire zetel in België, is bijgevolg gerechtvaardigd omwille van de nationale veiligheid. Het betreft hier een afweging van de belangen. De NVO kan onmogelijk het vereiste veiligheidsonderzoek voeren en het toezicht uitoefenen op het respecteren van de beschermingsmaatregelen indien de vennootschap niet gevestigd is in België. De te onderzoeken inlichtingen van een in het buitenland geregistreerde rechtspersoon zijn niet toegankelijk voor Belgische onderzoeksdiensten. Het onderzoek dient bijgevolg logischerwijze uitgevoerd te worden door de onderzoeksdienst van het thuisland. De resultaten van dit onderzoek, en de eventuele veiligheidsmachtiging die hieruit volgt, zijn te gebruiken in de Belgische procedures (voor zover een bilateraal veiligheidsakkoord hierin voorziet).

De bescherming van geclassificeerde informatie primeert in dit geval op de keuze van statutaire zetel.

De proportionaliteit blijkt duidelijk uit het feit dat dat buitenlandse vennootschappen in de regel niet uitgesloten worden van een geclassificeerde openbare aanbesteding. Indien zij hun statutaire zetel in België vestigen (of een vestigingseenheid in België hebben) kunnen zij wel in aanmerking genomen worden voor een toekenning van een veiligheidsmachtiging (of indien ze beschikken over een buitenlandse veiligheidsmachtiging die wordt erkend door de Nationale Veiligheids-overheid op basis van een veiligheidsakkoord). Verder verwijzen we naar (...) bepalingen⁸ die (...) geven heel duidelijk aan dat ondernemingen die aan deze voorwaarden voldoen, kunnen deelnemen aan openbare aanbestedingen.

Verder bestaat een analoge maatregel in andere EU lidstaten zoals Frankrijk."

D'après les explications fournies, l'exigence selon laquelle les personnes morales qui entendent soumissionner à des marchés publics impliquant, nécessitant et/ou contenant des informations classifiées de niveau « CONFIDENTIEL » ou « supérieur » doivent avoir un siège social en Belgique répond au souci d'assurer que ces entreprises présentent des garanties suffisantes en termes de confidentialité, de loyauté et d'intégrité de leurs organes, pour pouvoir avoir accès à de telles informations.

D'après la déléguée du Ministre, les personnes morales étrangères pourraient également soumissionner à de tels marchés si elles sont titulaires d'une habilitation de sécurité au motif qu'elles disposent d'un siège statutaire ou d'une unité d'établissement en Belgique. Il en irait de même pour les personnes morales qui disposent d'une habilitation de sécurité étrangère reconnue par l'Autorité nationale de Sécurité en application d'une convention internationale.

Si cette possibilité de faire valoir une habilitation de sécurité délivrée à l'étranger existe effectivement en application de textes existants tels les articles 9, 63, § 2, 4° et 5°, et 76 de l'arrêté royal du 23 janvier 2012 'relatif à la passation des marchés publics et de certains marchés de travaux, de fournitures et de services dans les domaines de la défense et de la sécurité', il n'apparaît pas qu'il en est de même s'agissant des marchés publics dans les domaines autres que ceux cités, domaines pour lesquels la loi du 17 juin 2016 trouve en principe à s'appliquer.

Dans ce cas, l'exclusion des personnes morales qui n'ont pas de siège social situé en Belgique alors qu'elles sont en mesure de répondre à toutes les exigences de sécurité en raison d'une attestation délivrée par une autorité étrangère et reconnue par l'Autorité nationale de Sécurité en vertu d'une convention internationale n'apparaît pas proportionnée.

Il y a lieu de souligner à cet égard qu'en matière nucléaire l'article 8bis de la loi du 11 décembre 1998 'relative à la classification, aux habilitations de sécurité, attestations de sécurité, avis de sécurité et au service public réglementé' habilite le Roi à autoriser les autorités belges désignées par lui à vérifier la validité de l'habilitation de sécurité délivrée par une autorité étrangère, une telle habilitation pouvant être délivrée par les autorités compétentes d'un pays tiers et reconnue par les conventions et traités internationaux qui lient la Belgique en cette matière.

L'article 84, alinéa 1^{er}, du projet sera revu à la lumière de cette observation.

2. La même observation vaut pour l'article 100, 1°, du projet, dont il se déduit que l'adjudicataire dont l'Autorité nationale de Sécurité vérifie s'il dispose d'une habilitation de sécurité ne peut être qu'un adjudicataire « enregistré sur le territoire », ce qui exclut tous les adjudicataires potentiels non enregistrés, compte tenu toutefois de la réponse suivante de la déléguée du Ministre, qui figurera également dans le rapport au Roi :

« Dit hangt samen met artikel 84 van het ontwerpbesluit (...). Enkel rechtspersonen waarvan de statutaire zetel in België is gevestigd, kunnen door de Nationale Veiligheidsoverheid gemachtigd worden in het kader van een Belgische geclassificeerde overheidsopdracht. De Nationale Veiligheidsoverheid heeft geen bevoegdheden (oa. van toezicht) ten aanzien van buitenlandse ondernemingen. De te onderzoeken inlichtingen van een in het buitenland geregistreerde rechtspersoon zijn ook niet toegankelijk voor de Belgische onderzoeksdiensten. Maar buitenlandse ondernemingen zijn op zich niet uitgesloten om deel te nemen aan geclassificeerde openbare aanbestedingen (...) ».

L'article 100, 1°, du projet sera également revu.

3. Invitée par ailleurs à indiquer comment la règle prévue à l'article 85, § 3, du projet, se concilie avec la libre circulation des personnes et des travailleurs au sens du droit de l'Union européenne, la déléguée du Ministre a apporté les éléments de réponse suivants :

« Artikel 85, § 3, van het ontwerpbesluit stelt dat de persoon belast met het dagelijks bestuur van de rechtspersoon in België moet verblijven en er gedomicilieerd zijn. Net zoals bij vraag 25 betreft het hier een afweging van de belangen: enerzijds is het belang van nationale veiligheid en anderzijds de vrijheid van werknemers. De persoon belast met het dagelijks bestuur van de rechtspersoon vormt een 'sleutelfiguur' van de organisatie.

Uit die uitleg volgt dat het vereiste dat zegt dat rechtspersonen die willen inschrijven op overheidsopdrachten die geclassificeerde informatie van het niveau "VERTROUWELIJK" of "hoger" inhouden, vereisen en/of bevatten, een statutaire zetel moeten hebben in België, beantwoordt aan de bezorgdheid dat die ondernemingen voldoende waarborgen bieden inzake geheimhouding, loyauté en integriteit van hun organen om toegang te kunnen hebben tot dergelijke informatie.

Volgens de gemachtigde van de minister zouden buitenlandse rechtspersonen eveneens kunnen inschrijven op dergelijke opdrachten als ze in het bezit zijn van een veiligheidsmachtiging om reden dat ze een statutaire zetel of een vestigingseenheid hebben in België. Hetzelfde zou gelden voor rechtspersonen die beschikken over een met toepassing van een internationale overeenkomst door de Nationale Veiligheidsoverheid erkende buitenlandse veiligheidsmachtiging.

Hoewel die mogelijkheid om zich te kunnen beroepen op een in het buitenland afgegeven veiligheidsmachtiging daadwerkelijk bestaat met toepassing van de bestaande teksten zoals de artikelen 9, 63, § 2, 4° en 5°, en 76 van het koninklijk besluit van 23 januari 2012 'plaatsing overheidsopdrachten en bepaalde opdrachten voor werken, leveringen en diensten op defensie— en veiligheidsgebied', blijkt niet dat dit ook geldt voor overheidsopdrachten in andere dan de gebieden waarnaar verwezen wordt en waarvoor in principe de wet van 17 juni 2016 van toepassing is.

In dat geval blijkt de uitsluiting van rechtspersonen die geen statutaire zetel hebben in België terwijl ze wel kunnen beantwoorden aan alle veiligheidsvereisten op grond van een attest afgegeven door een buitenlandse overheid en erkend door de Nationale Veiligheidsoverheid krachtens een internationale overeenkomst, niet evenredig.

In dat verband dient onderstreept te worden dat wat het nucleaire betreft, de Koning bij artikel 8bis van de wet van 11 december 1998 'betreffende de classificatie, de veiligheidsmachtigingen, veiligheidsattesten, veiligheidsadviezen en de publiek gereguleerde dienst' de door hem aangewezen Belgische overheden kan machtigen om de geldigheid van een door een buitenlandse overheid uitgereikte veiligheidsmachtiging na te gaan, welke machtiging afgeleverd kan worden door de bevoegde overheden van een derde land en erkend kan worden door de internationale overeenkomsten en verdragen die België ter zake binden.

Artikel 84, eerste lid, van het ontwerp moet herzien worden in het licht van die opmerking.

2. Dezelfde opmerking geldt voor artikel 100, 1°, van het ontwerp, waaruit afgeleid kan worden dat de opdrachtnemer van wie de Nationale Veiligheidsoverheid nagaat of hij over een veiligheidsmachtiging beschikt, alleen een "op het grondgebied geregistreerde" opdrachtnemer mag zijn, wat alle potentiële niet geregistreerde opdrachtnemers uitsluit, evenwel rekening houdend met het volgende antwoord van de gemachtigde van de minister, dat eveneens opgenomen moet worden in het verslag aan de Koning:

« Dit hangt samen met artikel 84 van het ontwerpbesluit (...). Enkel rechtspersonen waarvan de statutaire zetel in België is gevestigd, kunnen door de Nationale Veiligheidsoverheid gemachtigd worden in het kader van een Belgische geclassificeerde overheidsopdracht. De Nationale Veiligheidsoverheid heeft geen bevoegdheden (oa. van toezicht) ten aanzien van buitenlandse ondernemingen. De te onderzoeken inlichtingen van een in het buitenland geregistreerde rechtspersoon zijn ook niet toegankelijk voor de Belgische onderzoeksdiensten. Maar buitenlandse ondernemingen zijn op zich niet uitgesloten om deel te nemen aan geclassificeerde openbare aanbestedingen (...) ».

Artikel 100, 1°, van het ontwerp moet eveneens herzien worden.

3. Op de vraag hoe de regel vervat in artikel 85, § 3, van het ontwerp te rijmen valt met het vrij verkeer van personen en werknemers in de zin van het recht van de Europese Unie, heeft de gemachtigde van de minister het volgende antwoord gegeven:

« Artikel 85, § 3, van het ontwerpbesluit stelt dat de persoon belast met het dagelijks bestuur van de rechtspersoon in België moet verblijven en er gedomicilieerd zijn. Net zoals bij vraag 25 betreft het hier een afweging van de belangen: enerzijds is het belang van nationale veiligheid en anderzijds de vrijheid van werknemers. De persoon belast met het dagelijks bestuur van de rechtspersoon vormt een 'sleutelfiguur' van de organisatie.

De Classificatiewet bepaalt dat een veiligheidsmachtiging enkel kan afgeleverd worden nadat een veiligheidsonderzoek is gevoerd (artikel 16 ev. Classificatiewet). Het onderzoek moet gevoerd worden volgens de regels vervat in de Classificatiewet. Indien het onderzoek niet gevoerd kan worden overeenkomstig deze regels dan kan er geen veiligheidsmachtiging afgeleverd worden. Een andere conclusie is contra legem en ondergraaft het veiligheidssysteem. Bovendien is België op grond van veiligheidsakkoorden verplicht ervoor te zorgen dat personen die een veiligheidsmachtiging hebben op een correcte manier gehabiteerd zijn. Wanneer zou blijken dat dit niet het geval zou zijn, dan brengt dit de internationale samenwerking in het gedrang.

Indien een persoon niet in België verblijft gedurende een bepaalde periode kan er geen veiligheidsonderzoek gevoerd worden overeenkomstig de voormelde regels wegens een gebrek aan voldoende informatie ».

Ces éléments de réponse figureront de même dans le rapport au Roi.

II. La réglementation envisagée au regard du principe d'autonomie des compétences

L'article 2, alinéa 1^{er}, du projet, prévoit ce qui suit :

« En application de l'article 1bis, 15°, a) de la loi, les membres du Gouvernement fédéral et des gouvernements des entités fédérées désignent un officier de sécurité au sein de leur cellule stratégique et au moins un officier de sécurité au sein de chaque administration publique relevant de leur autorité, dans laquelle des informations classifiées de niveau 'CONFIDENTIEL' ou supérieur sont utilisées ».

Ce faisant, l'arrêté royal en projet crée des obligations à charge des entités fédérées.

Il va de soi que le mécanisme ainsi envisagé doit respecter l'autonomie des entités fédérées concernées. L'autorité fédérale ne pourrait en effet imposer unilatéralement – par le biais d'un arrêté royal – une collaboration forcée des entités fédérées au système mis en place par le projet en requérant des autorités régionales ou communautaires qu'elles désignent d'office des officiers de sécurité au sein de leurs organes et de leurs administrations. La section de législation a rappelé à de nombreuses reprises qu'imposer des obligations aux entités fédérées est contraire au principe d'autonomie et requiert, en principe, la conclusion d'un accord de coopération⁹. À défaut, l'intervention des entités fédérées ne peut être envisagée que sous l'angle d'une simple faculté.

Interrogée à propos de la compatibilité de la disposition envisagée, dans un projet d'arrêté royal, avec le respect du principe d'autonomie ainsi rappelé, la déléguée du Ministre a notamment précisé ce qui suit :

« Het classificeren, zoals wordt omschreven in de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, veiligheidsattesten, veiligheidsadviezen en de publiek geregelde dienst (Classificatiewet), heeft als doel de belangen te beschermen die zijn opgesomd in artikel 3 van voormelde wet. Deze belangen raken de (bescherming van de) nationale veiligheid, hetgeen een federale kernopdracht is. De preventieve bescherming van de 'fundamentele belangen' van het land behoort tot de exclusieve restbevoegdheid van de federale Staat. De Classificatiewet is van toepassing op éénieder die geclassificeerde informatie aanwendt. Ook als deze informatie wordt aangewend door de gefedereerde entiteiten, moeten de beschermingsmaatregelen (zoals de aanstelling van een veiligheidsofficier), zoals deze door de Classificatiewet worden bepaald, in acht worden genomen. De autonomie van de verschillende beleidsniveaus wordt in acht genomen, de gefedereerde entiteiten worden niet gedwongen om geclassificeerde informatie aan te wenden. Maar indien de gefedereerde entiteiten geclassificeerde informatie aanwenden, worden zij wel geacht om de beschermingsmaatregelen erop toe te passen. De veiligheidsofficier waakt over de naleving van de veiligheidsregels en de beschermingsmaatregelen en speelt een essentiële rol. Het is bijgevolg noodzakelijk dat de gefedereerde entiteiten een veiligheidsofficier aanwijzen opdat zij toegang zouden kunnen hebben tot geclassificeerde informatie en opdat deze geclassificeerde informatie op adequate wijze beschermd wordt. Het aanwijzen van deze veiligheidsofficier behoort tot de bevoegdheid van de gefedereerde entiteiten en niet van de federale overheid. De autonomie van de verschillende niveaus wordt aldus gerespecteerd ».

De Classificatiewet bepaalt dat een veiligheidsmachtiging enkel kan afgeleverd worden nadat een veiligheidsonderzoek is gevoerd (artikel 16 ev. Classificatiewet). Het onderzoek moet gevoerd worden volgens de regels vervat in de Classificatiewet. Indien het onderzoek niet gevoerd kan worden overeenkomstig deze regels dan kan er geen veiligheidsmachtiging afgeleverd worden. Een andere conclusie is contra legem en ondergraaft het veiligheidssysteem. Bovendien is België op grond van veiligheidsakkoorden verplicht ervoor te zorgen dat personen die een veiligheidsmachtiging hebben op een correcte manier gehabiteerd zijn. Wanneer zou blijken dat dit niet het geval zou zijn, dan brengt dit de internationale samenwerking in het gedrang.

Indien een persoon niet in België verblijft gedurende een bepaalde periode kan er geen veiligheidsonderzoek gevoerd worden overeenkomstig de voormelde regels wegens een gebrek aan voldoende informatie.”

Dat antwoord moet ook in het verslag aan de Koning opgenomen worden.

II. De beoogde regelgeving in het licht van het beginsel van de autonome bevoegdheidsuitoefening

Artikel 2, eerste lid, van het ontwerp, luidt als volgt:

“In toepassing van artikel 1bis, 15°, a) van de wet, duiden de leden van de federale Regering en van de deelstatenregeringen een veiligheidsofficier aan binnen hun beleidsceel en ten minste één veiligheidsofficier binnen elk openbaar bestuur dat onder hun gezag ressorteert, waarbinnen geclassificeerde informatie met het beschermingsniveau “VERTROUWELIJK” of hoger wordt aangewend.”

Aldus houdt het ontworpen koninklijk besluit verplichtingen in ten laste van de deelentiteiten.

Het spreekt voor zich dat de aldus beoogde regeling de autonomie van de betrokken deelentiteiten in acht moet nemen. De federale overheid kan de deelentiteiten immers niet eenzijdig – bij wege van een koninklijk besluit – een gedwongen medewerking opleggen aan de regeling die bij het ontwerp wordt ingevoerd, door van de overheden van de gewesten of de gemeenschappen te eisen dat ze ambtshalve veiligheidsofficieren aanstellen bij hun organen en administraties. De afdeling Wetgeving heeft meermaals gesteld dat het opleggen van verplichtingen aan de deelentiteiten in strijd is met het beginsel van de autonomie en in principe vereist dat een samenwerkingsakkoord wordt gesloten⁹. Zonder een dergelijk samenwerkingsakkoord kan het optreden van de deelentiteiten enkel als een mogelijkheid worden opgevat.

Op de vraag of de beoogde bepaling, in een ontwerp van koninklijk besluit, wel verenigbaar is met het aldus in herinnering gebrachte beginsel van autonomie, heeft de gemachtigde van de minister inzonderheid het volgende gesteld:

“Het classificeren, zoals wordt omschreven in de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, veiligheidsattesten, veiligheidsadviezen en de publiek geregelde dienst (Classificatiewet), heeft als doel de belangen te beschermen die zijn opgesomd in artikel 3 van voormelde wet. Deze belangen raken de (bescherming van de) nationale veiligheid, hetgeen een federale kernopdracht is. De preventieve bescherming van de 'fundamentele belangen' van het land behoort tot de exclusieve restbevoegdheid van de federale Staat. De Classificatiewet is van toepassing op éénieder die geclassificeerde informatie aanwendt. Ook als deze informatie wordt aangewend door de gefedereerde entiteiten, moeten de beschermingsmaatregelen (zoals de aanstelling van een veiligheidsofficier), zoals deze door de Classificatiewet worden bepaald, in acht worden genomen. De autonomie van de verschillende beleidsniveaus wordt in acht genomen, de gefedereerde entiteiten worden niet gedwongen om geclassificeerde informatie aan te wenden. Maar indien de gefedereerde entiteiten geclassificeerde informatie aanwenden, worden zij wel geacht om de beschermingsmaatregelen erop toe te passen. De veiligheidsofficier waakt over de naleving van de veiligheidsregels en de beschermingsmaatregelen en speelt een essentiële rol. Het is bijgevolg noodzakelijk dat de gefedereerde entiteiten een veiligheidsofficier aanwijzen opdat zij toegang zouden kunnen hebben tot geclassificeerde informatie en opdat deze geclassificeerde informatie op adequate wijze beschermd wordt. Het aanwijzen van deze veiligheidsofficier behoort tot de bevoegdheid van de gefedereerde entiteiten en niet van de federale overheid. De autonomie van de verschillende niveaus wordt aldus gerespecteerd.”

Elle indique en outre ce qui suit, s'agissant de la référence à l'article 1bis, 15°, a), de la loi du 11 décembre 1998 :

« Het begrip 'openbare besturen' in artikel 1bis, 15°, a), van de Classificatiewet wordt ruim opgevat, zodat ook gefedereerde entiteiten of instanties die een taak van algemeen belang uitvoeren hieronder kunnen vallen, voor zover deze geclassificeerde informatie aanwenden. Rien n'indique dans cette disposition, ni dans les travaux préparatoires une volonté de limiter l'application au Fédéral ».

Compte tenu de la matière réglée, il ne saurait effectivement se déduire de l'article 1bis, 15°, a), de la loi du 11 décembre 1998 que cette dernière ne s'appliquerait qu'aux autorités publiques fédérales. Toutefois, sur la base du principe d'autonomie des diverses entités dont la portée a été rappelée ci-dessus, cette disposition ne peut être lue ou interprétée comme habilitant le Roi à y puiser un fondement juridique pour imposer unilatéralement aux entités fédérées des obligations auxquelles ces dernières n'auraient pas librement consenti puisque, dans le cas d'espèce, l'instrument juridique requis pour les contraindre – l'accord de coopération – fait défaut.

Par conséquent, ce n'est donc que lorsque les entités fédérées choisissent, de leur propre initiative, de s'inscrire dans une démarche de classification de documents à des fins de sécurité dans les matières qui sont de leur ressort que l'article 2, alinéa 1^{er}, du projet est admissible. Il y a en effet alors lieu de considérer que si une entité fédérée s'inscrit volontairement dans une telle démarche de classification pour bénéficier des effets qu'elle induit, elle doit nécessairement se soumettre aux conséquences opérationnelles impliquées par cette classification telles que l'autorité compétente en la matière, à savoir l'État fédéral, les établit, comme l'obligation de désigner un officier de sécurité dans les organes et services concernés, qui est prévue à l'article 2, alinéa 1^{er}, du projet.

C'est donc uniquement dans cette lecture que, sous l'angle des règles de répartition des compétences, l'article 2, alinéa 1^{er}, du projet peut être tenu pour conforme au principe d'autonomie réciproque des diverses entités.

Le rapport au Roi devrait contenir les clarifications requises et l'article 2, alinéa 1^{er}, sera au besoin revu pour rendre compte des nuances qui précèdent.

III. Le pouvoir réglementaire octroyé au Conseil national de Sécurité

1. Les articles 4, 13, 22, 23, 29, 31, 39, 41, 49, 54, 58, 60, 64, 70, 84, alinéa 2, 95, 96 et 98 du projet chargent le Conseil national de Sécurité¹⁰ de prendre des mesures qualifiées de mesures supplémentaires de nature administrative et technique ou d'adopter des directives.

Dans son avis 69.160/4, la section de législation a observé ce qui suit à propos de l'octroi d'un pouvoir réglementaire au Conseil national de Sécurité par la loi :

« L'alinéa 6 confie au Conseil national de sécurité un pouvoir réglementaire consistant en l'identification des 'zones sensibles' au sein desquelles les fournisseurs qualifiés comme étant 'à haut risque' ne pourront ni fournir des éléments de réseaux ni prêter des services.

Dès lors que la Constitution a attribué exclusivement au Roi le pouvoir réglementaire revenant au pouvoir exécutif fédéral et que les pouvoirs doivent être exercés de la manière déterminée par la Constitution, le principe de l'unité du pouvoir réglementaire s'applique et il est par conséquent exclu que le pouvoir réglementaire soit exercé d'une autre manière que celle prescrite par la Constitution. Dès lors, le législateur fédéral ne peut en principe déléguer des compétences normatives qu'au Roi.

Cette règle vaut d'autant plus en l'espèce que le Conseil national de sécurité est un organe stratégique et de coordination, ne disposant pas de pouvoir de décision propre, qui a été créé par le Roi sur la base de l'article 37 de la Constitution¹¹ »¹².

Interrogée à propos de l'octroi d'un pouvoir réglementaire au Conseil national de Sécurité, la déléguée du Ministre a précisé ce qui suit :

« De wetgever heeft de Nationale Veiligheidsraad als coördinerend beleidsorgaan specifiek belast met onder meer de bepaling van het algemeen beleid betreffende de bescherming van gevoelige informatie (artikel 3 van het koninklijk besluit van 22 december 2020 tot oprichting van de Nationale Veiligheidsraad, het Strategisch Comité Inlichtingen en Veiligheid en het Coördinatiecomité Inlichtingen en Veiligheid). De leden van de Raad zijn de Eerste Minister, die de Raad voorzigt, de

Met betrekking tot de verwijzing naar artikel 1bis, 15°, a), van de wet van 11 december 1998 stelt ze voorts het volgende:

“Het begrip 'openbare besturen' in artikel 1bis, 15°, a), van de Classificatiewet wordt ruim opgevat, zodat ook gefedereerde entiteiten of instanties die een taak van algemeen belang uitvoeren hieronder kunnen vallen, voor zover deze geclassificeerde informatie aanwenden. Rien n'indique dans cette disposition, ni dans les travaux préparatoires une volonté de limiter l'application au Fédéral.”

Gelet op de geregelde materie kan uit artikel 1bis, 15°, a), van de wet van 11 december 1998 inderdaad niet worden afgeleid dat die wet enkel van toepassing zou zijn op de federale overheidsinstanties. Op basis van het beginsel van de autonomie van de verschillende deeltentiteiten, waarvan de strekking hiervoor in herinnering is gebracht, kan die bepaling evenwel niet gelezen of geïnterpreteerd worden als zou daarbij de Koning gemachtigd worden om aan die bepaling rechtsgrond te ontlelen om aan de deeltentiteiten op eenzijdige wijze verplichtingen op te leggen waarmee laatstgenoemden niet vrijwillig ingestemd zouden hebben, aangezien in casu het vereiste juridisch instrument om hen daartoe te verplichten – het samenwerkingsakkoord – ontbreekt.

Bijgevolg is artikel 2, eerste lid, van het ontwerp slechts aanvaardbaar indien de deeltentiteiten er uit eigen beweging voor kiezen om ter wille van de veiligheid mee te werken aan een classificatie van documenten in de aangelegenheden waarvoor zij bevoegd zijn. Er is dan immers reden om aan te nemen dat, wanneer een deeltentiteit vrijwillig aan een dergelijke classificatie meewerkt om de voordelen die dat met zich meebrengt te genieten, zij zich automatisch moet schikken naar de operationele gevolgen die deze classificatie met zich meebrengt, die worden vastgesteld door de overheid die ter zake bevoegd is, namelijk de federale Staat, zoals de verplichting waarin artikel 2, eerste lid, van het ontwerp voorziet om een veiligheidsofficier aan te stellen bij de betrokken organen en diensten.

Alleen in die lezing kan artikel 2, eerste lid, van het ontwerp, vanuit het oogpunt van de regels inzake bevoegdheidsverdeling, geacht worden te stroken met het beginsel dat de verschillende deeltentiteiten autonoom zijn ten opzichte van elkaar.

In het verslag aan de Koning zouden de vereiste verduidelijkingen moeten worden opgenomen en artikel 2, eerste lid, moet indien nodig aldus worden herzien dat daarin rekening wordt gehouden met de hiervoor vermelde nuances.

III. De verordenende bevoegdheid toegekend aan de Nationale Veiligheidsraad.

1. Bij de artikelen 4, 13, 22, 23, 29, 31, 39, 41, 49, 54, 58, 60, 64, 70, 84, tweede lid, 95, 96 en 98 van het ontwerp wordt de Nationale Veiligheidsraad¹⁰ ermee belast maatregelen te treffen die aangemerkt worden als bijkomende maatregelen van administratieve en technische aard of om richtlijnen vast te stellen.

In advies 69.160/4 heeft de afdeling Wetgeving het volgende opgemerkt in verband met het bij wet verlenen van een verordenende bevoegdheid aan de Nationale Veiligheidsraad:

“Bij het zesde lid wordt aan de Nationale Veiligheidsraad een verordenende bevoegdheid toegekend, die erin bestaat de 4gevoelige zones4 aan te wijzen waarbinnen de leveranciers die geacht worden 4een hoog risico te vormen4 noch netwerkelementen mogen leveren, noch diensten mogen verrichten.

Doordat de Grondwet de aan de federale uitvoerende macht toekomende verordenende bevoegdheid alleen aan de Koning toegekend heeft en de machten uitgeoefend dienen te worden op de wijze bij de Grondwet bepaald, geldt het beginsel van de eenheid van de verordenende macht, zodat uitgesloten is dat de verordenende macht op een andere wijze uitgeoefend wordt dan door de Grondwet voorgeschreven is. In beginsel mag de federale wetgever derhalve alleen aan de Koning normatieve bevoegdheden delegeren.

Die regel geldt in casu des te meer daar de Nationale Veiligheidsraad een strategisch en coördinerend orgaan is, dat niet over een eigen beslissingsbevoegdheid beschikt en door de Koning opgericht is op grond van artikel 37 van de Grondwet¹¹.”¹²

Op een vraag in verband met het toekennen van een verordenende bevoegdheid aan de Nationale Veiligheidsraad heeft de gemachtigde van de minister het volgende gesteld:

“De wetgever heeft de Nationale Veiligheidsraad als coördinerend beleidsorgaan specifiek belast met onder meer de bepaling van het algemeen beleid betreffende de bescherming van gevoelige informatie (artikel 3 van het koninklijk besluit van 22 december 2020 tot oprichting van de Nationale Veiligheidsraad, het Strategisch Comité Inlichtingen en Veiligheid en het Coördinatiecomité Inlichtingen en Veiligheid). De leden van de Raad zijn de Eerste Minister, die de Raad voorzigt, de

ministers die Justitie, Landsverdediging, Binnenlandse Zaken en Buitenlandse Zaken binnen hun bevoegdheid hebben, en de Vice-eersteministers die geen van deze bevoegdheden hebben (artikel 2 van voormeld koninklijk besluit).

De richtlijnen of aanbevelingen van de Nationale Veiligheidsraad voegen geen nieuwe rechtsregels toe en zijn in die zin niet als 'reglementair' te beschouwen. Deze richtlijnen zijn wél, net zoals de nog steeds bestaande richtlijnen van het vroegere Ministerieel Comité voor Inlichting en Veiligheid van mei 2001, gezaghebbend, gelet op de opdrachten van de Nationale Veiligheidsraad om het algemeen beleid betreffende de bescherming van gevoelige informatie te bepalen. De richtlijnen van de Nationale Veiligheidsraad interpreteren en concretiseren de wet en de beschermingsmaatregelen vastgelegd door het uitvoeringsbesluit, ontwikkelen praktijken, leggen het partnerbeleid vast, ... De richtlijnen zijn in elk geval bindend voor de diensten die onder de ministers ressorteren die in de Nationale Veiligheidsraad zetelen. Omwille van de technische complexiteit en omwille van veiligheidsredenen is het wenselijk om de maatregelen, die door het uitvoeringsbesluit worden vastgelegd, nader uiteen te zetten via richtlijnen van de Nationale Veiligheidsraad. De richtlijnen zorgen ook voor éénvormigheid binnen de instanties die geclassificeerde informatie aanwenden.

Indien beslissingen van de Nationale Veiligheidsraad een reglementair karakter verkrijgen, worden deze in principe bevestigd via een koninklijk of ministerieel besluit, dat voor advies wordt voorgelegd aan de Raad van State en gepubliceerd wordt in het *Belgisch Staatsblad*.

Il apparaît toutefois que les mesures que le Conseil national de Sécurité peut fixer en vertu des articles précités du projet ont un caractère réglementaire et ne peuvent être considérées ni comme de simples directives ne liant que les services relevant des ministres siégeant au sein du Conseil national de Sécurité ni comme des instruments de nature à interpréter et concrétiser les normes contenues dans la loi du 11 décembre 1998 et ses arrêtés d'exécution. Il y a dès lors bien délégation d'un pouvoir réglementaire.

Ce constat est confirmé par le fait que l'article 107 du projet attache au non-respect des mesures fixées par le Conseil national de Sécurité des sanctions administratives. Celui-ci dispose, en effet, qu'en cas de violation des mesures de protection, telles que prévues notamment pas les directives du Conseil national de Sécurité, l'Autorité nationale de Sécurité peut procéder à la suspension immédiate ou au retrait de l'approbation si la gravité de la situation le justifie.

Il est de jurisprudence constante que des délégations telles que celles envisagées par le projet ne peuvent se justifier que pour des raisons pratiques et dans la mesure où elles ont une portée très limitée ou principalement technique et où il peut être considéré que les organismes qui doivent appliquer la réglementation concernée ou la contrôler sont également les mieux placés pour l'élaborer en connaissance de cause¹³.

Compte tenu de la portée des mesures que le Conseil national de Sécurité est habilité à adopter, le dispositif examiné n'est, en l'état, pas admissible et sera revu.

2. Dans le même ordre d'idées, invitée à préciser quelle pourrait être « une autre instance » au sens de l'article 58, alinéa 1^{er}, 2^o, du projet, la déléguée du Ministre a indiqué ce qui suit :

« Dit kan bijvoorbeeld de Koninklijke Militaire School zijn ».

S'agissant des conditions auxquelles cette « autre instance » doit répondre, contenues dans les « directives du Conseil national de Sécurité », la déléguée du Ministre a précisé ce qui suit :

« De richtlijnen van de Nationale Veiligheidsraad hebben geen reglementair karakter, maar hebben tot doel dat de beschermingsmaatregelen in de wet en het uitvoeringsbesluit op éénvormige wijze worden toegepast door (voor de diensten) bindende aanbevelingen te formuleren ».

Dès lors que le Conseil national de Sécurité est habilité à déterminer des conditions, il doit en être déduit que ces « directives » ont un caractère réglementaire, ce qui appelle la même réserve que celle formulée dans l'observation qui précède.

ministers die Justitie, Landsverdediging, Binnenlandse Zaken en Buitenlandse Zaken binnen hun bevoegdheid hebben, en de Vice-eersteministers die geen van deze bevoegdheden hebben (artikel 2 van voormeld koninklijk besluit).

De richtlijnen of aanbevelingen van de Nationale Veiligheidsraad voegen geen nieuwe rechtsregels toe en zijn in die zin niet als 'reglementair' te beschouwen. Deze richtlijnen zijn wél, net zoals de nog steeds bestaande richtlijnen van het vroegere Ministerieel Comité voor Inlichting en Veiligheid van mei 2001, gezaghebbend, gelet op de opdrachten van de Nationale Veiligheidsraad om het algemeen beleid betreffende de bescherming van gevoelige informatie te bepalen. De richtlijnen van de Nationale Veiligheidsraad interpreteren en concretiseren de wet en de beschermingsmaatregelen vastgelegd door het uitvoeringsbesluit, ontwikkelen praktijken, leggen het partnerbeleid vast, ... De richtlijnen zijn in elk geval bindend voor de diensten die onder de ministers ressorteren die in de Nationale Veiligheidsraad zetelen. Omwille van de technische complexiteit en omwille van veiligheidsredenen is het wenselijk om de maatregelen, die door het uitvoeringsbesluit worden vastgelegd, nader uiteen te zetten via richtlijnen van de Nationale Veiligheidsraad. De richtlijnen zorgen ook voor éénvormigheid binnen de instanties die geclassificeerde informatie aanwenden.

Indien beslissingen van de Nationale Veiligheidsraad een reglementair karakter verkrijgen, worden deze in principe bevestigd via een koninklijk of ministerieel besluit, dat voor advies wordt voorgelegd aan de Raad van State en gepubliceerd wordt in het *Belgisch Staatsblad*.

De maatregelen die de Nationale Veiligheidsraad kan treffen krachtens de voornoemde artikelen van het ontwerp blijken evenwel van verordenende aard te zijn en kunnen niet beschouwd worden als gewone richtlijnen die enkel bindend zijn voor de diensten die ressorteren onder de ministers die zitting hebben in de Nationale Veiligheidsraad, noch als instrumenten bedoeld om de normen die vervat zijn in de wet van 11 december 1998 en de uitvoeringsbesluiten ervan te interpreteren en te concretiseren. Er is derhalve wel degelijk sprake van een delegatie van verordenende bevoegdheid.

Die vaststelling wordt bevestigd door het feit dat bij artikel 107 van het ontwerp administratieve sancties worden opgelegd indien de maatregelen vastgesteld door de Nationale Veiligheidsraad niet gerespecteerd worden. In dat artikel wordt immers bepaald dat in geval van schendingen van de beschermingsmaatregelen, zoals bepaald in inzonderheid de richtlijnen van de Nationale Veiligheidsraad, de Nationale Veiligheidsoverheid kan overgaan tot de onmiddellijke schorsing of intrekking van de goedkeuring indien de ernst van de situatie dat rechtvaardigt.

Volgens een vaste adviespraktijk kunnen delegaties zoals die welke beoogd worden in het ontwerp enkel worden gebillijkt op grond van praktische redenen en voor zover zij een zeer beperkte of een hoofdzakelijk technische draagwijdte hebben, en voor zover ervan uitgegaan mag worden dat de instellingen die de betrokken reglementering dienen toe te passen of er toezicht op moeten uitoefenen, ook het best geplaatst zijn om deze met kennis van zaken uit te werken.¹³

Gelet op de draagwijdte van de maatregelen die door de Nationale Veiligheidsraad getroffen mogen worden, is het voorliggende dispositief, zoals het thans is gesteld, niet aanvaardbaar en dient het herzien te worden.

2. In dezelfde gedachtegang heeft de gemachtigde van de minister op het verzoek om een voorbeeld te geven van "een andere instantie" in de zin van artikel 58, eerste lid, 2^o, van het ontwerp, het volgende geantwoord:

"Dit kan bijvoorbeeld de Koninklijke Militaire School zijn."

Wat betreft de voorwaarden waaraan die "andere instantie" moet voldoen en die vervat zijn in de "richtlijnen van de Nationale Veiligheidsraad" heeft de gemachtigde van de minister het volgende gesteld:

"De richtlijnen van de Nationale Veiligheidsraad hebben geen reglementair karakter, maar hebben tot doel dat de beschermingsmaatregelen in de wet en het uitvoeringsbesluit op éénvormige wijze worden toegepast door (voor de diensten) bindende aanbevelingen te formuleren."

Aangezien de Nationale Veiligheidsraad gemachtigd is om voorwaarden vast te stellen, moet daaruit worden afgeleid dat die "richtlijnen" van verordenende aard zijn, hetgeen aanleiding geeft tot hetzelfde voorbehoud als het voorbehoud dat gemaakt is in de voorgaande opmerking.

3. Une observation analogue vaut enfin pour l'article 10 du projet. Celui-ci habilite en effet, outre chaque ministre, chaque fonctionnaire dirigeant ainsi que le chef du Service Général du Renseignement et de la Sécurité des Forces armées en ce qui concerne la Défense, à prescrire des règles d'ordre technique en complément des règles relatives à la procédure pour la classification, la modification du niveau de classification et la déclassification et aux mesures de protection inhérentes à la classification contenues dans l'arrêté en projet. Ici encore, une telle délégation n'est pas admissible dans la mesure où elle confère aux autorités citées un pouvoir réglementaire.

OBSERVATIONS PARTICULIÈRES

PRÉAMBULE

1. À l'alinéa 1^{er}, la déléguée du Ministre a indiqué que la mention de l'article 107, alinéa 2, de la Constitution, relevait de l'erreur matérielle. Partant, elle sera omise.

2. À l'alinéa 2, il convient de mentionner les dispositions précises de la loi du 11 décembre 1998 qui constituent le fondement légal des dispositions du projet, ainsi que les modifications en vigueur qu'elles ont subies¹⁴⁻¹⁵. Ainsi :

- plutôt que viser un « dernier alinéa », il convient de viser les articles 1septies, alinéa 4, 4, alinéa 6, et 17, alinéa 4 ;
- il convient de viser plus précisément l'article 7, § 6, alinéa 2 ;

- la mention de la modification « par la loi du 7 avril 2023 » ne concerne pas les articles 6, alinéa 2, 12, alinéa 2, 17, alinéas 1^{er}, 2 et 4, ainsi que l'article 22, alinéas 1^{er} et 3.

L'auteur du projet s'assurera également de l'exécution complète de la loi du 11 décembre 1998. L'article 7, § 3, alinéa 7, de la loi contient en effet une habilitation au Roi qui ne semble pas mise en œuvre dans l'arrêté en projet. Le cas échéant, l'alinéa 2 du préambule sera complété par cette disposition si le projet venait à être complété sur ce point.

3. Par ailleurs, dans la mesure où le projet modifie l'arrêté royal du 24 mars 2000 'portant exécution de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité' pour ce qui concerne les attestations et avis de sécurité, il convient de viser, à l'alinéa 2 du préambule, les dispositions de la loi du 11 décembre 1998 qui habilitent le Roi à procéder à ces modifications.

4. Le préambule sera complété par un nouvel alinéa visant l'arrêté royal du 24 mars 2000, modifié par le projet.

5. Dès lors que le Comité R intervient en tant qu'Autorité de protection des données pour la matière concernée par le projet, l'alinéa 8 du préambule est superflu et sera omis.

6. L'alinéa relatif à l'avis de la section de législation du Conseil d'État sera déplacé en fin de préambule, en tant que dernier visa.

7. Aux alinéas 5 à 10, les visas relatifs aux formalités préalables obligatoires seront complétés par la date à laquelle celles-ci ont été accomplies.

DISPOSITIF

Aarticle 1^{er}

1. Au 3°, la portée des mots « ou le refus du service » figurant dans le texte en projet n'apparaît pas. Le rapport au Roi devrait en cerner la signification précise.

2. À la question de savoir si le sens des mots « mis en péril » (in gevaar komen) au 4° est identique à celui de « compromission » défini au 3°, la déléguée du Ministre a précisé ce qui suit :

« Bij compromittering zijn de gegevens in gevaar (en niet 'mogelijk in gevaar') gebracht; bij veiligheidsincident is er enkel een regel geschonden (zonder dat het vaststaat dat de gegevens in gevaar gebracht werden). 'In gevaar' zou bijgevolg kunnen worden opgevat als een synoniem voor 'compromittering', maar bij 'veiligheidsincident' ligt de nadruk op 'mogelijk' ».

3. Au 10°, sont définis les « préposés » de « la personne morale », sans que cette dernière notion soit définie.

3. Een soortgelijke opmerking geldt tot slot voor artikel 10 van het ontwerp. Bij dat artikel worden immers elke minister, elke leidend ambtenaar en de chef van de Algemene Dienst Inlichting en Veiligheid van de Krijgsmacht voor wat Defensie betreft, gemachtigd om bijkomende regels van technische aard voor te schrijven naast de regels betreffende de procedure voor classificatie, het wijzigen van een classificatieniveau en de declassificatie, en de beschermingsmaatregelen verbonden aan de classificatie vervat in het ontworpen besluit. Ook hier is een dergelijke delegatie niet aanvaardbaar in zoverre daarmee aan de genoemde overheden een verordenende bevoegdheid wordt toegekend.

BIJZONDERE OPMERKINGEN

AANHEF

1. In verband met het eerste lid heeft de gemachtigde van de minister aangegeven dat de vermelding van artikel 107, tweede lid, van de Grondwet een materiële fout was. Ze moet dan ook weggelaten worden.

2. In het tweede lid dienen de exacte bepalingen vermeld te worden van de wet van 11 december 1998 die rechtsgrond bieden voor de bepalingen van het ontwerp, alsook de nog van kracht zijnde wijzigingen die ze hebben ondergaan.¹⁴⁻¹⁵ Zo:

- dient verwezen te worden naar de artikelen 1septies, vierde lid, 4, zesde lid, en 17, vierde lid, in plaats van naar een "laatste lid";
- dient meer specifiek verwezen te worden naar artikel 7, § 6, tweede lid;

- heeft de vermelding van de wijziging "door de wet van 7 april 2023" geen betrekking op de artikelen 6, tweede lid, 12, tweede lid, 17, eerste, tweede en vierde lid, noch op artikel 22, eerste en derde lid.

De steller van het ontwerp moet er zich eveneens van vergewissen dat de wet van 11 december 1998 volledig ten uitvoer gelegd wordt. Artikel 7, § 3, zevende lid, van de wet bevat immers een machtiging aan de Koning die niet ten uitvoer gelegd lijkt te worden bij het ontwerpbesluit. In voorkomend geval moet het tweede lid van de aanhef aangevuld worden met die bepaling als het ontwerp aangevuld wordt op dat punt.

3. Voor zover het ontwerp strekt tot wijziging van het koninklijk besluit van 24 maart 2000 'tot uitvoering van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen', voor wat de veiligheidsadviezen en -attesten betreft, dient bovendien in het tweede lid van de aanhef verwezen te worden naar de bepalingen van de wet van 11 december 1998 waarbij de Koning gemachtigd wordt om die wijzigingen door te voeren.

4. De aanhef moet aangevuld worden met een nieuw lid waarin verwezen wordt naar het koninklijk besluit van 24 maart 2000, dat bij het ontwerp gewijzigd wordt.

5. Aangezien het Vast Comité I optreedt als Gegevensbeschermingsautoriteit voor de aangelegenheid die behandeld wordt in het ontwerp, is het achtste lid van de aanhef overbodig en moet het weggelaten worden.

6. Het lid betreffende het advies van de afdeling Wetgeving van de Raad van State moet verplaatst worden naar het einde van de aanhef, als laatste aanhefverwijzing.

7. De vijfde tot de tiende aanhefverwijzing, in verband met de verplichte voorafgaande vormvereisten, moeten aangevuld worden met de datum waarop die vormvereisten vervuld zijn.

DISPOSITIEF

Artikel 1

1. Het is niet duidelijk wat de strekking is van de woorden "of ontzegging van dienst" in punt 3° van de ontworpen tekst. In het verslag aan de Koning zou de exacte betekenis ervan toegelicht moeten worden.

2. Op de vraag of de betekenis van de woorden "in gevaar komen" (mis en péril) in punt 4° overeenkomt met die van "compromittering" gedefinieerd in punt 3°, heeft de gemachtigde van de minister het volgende aangegeven:

"Bij compromittering zijn de gegevens in gevaar (en niet 'mogelijk in gevaar') gebracht; bij veiligheidsincident is er enkel een regel geschonden (zonder dat het vaststaat dat de gegevens in gevaar gebracht werden). 'In gevaar' zou bijgevolg kunnen worden opgevat als een synoniem voor 'compromittering', maar bij 'veiligheidsincident' ligt de nadruk op 'mogelijk'."

3. In punt 10° wordt gedefinieerd wie de "aangestelden" zijn van de "rechtspersoon" maar wordt dat laatste begrip niet gedefinieerd.

Sur ce point, la déléguée du Ministre a indiqué ce qui suit :

« Het begrip ‘rechtspersoon’ verwijst naar artikel 1bis, 10°, b), van de Classificatiewet. Het begrip ‘rechtspersoon’ wordt niet gedefinieerd in deze wet. Een definitie van ‘rechtspersoon’ kan worden toegevoegd in het ontwerpbesluit door de opstellers ».

Par sécurité juridique, cette notion de « personne morale » sera précisée dans le projet.

4. De même, la notion d’« entité », dont question au 11°, n’est pas définie. La déléguée du Ministre a indiqué ce qui suit à propos de cette notion :

« ‘Entiteit’ moet hier in de meest ruime zin worden opgevat. Dit kunnen zowel publiekrechtelijke als privaatrechtelijke rechtspersonen zijn, administratieve overheden, ... Het gaat om alle instanties die enkel geclassificeerde informatie van het classificatieniveau ‘BEPERKT’ aanwenden en waarvoor het bijgevolg volstaat om een ‘contactpersoon voor de veiligheid’ te voorzien, die op de loonlijst staat van de entiteit of er contractueel mee verbonden is. Een definitie van ‘entiteit’ kan worden toegevoegd in het ontwerpbesluit door de opstellers ».

Par le même souci de sécurité juridique, cette notion d’« entité » sera définie dans le projet.

Article 6

Le 1° prévoit que la personne de contact pour la sécurité « est un membre du personnel de la personne morale ou la personne contractuellement liée à l’entité ».

Or, la définition donnée à la personne de contact pour la sécurité par l’article 1^{er}, 11°, du projet prévoit déjà que celle-ci est fonctionnaire, membre du personnel ou la personne contractuellement liée à l’entité.

Dès lors qu’il ne correspond pas de manière exacte à la définition de la personne de contact et qu’il est pour le surplus redondant, le 1° sera omis. Il en est d’autant plus ainsi que l’objet de la disposition examinée semble davantage consacré aux missions de la personne de contact qu’à son statut.

Article 12

Parmi les personnes qui, moyennant la possession d’une habilitation de sécurité du niveau de classification correspondante, sont habilitées à classifier, modifier ou déclassifier un niveau de classification « TRÈS SECRET », figurent, au 11°, « le procureur fédéral et les magistrats qu’il délègue à cet effet ».

Dans son avis 61.551/2 donné le 14 juin 2017, la section de législation a observé ce qui suit :

« Dans la mesure où les magistrats, en vertu de l’article 8 de la loi du 11 décembre 1998, ne doivent pas disposer d’une habilitation de sécurité, le Conseil d’État s’interroge quant à la cohérence de l’exigence qu’un magistrat, pour pouvoir être désigné officier de sécurité du Ministère public, doive être titulaire d’une habilitation de sécurité »¹⁶.

Compte tenu de cette observation, il apparaît de même incohérent de prévoir que « le procureur fédéral et les magistrats qu’il délègue à cet effet », visés au 11°, sont habilités à classifier, modifier ou déclassifier un niveau de classification « TRÈS SECRET » à la condition de posséder une habilitation de sécurité du niveau de classification correspondante.

Partant, l’article 12 sera revu de sorte que « le procureur fédéral et les magistrats qu’il délègue à cet effet » ne soient pas soumis à cette condition.

Cette observation vaut pour l’article 44, 2°, du projet, en ce qu’il implique que des magistrats, qui ne doivent pas posséder d’habilitation de sécurité en vertu de l’article 8, § 2, alinéa 1^{er}, de la loi du 11 décembre 1998, ne pourraient pas pénétrer dans une zone sécurisée, sauf à être toujours escortés par une personne habilitée, conformément à l’article 44, 3°, du projet.

Article 18

La version française du 1° sera rédigée de manière identique à la version néerlandaise.

Article 21

1. Invitée à préciser, au regard de la sécurité juridique, la ratio legis de l’alinéa 3, selon lequel « [l]es dispositions de la sous-section 1 ne s’appliquent pas aux documents classifiés en vertu des alinéas [1^{er} et 2], ce qui signifie que l’ensemble des règles relatives au marquage ne doit pas être appliqué à ces documents classifiés de manière collective, de sorte qu’en cas de classification collective, l’on serait confronté à des documents non marqués mais qui seront néanmoins

Wat dat punt betreft, heeft de gemachtigde van de minister het volgende aangegeven:

“Het begrip ‘rechtspersoon’ verwijst naar artikel 1bis, 10°, b), van de Classificatiewet. Het begrip ‘rechtspersoon’ wordt niet gedefinieerd in deze wet. Een definitie van ‘rechtspersoon’ kan worden toegevoegd in het ontwerpbesluit door de opstellers.”

Ter wille van de rechtszekerheid moet het begrip “rechtspersoon” gedefinieerd worden in het ontwerp.

4. Zo wordt ook het begrip “entiteit”, waarvan gewag gemaakt wordt in punt 11°, niet gedefinieerd. De gemachtigde van de minister heeft het volgende aangegeven in verband met dat begrip :

“‘Entiteit’ moet hier in de meest ruime zin worden opgevat. Dit kunnen zowel publiekrechtelijke als privaatrechtelijke rechtspersonen zijn, administratieve overheden, ... Het gaat om alle instanties die enkel geclassificeerde informatie van het classificatieniveau ‘BEPERKT’ aanwenden en waarvoor het bijgevolg volstaat om een ‘contactpersoon voor de veiligheid’ te voorzien, die op de loonlijst staat van de entiteit of er contractueel mee verbonden is. Een definitie van ‘entiteit’ kan worden toegevoegd in het ontwerpbesluit door de opstellers.”

Nog steeds ter wille van de rechtszekerheid moet het begrip “entiteit” gedefinieerd worden in het ontwerp.

Artikel 6

Punt 1° bepaalt dat de contactpersoon voor de veiligheid “de ambtenaar, het personeelslid van of de persoon verbonden aan de entiteit door een contract [is]”.

De definitie van contactpersoon voor de veiligheid die in artikel 1, 11°, van het ontwerp gegeven wordt, bepaalt evenwel al dat het gaat om de ambtenaar, het personeelslid of de persoon verbonden aan de entiteit door een contract.

Aangezien de definitie in punt 1° niet exact overeenkomt met de definitie van contactpersoon en dat punt bovendien overbodig is, moet het weggelaten worden. Dat is nog meer zo daar de strekking van de voorliggende bepaling meer lijkt te gaan om de opdrachten van de contactpersoon dan om zijn statuut.

Artikel 12

Onder de personen die, middels het bezit van een veiligheidsmachtiging van het overeenstemmende classificatieniveau, gemachtigd zijn om een classificatieniveau “ZEER GEHEIM” te classificeren, te wijzigen of te declassificeren, wordt in punt 11° “de federale procureur en de magistraten die hij hiertoe machtigt” vermeld.

In advies 61.551/2 van 14 juni 2017 heeft de afdeling Wetgeving het volgende opgemerkt:

“Aangezien magistraten krachtens artikel 8 van de wet van 11 december 1998 niet over een veiligheidsmachtiging moeten beschikken, vraagt de Raad van State zich af of het logisch is dat vereist wordt dat een magistraat houder moet zijn van een veiligheidsmachtiging om als veiligheidsofficier van het openbaar ministerie aangewezen te kunnen worden.”¹⁶

Rekening houdend met die opmerking blijkt het eveneens incoherent om te bepalen dat “de federale procureur en de magistraten die hij hiertoe machtigt”, genoemd in punt 11°, gemachtigd zijn om een classificatieniveau “ZEER GEHEIM” te classificeren, te wijzigen of te declassificeren op voorwaarde dat ze in het bezit zijn van een veiligheidsmachtiging van het overeenstemmende classificatieniveau.

Artikel 12 moet derhalve aldus herzien worden dat “de federale procureur en de magistraten die hij hiertoe machtigt” niet onderworpen zijn aan die voorwaarde.

Die opmerking geldt voor artikel 44, 2°, van het ontwerp in zoverre het impliceert dat magistraten, die niet in het bezit hoeven te zijn van een veiligheidsmachtiging krachtens artikel 8, § 2, eerste lid, van de wet van 11 december 1998, geen toegang hebben tot een beveiligde zone, behalve als ze telkens begeleid worden door een gemachtigd persoon, overeenkomstig artikel 44, 3°, van het ontwerp.

Artikel 18

De Franse tekst van punt 1° moet gesteld worden op dezelfde wijze als de Nederlandse tekst.

Artikel 21

1. Op de vraag om, ten aanzien van de rechtszekerheid, aan te geven wat de ratio legis is van het derde lid, volgens welk de “bepalingen van onderafdeling 1 (...) niet van toepassing [zijn] op de krachtens [het eerste en het tweede lid] geclassificeerde documenten”, wat betekent dat alle regels in verband met de markering niet collectief toegepast moeten worden op die geclassificeerde documenten, zodanig dat in geval van collectieve classificatie men geconfronteerd zou worden met

classifiés, même si cela n'apparaît pas clairement sur le document en cause, la déléguée du Ministre a indiqué ce qui suit :

« Deze regel staat al in huidige koninklijk besluit van 24 maart 2000 tot uitvoering van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen (artikel 32) en wordt soms toegepast op oude archieffondsen (van vóór de inwerkingtreding van de wet van 11 december 1998), waarvoor het niet aangewezen is omwille van hun kwetsbaarheid/fragiliteit, historische waarde, omvang of technische redenen (oude documenten op microfiches) het document zelf individueel te markeren. Daarbij wordt wel altijd via een schriftelijke beslissing van de overheid van oorsprong aangeduid dat het archieffonds in zijn geheel als ge(de-)classificeerd moet worden beschouwd ».

Ces explications figureront dans le rapport au Roi.

2. À l'alinéa 3, il y a lieu d'écrire « en vertu des alinéas 1^{er} et 2 ».

Article 22

La deuxième phrase, laquelle constitue une répétition de ce qui figure à l'article 1^{er}, 8°, du projet, qui définit le « titulaire », sera omise.

Article 23

1. À l'alinéa 3, il y a lieu d'écrire « distinct du registre visé à l'alinéa 2 ».

2. À l'alinéa 6, il y a lieu d'écrire « Les registres visés aux alinéas 2 et 3 [...] ».

Article 32

La rédaction des alinéas 2 et 3 doit être revue de telle sorte qu'il apparaisse plus clairement que l'entité doit prendre les mesures visant à empêcher la consultation.

La même observation vaut mutatis mutandis pour l'article 41, alinéas 3 et 4.

Articles 33 à 35

Les dispositions de la sous-section 7 concernent principalement la destruction des informations classifiées par le titulaire. Il n'est cependant pas clair si cette destruction est définitive, parce qu'elle concernerait l'information originale transmise par l'autorité d'origine, ou s'il s'agit seulement de la destruction de la copie, l'autorité d'origine en détenant toujours la version originale.

L'article 34, alinéa 2, en particulier, pourrait aussi concerner la destruction définitive de l'information originale par l'autorité d'origine.

Interprétés comme ne concernant que la destruction d'une ou de plusieurs copies des informations classifiées détenues par l'autorité d'origine, les articles 33 à 35 ne posent pas de difficultés.

Interprétés comme concernant la destruction définitive par le titulaire ou par l'autorité d'origine de l'information classifiée originale, les dispositions concernées doivent être articulées avec la loi du 24 juin 1955 'relative aux archives', en particulier l'article 5 de celle-ci qui prévoit que « [l]es autorités visées à l'article 1^{er}, alinéas 1 et 2, ne pourront procéder à la destruction de documents sans avoir obtenu l'autorisation de l'archiviste général du Royaume ou de ses délégués », ainsi qu'avec les articles 132 à 137 de la loi du 30 juillet 2018 'relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel', qui concernent le traitement de données à caractère personnel à des fins historiques, scientifiques ou statistiques dans le cadre de la loi du 11 décembre 1998, et avec les articles 21 et 21/1 de la loi du 30 novembre 1998 'organique des services de renseignement et de sécurité' ¹⁷. La simple mention « sans préjudice de l'article 25 de la loi et de l'article 21 de la loi du 30 novembre 1998 » n'est à cet égard pas suffisante puisque ces dispositions ne prévoient pas le respect de la loi du 24 juin 1955 ou de l'article 21/1 de la loi du 30 novembre 1998 pour toutes les autorités autres que celles visées par la loi du 30 novembre 1998.

Les articles 33 à 35 seront réexaminés à la lumière de cette observation.

niet gemarkeerde documenten die toch geënclassificeerd zullen zijn, zelfs al blijkt dat niet duidelijk op het document in kwestie, heeft de gemachtigde van de minister op het volgende gewezen:

“Deze regel staat al in huidige koninklijk besluit van 24 maart 2000 tot uitvoering van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen (artikel 32) en wordt soms toegepast op oude archieffondsen (van vóór de inwerkingtreding van de wet van 11 december 1998), waarvoor het niet aangewezen is omwille van hun kwetsbaarheid/fragiliteit, historische waarde, omvang of technische redenen (oude documenten op microfiches) het document zelf individueel te markeren. Daarbij wordt wel altijd via een schriftelijke beslissing van de overheid van oorsprong aangeduid dat het archieffonds in zijn geheel als ge(de-)classificeerd moet worden beschouwd.”

Die uitleg moet opgenomen worden in het verslag aan de Koning.

2. In het derde lid schrijve men “krachtens het eerste en het tweede lid”.

Artikel 22

De tweede zin, die een herhaling is van het bepaalde in artikel 1, 8°, van het ontwerp, waarin het begrip “houder” gedefinieerd wordt, moet weggelaten worden.

Artikel 23

1. In het derde lid schrijve men “gescheiden van het register bedoeld in het tweede lid”.

2. In het zesde lid schrijve men “De registers vermeld in het tweede en het derde lid (...)”.

Artikel 32

De tekst van het tweede en het derde lid moet aldus herzien worden dat duidelijker naar voren komt dat de entiteit verplicht is de maatregelen te nemen om het inkijken tegen te gaan.

Dezelfde opmerking geldt mutatis mutandis voor artikel 41, derde en vierde lid.

Artikelen 33 tot 35

De bepalingen van onderafdeling 7 hebben hoofdzakelijk betrekking op de vernietiging van de geënclassificeerde informatie door de houder. Het is evenwel niet duidelijk of die vernietiging definitief is omdat ze alleen betrekking zou hebben op de originele informatie die bezorgd is door de overheid van oorsprong, dan wel of het alleen gaat om de vernietiging van de kopie, waarbij de overheid van oorsprong steeds de originele versie behoudt.

Artikel 34, tweede lid, in het bijzonder, zou ook betrekking kunnen hebben op de definitieve vernietiging van de originele informatie door de overheid van oorsprong.

Als de artikelen 33 tot 35 aldus geïnterpreteerd worden dat ze alleen betrekking hebben op de vernietiging van één of meerdere kopieën van de geënclassificeerde informatie in het bezit van de overheid van oorsprong, leveren ze geen moeilijkheden op.

Als ze aldus geïnterpreteerd worden dat ze betrekking hebben op de definitieve vernietiging van de geënclassificeerde originele informatie door de houder of door de overheid van oorsprong, moeten de bepalingen in kwestie in overeenstemming gebracht worden met de ‘archiefwet’ van 24 juni 1955, in het bijzonder met artikel 5 ervan dat bepaalt dat de “overheden bedoeld in het eerste artikel, leden 1 en 2, (...) geen archiefdocumenten [mogen] vernietigen zonder toestemming van de algemene rijksarchivaris of van diens gemachtigden”, alsook met de artikelen 132 tot 137 van de wet van 30 juli 2018 ‘betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens’, die betrekking hebben op de verwerking van persoonsgegevens voor historische, wetenschappelijke of statistische doeleinden in het kader van de wet van 11 december 1998, en met de artikelen 21 en 21/1 van de organieke wet van 30 november 1998 ‘houdende regeling van de inlichtingen- en veiligheidsdiensten’ ¹⁷. De eenvoudige vermelding “Onverminderd artikel 25 van de wet en artikel 21 van de wet van 30 november 1998” volstaat in dat verband niet aangezien die bepalingen niet strekken tot naleving van de wet van 24 juni 1955 of van artikel 21/1 van de wet van 30 november 1998 voor alle andere overheden dan die bedoeld in de wet van 30 november 1998.

De artikelen 33 tot 35 moeten herzien worden in het licht van die opmerking.

Article 46

À la question de savoir s'il existe un modèle de déclaration de conformité, la déléguée du Ministre a indiqué ce qui suit :

« Deze documenten zullen op de website van de Nationale Veiligheidsoverheid ter beschikking worden gesteld. Dit laat toe om deze documenten snel aan te passen indien nodig ».

La section de législation se demande si ce modèle ne gagnerait pas à être annexé à l'arrêté royal examiné, à l'instar des modèles qui figurent aux annexes 2 à 5 du projet.

Cette observation vaut également pour la déclaration de conformité visée à l'article 50, alinéas 2 et 3, du projet.

Article 48

La disposition examinée s'inscrit dans la section 2 du titre III, chapitre 2, du projet, relative aux zones administratives et sécurisées.

Les articles 42 à 47 du projet sont consacrés à la procédure d'approbation de ces zones.

S'agissant de la zone de sécurité, l'article 47 prévoit que l'Autorité nationale de Sécurité notifie à l'officier de sécurité sa décision concernant l'approbation de la zone au sein de l'installation physique. D'après l'article 48 examiné, tout changement apporté à l'installation physique en question doit être immédiatement signalé à l'Autorité nationale de Sécurité.

Le dispositif reste toutefois en défaut de préciser les conséquences qui s'attachent à ce signalement en manière telle que la question se pose de savoir si l'ensemble de la procédure d'approbation doit à nouveau être appliquée ou non.

Le dispositif sera revu compte tenu de l'observation.

Article 53

1. Dans l'hypothèse où l'Autorité Nationale de Sécurité adopte une décision de refus d'approbation du système de communication et d'information, la déléguée du Ministre a répondu comme suit à propos de la possibilité d'un recours contre ce type de décision :

« Deze beslissing tot weigering van de goedkeuring van een communicatie- en informatiesysteem vormt een administratieve beslissing, waartegen een beroep open staat bij de afdeling bestuursrechtspreek van de Raad van State overeenkomstig artikel 14 van de gecoördineerde wetten op de Raad van State, tenzij de wetgever in de toekomst nog zal beslissen om dit toe te vertrouwen aan een specifiek daartoe opgericht administratief rechtscollege, zoals het Beroepsorgaan inzake veiligheidsmachtigingen, – attesten of – adviezen. Dit is echter niet aan de opstellers van het ontwerpbesluit om te beslissen ».

Cette réponse vaut également pour l'article 61 du projet, en cas de décision de refus d'approbation d'un produit cryptographique, et pour les articles 107 et 111 du projet, pour les cas de suspension (immédiate) ou de retrait de l'approbation.

2. Invitée à justifier la période fort réduite, prévue au paragraphe 2, durant laquelle une demande de renouvellement doit être introduite, la déléguée du Ministre a indiqué ce qui suit :

« – Mbt de geldigheidsduur van de beslissing tot goedkeuring van een communicatie- en informatiesysteem: in de vroegere wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen (artikel 13, 2°) luidde de definitie van veiligheidsmachtiging als volgt: '[...] – een rechtspersoon voldoende garanties biedt inzake de materiële en de technische middelen en de methoden, gebruikt om deze gegevens te beschermen, en inzake [...]'. De goedkeuring van een communicatie- en informatiesysteem maakte bijgevolg deel uit van een veiligheidsmachtiging voor rechtspersonen. De wetgever heeft er in de wet van 7 april 2023 houdende wijziging van de wet van 11 december 1998, betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen voor gekozen om hier een aparte beslissing van te maken (zie artikel 1bis, 10° en artikel 1quater, 6°). De veiligheidsmachtiging wordt volgens het koninklijk besluit van 24 maart 2000 toegestaan voor een periode van maximum vijf jaar (hetgeen dus eveneens korter kon zijn).

In het ontwerpbesluit wordt een geldigheidsduur van maximum drie jaar voorzien voor informatie- en communicatiesystemen (artikel 53, § 2 van het ontwerpbesluit), omwille van de snelle technologische evolutie. Idem voor cryptografische producten (artikel 61 van het ontwerpbesluit).

Artikel 46

Op de vraag of er een model bestaat voor de conformiteitsverklaring heeft de gemachtigde van de minister het volgende aangegeven:

“Deze documenten zullen op de website van de Nationale Veiligheidsoverheid ter beschikking worden gesteld. Dit laat toe om deze documenten snel aan te passen indien nodig.”

De afdeling Wetgeving vraagt zich af of het geen aanbeveling verdient dat model als bijlage te voegen bij het voorliggende koninklijk besluit, naar het voorbeeld van de modellen die opgenomen zijn in de bijlagen 2 tot 5 van het ontwerp.

Die opmerking geldt eveneens voor de conformiteitsverklaring, bedoeld in artikel 50, tweede en derde lid, van het ontwerp.

Artikel 48

De voorliggende bepaling maakt deel uit van afdeling 2 van titel III, hoofdstuk 2, van het ontwerp, in verband met de administratieve en beveiligde zones.

De artikelen 42 tot 47 van het ontwerp zijn gewijd aan de goedkeuringsprocedure met betrekking tot die zones.

Wat de veiligheidszone betreft, bepaalt artikel 47 dat de Nationale Veiligheidsoverheid haar beslissing betreffende de goedkeuring van de beveiligde zone binnen de fysieke installatie ter kennis brengt van de veiligheidsofficier. Luidens het voorliggende artikel 48 dient iedere wijziging aan de fysieke installatie in kwestie onverwijld gemeld te worden aan de Nationale Veiligheidsoverheid.

In het dispositief wordt evenwel niet gepreciseerd wat de gevolgen zijn van die melding zodat de vraag rijst of de hele goedkeuringsprocedure opnieuw toegepast moet worden of niet.

Het dispositief moet herzien worden in het licht van die opmerking.

Artikel 53

1. In het geval dat de Nationale Veiligheidsoverheid een beslissing neemt tot weigering van de goedkeuring van het communicatie- en informatiesysteem, heeft de gemachtigde van de minister het volgende antwoord gegeven in verband met het mogelijk beroep tegen een dergelijke beslissing:

“Deze beslissing tot weigering van de goedkeuring van een communicatie- en informatiesysteem vormt een administratieve beslissing, waartegen een beroep open staat bij de afdeling bestuursrechtspreek van de Raad van State overeenkomstig artikel 14 van de gecoördineerde wetten op de Raad van State, tenzij de wetgever in de toekomst nog zal beslissen om dit toe te vertrouwen aan een specifiek daartoe opgericht administratief rechtscollege, zoals het Beroepsorgaan inzake veiligheidsmachtigingen, – attesten of – adviezen. Dit is echter niet aan de opstellers van het ontwerpbesluit om te beslissen.”

Dat antwoord geldt eveneens voor artikel 61 van het ontwerp, in geval van een beslissing tot weigering van een cryptografisch product, en voor de artikelen 107 en 111 van het ontwerp, voor de gevallen van (onmiddellijke) schorsing of van intrekking van de goedkeuring.

2. Op de vraag om de heel korte, in paragraaf 2 bepaalde periode tijdens welke een vernieuwing aangevraagd kan worden te verantwoorden, heeft de gemachtigde van de minister het volgende aangegeven:

“– Mbt de geldigheidsduur van de beslissing tot goedkeuring van een communicatie- en informatiesysteem: in de vroegere wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen (artikel 13, 2°) luidde de definitie van veiligheidsmachtiging als volgt: '[...] – een rechtspersoon voldoende garanties biedt inzake de materiële en de technische middelen en de methoden, gebruikt om deze gegevens te beschermen, en inzake [...]'. De goedkeuring van een communicatie- en informatiesysteem maakte bijgevolg deel uit van een veiligheidsmachtiging voor rechtspersonen. De wetgever heeft er in de wet van 7 april 2023 houdende wijziging van de wet van 11 december 1998, betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen voor gekozen om hier een aparte beslissing van te maken (zie artikel 1bis, 10° en artikel 1quater, 6°). De veiligheidsmachtiging wordt volgens het koninklijk besluit van 24 maart 2000 toegestaan voor een periode van maximum vijf jaar (hetgeen dus eveneens korter kon zijn).

In het ontwerpbesluit wordt een geldigheidsduur van maximum drie jaar voorzien voor informatie- en communicatiesystemen (artikel 53, § 2 van het ontwerpbesluit), omwille van de snelle technologische evolutie. Idem voor cryptografische producten (artikel 61 van het ontwerpbesluit).

– Mbt de vraag tot hernieuwing van de beslissing tot goedkeuring: een termijn tussen de zes en de zeven maanden vóór het einde van de geldigheidsduur van de beslissing werd door de diensten realistisch geacht. Het kan immers niet de bedoeling zijn dat de aanvraag een dag vóór het einde van de geldigheidsduur van de beslissing wordt aangevraagd en de functionele autoriteit vervolgens zonder homologatie verder werkt met het communicatie- en informatiesysteem. De termijn voor de vraag tot hernieuwing is nieuw en stond nog niet in het huidige koninklijk besluit van 24 maart 2000 ».

Ces éléments de réponse figurent dans le rapport au Roi suggéré dans l'observation préalable n° 2.

Article 59

De l'accord de la déléguée du Ministre, les mots « de niveau « RESTREINT » ou supérieur » seront omis.

Article 60

S'agissant de la compétence donnée au Conseil national de Sécurité de prévoir les cas où l'Autorité nationale de Sécurité peut demander à un autre pays ou une autre instance de procéder à l'évaluation d'un produit cryptographique, la déléguée du Ministre a renvoyé à ses éléments de réponse reproduits dans l'observation générale n° III et a suggéré d'omettre, à l'article 60, les mots « Dans les cas prévus par le Conseil national de Sécurité ».

L'article 60 sera modifié en ce sens.

Article 64

Interrogée à propos du fondement légal de l'article 64, par lequel le Roi impose la possession d'une licence cryptographique, compte tenu de ce que si l'article 7, § 1^{er}, alinéa 2, de la loi du 11 décembre 1998 prévoit certes que « [l]e Roi détermine, par arrêté délibéré en Conseil des ministres, les modalités concernant les procédures d'approbation visées à l'article 1bis, 11°, 12° et 13° », aucun de ces points n'est relatif à une licence cryptographique, la déléguée du Ministre a précisé ce qui suit :

« Het beheer en de verdeling van cryptografisch materiaal is een bevoegdheid van de Nationale Veiligheidsoverheid (artikel 1^{quater}, 8° van de Classificatiewet). Opdat de Nationale Veiligheidsoverheid cryptografisch materiaal kan verdelen aan instanties die dit materiaal wensen te gebruiken voor het versturen van geclassificeerde informatie, is een door de Nationale Veiligheidsoverheid goedgekeurde cryptollicentie nodig. Zoniet zou de werking van de Nationale Veiligheidsoverheid met betrekking tot het beheer en de verdeling van het cryptografisch materiaal ernstig verstoord worden. De wetgever heeft in artikel 1^{ter} van voormelde wet bepaald dat de Nationale Veiligheidsoverheid een veiligheidsoverheid is waarvan de werking en de organisatie bepaald worden door de Koning, bij een besluit vastgesteld in overleg in de Ministerraad. Artikel 64 van het ontwerpbesluit heeft hierop betrekking. Artikel 1^{ter} van voormelde wet wordt ook vermeld in de rechtsgronden die worden opgesomd in de aanhef van het ontwerpbesluit.

Verder stelt artikel 7, § 1 van voormelde wet dat de Koning, bij een besluit vastgesteld na overleg in de Ministerraad, de nadere regels bepaalt van de bescherming en de declassificatie van geclassificeerde informatie. Het bezit van een door de Nationale Veiligheidsoverheid goedgekeurde cryptollicentie is vereist alvorens cryptografisch materiaal aan de bezitter ervan kan worden verdeeld voor het gebruik van geclassificeerde informatie ».

Ces éléments de réponse figureront dans le rapport au Roi dès lors qu'ils permettent de localiser les fondements légaux de la disposition en projet dans les articles 1^{ter} et 7 de la loi du 11 décembre 1998.

Articles 67 et 68

S'agissant de déterminer ce qu'il y a lieu d'entendre par « circonstances exceptionnelles », ainsi que l'indique la déléguée du Ministre, les hypothèses visées à l'article 67, (a) et (b), doivent être comprises comme étant exhaustives. En outre, elle précise que les hypothèses visées au (a) et (b) doivent être cumulativement réunies.

Compte tenu de ces précisions, à l'article 67, les mots « Dans des circonstances exceptionnelles, » seront omis et les mots « les circonstances exceptionnelles suivantes sont cumulativement réunies » seront insérés après le mot « si ».

– Mbt de vraag tot hernieuwing van de beslissing tot goedkeuring: een termijn tussen de zes en de zeven maanden vóór het einde van de geldigheidsduur van de beslissing werd door de diensten realistisch geacht. Het kan immers niet de bedoeling zijn dat de aanvraag een dag vóór het einde van de geldigheidsduur van de beslissing wordt aangevraagd en de functionele autoriteit vervolgens zonder homologatie verder werkt met het communicatie- en informatiesysteem. De termijn voor de vraag tot hernieuwing is nieuw en stond nog niet in het huidige koninklijk besluit van 24 maart 2000.”

Dat antwoord moet in het in de voorafgaande opmerking 2 gesuggereerde verslag aan de Koning opgenomen worden.

Artikel 59

De gemachtigde van de minister is het ermee eens dat de woorden “met het classificatieniveau “BEPERKT” of hoger” weggelaten moeten worden.

Artikel 60

Wat betreft de bevoegdheid die aan de Nationale Veiligheidsraad wordt verleend om te bepalen in welke gevallen de Nationale Veiligheidsoverheid een ander land of een andere instantie kan verzoeken om een evaluatie uit te voeren van een cryptografisch product, heeft de gemachtigde van de minister verwezen naar haar antwoord dat overgenomen is in algemene opmerking nr. III en voorgesteld om de woorden “In de gevallen bepaald door de Nationale Veiligheidsraad” uit artikel 60 weg te laten.

Artikel 60 moet in die zin gewijzigd worden.

Artikel 64

Op de vraag wat de rechtsgrond is voor artikel 64, waarbij de Koning het bezit van een cryptollicentie oplegt, gelet op het feit dat artikel 7, § 1, tweede lid, van de wet van 11 december 1998 weliswaar bepaalt dat “[d]e Koning (...), bij een besluit vastgesteld na overleg in de Ministerraad, de nadere regels betreffende de goedkeuringsprocedures bedoeld in artikel 1bis, 11°, 12° en 13° [bepaalt]”, maar geen van die punten betrekking heeft op een cryptollicentie, heeft de gemachtigde van de minister het volgende geantwoord:

“Het beheer en de verdeling van cryptografisch materiaal is een bevoegdheid van de Nationale Veiligheidsoverheid (artikel 1^{quater}, 8° van de Classificatiewet). Opdat de Nationale Veiligheidsoverheid cryptografisch materiaal kan verdelen aan instanties die dit materiaal wensen te gebruiken voor het versturen van geclassificeerde informatie, is een door de Nationale Veiligheidsoverheid goedgekeurde cryptollicentie nodig. Zo niet zou de werking van de Nationale Veiligheidsoverheid met betrekking tot het beheer en de verdeling van het cryptografisch materiaal ernstig verstoord worden. De wetgever heeft in artikel 1^{ter} van voormelde wet bepaald dat de Nationale Veiligheidsoverheid een veiligheidsoverheid is waarvan de werking en de organisatie bepaald worden door de Koning, bij een besluit vastgesteld in overleg in de Ministerraad. Artikel 64 van het ontwerpbesluit heeft hierop betrekking. Artikel 1^{ter} van voormelde wet wordt ook vermeld in de rechtsgronden die worden opgesomd in de aanhef van het ontwerpbesluit.

Verder stelt artikel 7, § 1 van voormelde wet dat de Koning, bij een besluit vastgesteld na overleg in de Ministerraad, de nadere regels bepaalt van de bescherming en de declassificatie van geclassificeerde informatie. Het bezit van een door de Nationale Veiligheidsoverheid goedgekeurde cryptollicentie is vereist alvorens cryptografisch materiaal aan de bezitter ervan kan worden verdeeld voor het gebruik van geclassificeerde informatie”.

Dat antwoord moet overgenomen worden in het verslag aan de Koning, aangezien op basis daarvan kan worden uitgemaakt dat de rechtsgronden voor de ontworpen bepaling terug te vinden zijn in artikel 1^{ter} en artikel 7 van de wet van 11 december 1998.

Artikelen 67 en 68

Als het er, zoals de gemachtigde van de minister aangeeft, om gaat te bepalen wat verstaan moet worden onder “uitzonderlijke omstandigheden”, moeten de voorwaarden bedoeld in artikel 67, (a) en (b), begrepen worden als zijnde de enige voorwaarden. De gemachtigde van de minister wijst er voorts op dat aan beide voorwaarden bedoeld in (a) en (b) samen voldaan moet worden.

Gelet op die toelichting moeten in artikel 67 de woorden “In uitzonderlijke omstandigheden,” weggelaten worden en de inleidende zin moet als volgt geherformuleerd worden: “Geclassificeerde informatie met het classificatieniveau “BEPERKT” of “VERTROUWELIJK” kan door middel van een voor een lager classificatieniveau goedgekeurd cryptografisch product of zonder versleuteling worden doorgestuurd, wanneer de volgende uitzonderlijke omstandigheden zich tegelijk voordoen.”.

Par ailleurs, à l'article 68, il y a lieu d'écrire « Dans les circonstances exceptionnelles visées à l'article 67 ».

Article 70

Le paragraphe 3 ne déroge qu'au paragraphe 2 du même article ; la disposition sera revue en conséquence.

Article 71

Au paragraphe 1^{er}, à défaut d'être en mesure d'en préciser la portée, le mot « précisément » sera omis.

Article 72

Dans la version française de l'alinéa 1^{er}, il y a lieu de se référer aux documents visés « à l'article 17, alinéa 3, de la loi ».

Article 74

À la question de savoir si l'Autorité nationale de Sécurité doit également se prononcer sur la recevabilité d'une demande d'habilitation de sécurité dans un certain délai, compte tenu de ce que tant l'officier de sécurité (15 jours – article 73) que le service de renseignement et de sécurité (2 à 6 mois selon le niveau de confidentialité, le cas échéant prolongé de 3 mois – article 76) sont tenus par des délais, la déléguée du Ministre a indiqué ce qui suit :

« Neen, een specifieke termijn is niet voorzien voor de controle van de aanvraag. De tekst spreekt van 'onverwijld' dwz zo snel mogelijk (artikel 74 ontwerpbesluit). De beslissing gebeurt gelijktijdig met de overzending van het dossier naar de inlichtingen- en veiligheidsdiensten (de factuur voor de betaling van de retributie wordt dan ook automatisch verzonden). In de praktijk verloopt dit vrij snel, gezien dit normaliter digitaal gebeurt (via het platform HABIL+). Maar de opstellers van het ontwerpbesluit wilden de mogelijkheid behouden om, bijvoorbeeld bij een panne van HABIL+, de overzending manueel te laten verlopen. Er is geen bezwaar om de term 'onverwijld' te vervangen door 'een maand' zoals in artikel 25, tweede lid van het huidige koninklijk besluit van 24 maart 2000 ».

Ces explications gagneront à figurer dans le rapport au Roi dans la mesure où elles éclaireraient le choix de ne pas fixer un tel délai pour l'Autorité nationale de Sécurité.

Article 75

Par sécurité juridique et à l'instar de ce que prévoit l'article 80, alinéa 2, du projet, il convient de se référer à l'article 71, § 2, alinéa 7, qui concerne précisément les cas où la demande est signée « par l'autorité directement concernée ou par la personne qui requiert une habilitation de sécurité ».

Article 76

Interpellée sur le fait que les délais fixés n'apparaissent pas être cohérents avec ceux visés à l'annexe 2 – Note explicative, point 2. c. et interrogée dès lors sur la manière dont les délais de 6, 7 et 10 mois visés dans cette note explicative sont calculés, la déléguée du Ministre a apporté les éléments de réponse suivants :

« Artikel 76 van het ontwerp spreekt over 2 maanden voor het onderzoek voor het niveau vertrouwelijk, 3 maanden voor het niveau geheim en 6 maanden voor het niveau zeer geheim. Deze termijn verwijst enkel naar de duurtijd van het veiligheidsonderzoek door de inlichtingen- en veiligheidsdiensten.

Het doel van de verklarende nota is aan betrokkene uitleg te geven over de aanvraagprocedure inzake de veiligheidsmachtigingen. De termijnen vermeld in de verklarende nota willen betrokkene informeren over de totale vermoedelijke wachttijd.

De aanvraagprocedure voorziet dat de veiligheidsofficier over 15 dagen beschikt om de documenten aan de NVO over te zenden. De NVO heeft ongeveer een maand ('onverwijld') om deze over te zenden naar de inlichtingen- en veiligheidsdiensten. De inlichtingen- en veiligheidsdiensten beschikken over 2, 3 of 6 maanden om hun onderzoek af te ronden. Zodra de Nationale Veiligheidsoverheid de resultaten van het veiligheidsonderzoek heeft ontvangen, heeft ze één maand de tijd om zich over de aanvraag om een veiligheidsmachtiging uit te spreken en haar beslissing aan de veiligheidsofficier over te zenden.

De betrokkene zal dus ongeveer 5 maanden moeten wachten voor een veiligheidsmachtiging van het niveau 'vertrouwelijk', 6 maanden voor het niveau 'geheim' en 9 maanden voor het niveau 'zeer geheim'. De in de bijlage vermelde termijnen moeten bijgevolg aangepast worden door de opstellers van het ontwerp ».

Bovendien schrijve men in artikel 68 "In de in artikel 67 bedoelde uitzonderlijke omstandigheden".

Artikel 70

Paragraaf 3 wijkt enkel af van paragraaf 2 van hetzelfde artikel; de bepaling moet dienovereenkomstig herzien worden.

Artikel 71

In paragraaf 1 moet het woord "nauwkeurig" weggelaten worden, aangezien de strekking ervan niet verduidelijkt kan worden.

Artikel 72

In de Franse tekst van het eerste lid moet verwezen worden naar de "documents visés à l'article 17, alinéa 3, de la loi".

Artikel 74

Op de vraag of de Nationale Veiligheidsoverheid zich eveneens binnen een bepaalde termijn moet uitspreken over de ontvankelijkheid van een aanvraag van een veiligheidsmachtiging, gelet op het feit dat zowel de veiligheidsofficier (15 dagen – artikel 73) als de inlichtingen- en veiligheidsdienst (2 tot 6 maanden naargelang het niveau van vertrouwelijkheid, in voorkomend geval verlengd met 3 maanden – artikel 76) aan termijnen gebonden zijn, heeft de gemachtigde van de minister het volgende geantwoord:

"Neen, een specifieke termijn is niet voorzien voor de controle van de aanvraag. De tekst spreekt van 'onverwijld' dwz zo snel mogelijk (artikel 74 ontwerpbesluit). De beslissing gebeurt gelijktijdig met de overzending van het dossier naar de inlichtingen- en veiligheidsdiensten (de factuur voor de betaling van de retributie wordt dan ook automatisch verzonden). In de praktijk verloopt dit vrij snel, gezien dit normaliter digitaal gebeurt (via het platform HABIL+). Maar de opstellers van het ontwerpbesluit wilden de mogelijkheid behouden om, bijvoorbeeld bij een panne van HABIL+, de overzending manueel te laten verlopen. Er is geen bezwaar om de term 'onverwijld' te vervangen door 'een maand' zoals in artikel 25, tweede lid van het huidige koninklijk besluit van 24 maart 2000."

Het verdient aanbeveling om die toelichtingen op te nemen in het verslag aan de Koning, aangezien ze verduidelijken waarom er niet voor gekozen is om een dergelijke termijn te bepalen voor de Nationale Veiligheidsoverheid.

Artikel 75

Ter wille van de rechtszekerheid en naar het voorbeeld van het bepaalde in artikel 80, tweede lid, van het ontwerp, dient verwezen te worden naar artikel 71, § 2, zevende lid, welke bepaling specifiek de gevallen betreft waarin de aanvraag ondertekend wordt "door de rechtstreeks betrokken overheid of de persoon die een veiligheidsmachtiging behoeft".

Artikel 76

Naar aanleiding van een opmerking over het feit dat er geen samenhang blijkt te bestaan tussen de vastgestelde termijnen en de termijnen bedoeld in bijlage 2 – Toelichting, punt 2.c. en op de vraag hoe bijgevolg de in die toelichting bedoelde termijnen van 6, 7 en 10 maanden berekend worden, heeft de gemachtigde van de minister het volgende geantwoord:

"Artikel 76 van het ontwerp spreekt over 2 maanden voor het onderzoek voor het niveau vertrouwelijk, 3 maanden voor het niveau geheim en 6 maanden voor het niveau zeer geheim. Deze termijn verwijst enkel naar de duurtijd van het veiligheidsonderzoek door de inlichtingen- en veiligheidsdiensten.

Het doel van de verklarende nota is aan betrokkene uitleg te geven over de aanvraagprocedure inzake de veiligheidsmachtigingen. De termijnen vermeld in de verklarende nota willen betrokkene informeren over de totale vermoedelijke wachttijd.

De aanvraagprocedure voorziet dat de veiligheidsofficier over 15 dagen beschikt om de documenten aan de NVO over te zenden. De NVO heeft ongeveer een maand ('onverwijld') om deze over te zenden naar de inlichtingen- en veiligheidsdiensten. De inlichtingen- en veiligheidsdiensten beschikken over 2, 3 of 6 maanden om hun onderzoek af te ronden. Zodra de Nationale Veiligheidsoverheid de resultaten van het veiligheidsonderzoek heeft ontvangen, heeft ze één maand de tijd om zich over de aanvraag om een veiligheidsmachtiging uit te spreken en haar beslissing aan de veiligheidsofficier over te zenden.

De betrokkene zal dus ongeveer 5 maanden moeten wachten voor een veiligheidsmachtiging van het niveau 'vertrouwelijk', 6 maanden voor het niveau 'geheim' en 9 maanden voor het niveau 'zeer geheim'. De in de bijlage vermelde termijnen moeten bijgevolg aangepast worden door de opstellers van het ontwerp."

Il convient toutefois de réitérer les observations suivantes, formulées dans l'avis 29.381/2 donné le 12 juillet 1999 sur un projet devenu l'arrêté royal du 24 mars 2000 'portant exécution de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité', sur les potentielles incohérences entre le dispositif envisagé et la note explicative en annexe :

« 3. Quant au point 3, d., de la note explicative qui fixe certains délais à respecter, ceux-ci doivent être insérés dans le dispositif en projet plutôt que dans une annexe. À cet égard, le Conseil d'État s'interroge sur les délais prévus au point (2) qui se différencient de ceux fixés par l'article 9, point 3, du projet.

Une telle façon de faire peut engendrer la plus grande insécurité juridique, ces délais étant d'autant plus importants qu'ils sont déterminants pour la procédure de recours organisée devant le Comité permanent R en vertu de la loi du 11 décembre 1998 portant création d'un organe de recours en matière d'habilitations de sécurité.

Comme expliqué ci-dessus sous le point 1 les règles essentielles doivent se trouver dans le projet d'arrêté et non dans une note explicative ».

Article 80

Les mots « à l'autorité directement concernée ou » seront insérés entre les mots « sa décision » et les mots « à la personne concernée ».

Article 82

1. À l'alinéa 3, il y a lieu d'écrire « des éléments visés aux alinéas 1^{er} et 2 [...] ».

2. Au même alinéa, la deuxième phrase, qui se borne à rappeler qu'une disposition de la loi du 11 décembre 1998 peut, le cas échéant, s'appliquer, sera omise.

Articles 83 et 84

L'article 83 prévoit que toute personne morale peut être autorisée à accéder à des informations classifiées pour autant que le besoin d'en connaître soit reconnu par l'autorité et que cette personne morale dispose d'une habilitation de sécurité pour les personnes morales.

Quant à l'article 84, alinéa 2, il prévoit que, pour ce qui concerne les marchés publics qui impliquent, nécessitent et/ou contiennent des informations classifiées de niveau « restreint », l'administrateur ICT doit être en possession d'une habilitation de sécurité du niveau fixé par une directive du Conseil national de Sécurité.

Or l'article 8, § 2, alinéa 3, de la loi du 11 décembre 1998 précise que, par dérogation à l'alinéa 1^{er} de la même disposition, une personne ne doit pas être titulaire d'une habilitation de sécurité pour avoir accès aux informations classifiées de niveau restreint.

Dès lors, en ce qu'il vise l'ensemble des informations classifiées, sans prévoir d'exception concernant celles de niveau restreint, l'article 83 du projet n'est pas conforme à l'article 8, § 2, de la loi. Il en est de même en ce qui concerne l'article 84, alinéa 2, en ce qu'il contient l'exigence de détenir une habilitation de sécurité pour ce type d'informations.

Les deux dispositions seront revues à la lumière de cette observation.

Article 87

L'alinéa 2 gagnera à débiter par les mots « En cas de demande recevable, [...] ».

Article 88

L'article examiné dispose que les articles 76 à 78 sont applicables aux demandes d'habilitation de sécurité pour les personnes morales.

L'article 77, applicable aux demandes de personnes morales, renvoie aux annexes 2 à 5 pour ce qui concerne le modèle des documents visés à l'article 17, alinéas 1^{er} et 2, de la loi du 11 décembre 1998. Or, ces annexes apparaissent rédigées spécifiquement pour les demandes d'habilitation de sécurité par des personnes physiques.

De volgende opmerkingen die in advies 29.381/2 van 12 juli 1999 gemaakt zijn over een ontwerp dat geleid heeft tot het koninklijk besluit van 24 maart 2000 'tot uitvoering van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen' dienen evenwel herhaald te worden met betrekking tot de mogelijke inconsistenties tussen het ontworpen dispositief en de toelichting in bijlage:

“3. In punt 3, d., van de verklarende nota worden bepaalde termijnen voorgeschreven. Deze termijnen horen thuis in het dispositief van het ontwerp en niet in een bijlage. In dat verband plaatst de Raad van State vraagtekens bij het feit dat de termijnen in punt (2) verschillen van de termijnen in artikel 9, punt 3, van het ontwerp.

Een dergelijke werkwijze kan tot zeer grote rechtsonzekerheid leiden, waarbij die termijnen des te belangrijker zijn daar ze doorslaggevend zijn voor wie krachtens de wet van 11 december 1998 tot oprichting van een beroepsorgaan inzake veiligheidsmachtigingen beroep wil instellen bij het vast comité I.

Zoals hierboven onder punt 1 is uiteengezet, horen de fundamentele voorschriften in het ontwerpbesluit te staan en niet in een verklarende nota.”

Artikel 80

De woorden “van de rechtstreeks betrokken overheid of” moeten ingevoegd worden tussen de woorden “ter kennis” en de woorden “van de betrokken persoon”.

Artikel 82

1. In het derde lid schrijft men “elementen zoals bedoeld in het eerste en het tweede lid (...)”.

2. In hetzelfde lid moet de tweede zin weggelaten worden. Die zin beperkt zich ertoe in herinnering te brengen dat in voorkomend geval een bepaling van de wet van 11 december 1998 van toepassing kan zijn.

Artikelen 83 en 84

Artikel 83 bepaalt dat iedere rechtspersoon toegang kan krijgen tot geclassificeerde informatie, indien de noodzaak tot kennisname wordt erkend door de overheid en deze rechtspersoon beschikt over een veiligheidsmachtiging voor rechtspersonen.

In artikel 84, tweede lid, wordt dan weer bepaald dat, voor wat betreft overheidsopdrachten die betrekking hebben op geclassificeerde informatie van het niveau “BEPERKT” of deze noodzakelijk maken en/of bevatten, de ICT-beheerder in het bezit moet zijn van een veiligheidsmachtiging waarvan het niveau wordt bepaald door een richtlijn van de Nationale Veiligheidsraad.

In artikel 8, § 2, derde lid, van de wet van 11 december 1998 wordt evenwel gesteld dat, in afwijking van het eerste lid van dezelfde bepaling, een persoon geen houder hoeft te zijn van een veiligheidsmachtiging om toegang te hebben tot geclassificeerde informatie van het niveau BEPERKT.

Doordat artikel 83 van het ontwerp betrekking heeft op alle geclassificeerde informatie zonder in een uitzondering te voorzien voor geclassificeerde informatie van het niveau BEPERKT, is het bijgevolg niet in overeenstemming met artikel 8, § 2, van de wet. Hetzelfde geldt voor artikel 84, tweede lid, doordat die bepaling het vereiste bevat dat men in het bezit moet zijn van een veiligheidsmachtiging voor dat soort van informatie.

Beide bepalingen moeten herzien worden in het licht van die opmerking.

Artikel 87

Het verdient aanbeveling om het begin van het tweede lid als volgt te stellen: “Ingeval de aanvraag ontvankelijk is, wordt de aanvraag om een veiligheidsonderzoek op te starten door de Nationale Veiligheids-overheid (...)”.

Artikel 88

Het voorliggende artikel bepaalt dat de artikelen 76 tot 78 van toepassing zijn op de aanvragen van een veiligheidsmachtiging voor rechtspersonen.

In artikel 77 dat van toepassing is op de aanvragen van rechtspersonen wordt verwezen naar de bijlagen 2 tot 5 voor wat betreft het model van de documenten bedoeld in artikel 17, eerste en tweede lid, van de wet van 11 december 1998. Die bijlagen blijken echter specifiek opgesteld te zijn voor de aanvragen van een veiligheidsmachtiging door natuurlijke personen.

Interrogée quant à l'utilité d'établir des modèles spécifiques pour les personnes morales, la déléguée du Ministre a indiqué ce qui suit :

« Vennootschappen vullen geen basisvragenlijst in, zij verstrekken wel bepaalde gegevens (naam, juridisch statuut, adres, kbo-nummer, aard van de activiteiten, aantal tewerkgestelde personen, omzetcijfer van laatste 5 jaar, aandeelhouders/ vennoten die minstens 20% van de aandelen bezitten) betreffende de rechtspersoon aan de Nationale Veiligheidsoverheid. Zij geven ook geen instemming omdat zij geen persoonsgegevens hebben. Art. 77 verwijst inderdaad naar die bijlagen. Dat moet aangepast worden ».

Le renvoi figurant à l'article 88 sera revu à la lumière de cette observation.

Article 90

L'article examiné prévoit que la décision est notifiée « aux préposés mentionnés à l'article 85, § 1^{er}, alinéa 1^{er}, 3^o ». La déléguée du Ministre a été invitée à préciser si cette disposition a pour effet que des éléments relatifs à la vie privée de certains préposés, collectés lors de l'enquête et figurant, le cas échéant, dans la décision de refus ou d'octroi de l'habilitation de sécurité, seront portés à la connaissance de l'ensemble des préposés de la personne morale, tels que définis à l'article 1^{er}, 10^o, du projet, et, en cas de réponse positive, à justifier en quoi cette règle se concilie avec le principe de protection de la vie privée, en ce compris les données à caractère personnel, garanti notamment par l'article 22 de la Constitution. Elle a apporté les éléments de réponse suivants :

« In artikel 90 van het ontwerpbesluit gaat het over de kennisgeving van de beslissing inzake de veiligheidsmachtiging van de rechtspersoon en niet over de veiligheidsmachtiging van de bestuurders. De kennisgeving dient gemotiveerd te zijn.

De kennisgeving zal aangeven of de rechtspersoon voldoet aan de voorwaarden geheimhouding, loyaliteit en integriteit. Nooit zullen persoonsgegevens van een bepaalde bestuurder gedeeld worden met andere personen. Wanneer de NVO persoonsgegevens verwerkt in de uitoefening van de Classificatiewet is zij gebonden aan de regels vervat in titel 3, ondertitel 3 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens. Het delen van persoonsgegevens zou strijdig zijn met de fundamentele beginselen van gegevensverwerking, in casu de minimale verwerking en het beginsel van de doelbinding.

De gegevens van vennootschappen maken geen persoonsgegevens uit. Er worden nooit gegevens betreffende het privé-leven van de aangestelden meegedeeld in de beslissing betreffende de veiligheidsmachtiging van de rechtspersoon. Dit vormt een aparte beslissing ».

Ces éléments de réponse figureront dans le rapport au Roi.

Article 92

Invitée à indiquer pour quelle raison une enquête de sécurité complémentaire n'est pas prévue pour les personnes morales, à l'instar de ce qui est prévu pour les personnes physiques à l'article 82 du projet, d'autant plus que cette enquête complémentaire pourrait être justifiée par les éléments communiqués par l'officier de sécurité à l'Autorité nationale de Sécurité sur la base de l'article 92, la déléguée du Ministre a admis que « [d]ezelfde regeling kan inderdaad ook voorzien worden voor rechtspersonen ».

Le projet sera dès lors complété en ce sens.

Article 93

La correspondance entre la version française et la version néerlandaise de l'alinéa 2 du projet sera assurée ¹⁸.

Article 100

Aux 1^o, 3^o et 4^o, une virgule sera chaque fois insérée après le mot « précontractuel ».

Article 102

Interrogée à propos de l'application de la règle prévue, soit la restitution des informations classifiées dans les 15 jours de la décision de non-sélection, en cas de recours contre cette décision de non-sélection, compte tenu de ce que pourrait s'avérer contraire au droit effectif au recours garanti par l'article 13 de la Convention européenne des droits de l'homme, le fait que le candidat non retenu n'a pas le droit de conserver ces informations classifiées dans le cadre de la procédure de recours qu'il introduit (pièces à l'appui de son recours, éléments d'appréciation du bien-fondé de celui-ci), la déléguée du Ministre a

Op de vraag wat het nut is van het opstellen van specifieke modellen voor rechtspersonen heeft de gemachtigde van de minister het volgende geantwoord:

“Vennootschappen vullen geen basisvragenlijst in, zij verstrekken wel bepaalde gegevens (naam, juridisch statuut, adres, kbo-nummer, aard van de activiteiten, aantal tewerkgestelde personen, omzetcijfer van laatste 5 jaar, aandeelhouders/vennoten die minstens 20% van de aandelen bezitten) betreffende de rechtspersoon aan de Nationale Veiligheidsoverheid. Zij geven ook geen instemming omdat zij geen persoonsgegevens hebben. Art. 77 verwijst inderdaad naar die bijlagen. Dat moet aangepast worden.”

De verwijzing in artikel 88 moet herzien worden in het licht van die opmerking.

Artikel 90

Het voorliggende artikel bepaalt dat de beslissing ter kennis gebracht wordt “aan de aangestelden vermeld in artikel 85, § 1, eerste lid, 3^o”. De gemachtigde van de minister werd verzocht te verduidelijken of die bepaling tot gevolg heeft dat van de gegevens betreffende het privéleven van sommige aangestelden, verzameld tijdens het onderzoek en, in voorkomend geval, opgenomen in de beslissing tot weigering of tot toekenning van de veiligheidsmachtiging, kennis gegeven moet worden aan alle aangestelden van de rechtspersoon, zoals die in artikel 1, 10^o, van het ontwerp omschreven worden, en in geval van een bevestigend antwoord, aan te tonen in welk opzicht die regel verenigbaar is met het beginsel van de bescherming van de persoonlijke levenssfeer, en dus van de persoonsgegevens, dat onder meer door artikel 22 van de Grondwet gewaarborgd wordt. De gemachtigde van de minister heeft het volgende geantwoord:

“In artikel 90 van het ontwerpbesluit gaat het over de kennisgeving van de beslissing inzake de veiligheidsmachtiging van de rechtspersoon en niet over de veiligheidsmachtiging van de bestuurders. De kennisgeving dient gemotiveerd te zijn.

De kennisgeving zal aangeven of de rechtspersoon voldoet aan de voorwaarden geheimhouding, loyaliteit en integriteit. Nooit zullen persoonsgegevens van een bepaalde bestuurder gedeeld worden met andere personen. Wanneer de NVO persoonsgegevens verwerkt in de uitoefening van de Classificatiewet is zij gebonden aan de regels vervat in titel 3, ondertitel 3 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens. Het delen van persoonsgegevens zou strijdig zijn met de fundamentele beginselen van gegevensverwerking, in casu de minimale verwerking en het beginsel van de doelbinding.

De gegevens van vennootschappen maken geen persoonsgegevens uit. Er worden nooit gegevens betreffende het privé-leven van de aangestelden meegedeeld in de beslissing betreffende de veiligheidsmachtiging van de rechtspersoon. Dit vormt een aparte beslissing.”

Dat antwoord moet in het verslag aan de Koning opgenomen worden.

Artikel 92

Naar aanleiding van de vraag waarom, naar het voorbeeld van wat artikel 82 van het ontwerp bepaalt voor natuurlijke personen, niet voorzien wordt in een tussentijds veiligheidsonderzoek voor rechtspersonen, temeer daar dit tussentijds onderzoek verantwoord zou kunnen worden door de gegevens die op basis van artikel 92 door de veiligheidsofficier aan de Nationale Veiligheidsoverheid meegedeeld worden, heeft de gemachtigde van de minister toegegeven dat “[d]ezelfde regeling (...) inderdaad ook voorzien [kan] worden voor rechtspersonen”.

Het ontwerp moet bijgevolg in die zin aangevuld worden.

Artikel 93

Er moet voor overeenstemming gezorgd worden tussen de Nederlandse en de Franse tekst van het tweede lid van het ontwerp.¹⁸

Artikel 100

In de bepalingen onder 1^o, 3^o en 4^o moet telkens een komma geplaatst worden vóór het woord “beschikken”.

Artikel 102

Op een vraag in verband met de toepassing van de ontworpen regel, die erin bestaat dat de geclassificeerde informatie binnen de 15 dagen na de beslissing tot niet-selectie teruggestuurd moet worden, ingeval beroep ingesteld wordt tegen die beslissing tot niet-selectie, in het licht van de vaststelling dat zou kunnen blijken dat het in strijd is met het bij artikel 13 van het Europees Verdrag voor de rechten van de mens gewaarborgde recht op daadwerkelijke rechtshulp dat de niet-geselecteerde kandidaat niet het recht heeft om die geclassificeerde informatie bij te houden in het kader van de beroepsprocedure die hij

précisé ce qui suit :

« De ter beschikking gestelde geclassificeerde informatie is enkel nodig om de overheidsopdracht te kunnen uitvoeren. Toegang tot geclassificeerde informatie is afhankelijk van twee voorwaarden die cumulatief vervuld dienen te zijn. Deze zijn het hebben van een overeenstemmende veiligheidsmachtiging en de vereiste 'need to know' hebben. Indien de vennootschap niet geselecteerd werd, dan beschikt zij niet over de vereiste 'need to know' om kennis te kunnen nemen van de geclassificeerde informatie.

Er zal echter door de opstellers van het ontwerpbesluit een bepaling toegevoegd worden die de niet weerhouden kandidaat in staat stelt om zijn rechten uit te oefenen in het kader van een beroepsprocedure ».

Le projet sera utilement complété de la manière suggérée par la déléguée.

Article 104

À l'alinéa 2, dans la version française, le mot « recommandation » sera remplacé par le mot « proposition » afin de mieux correspondre à la version néerlandaise.

Articles 112 à 114 (titre IV)

Interrogée à propos du fondement légal qui habilite le Roi à prévoir des dispositions relatives à des informations non classifiées et, le cas échéant, à y apposer la mention « SENSIBLE NON CLASSIFIÉ », la déléguée du Ministre a indiqué ce qui suit :

« Titel IV spreekt inderdaad over niet geclassificeerde gegevens. Deze bepalingen zijn echter een actualisatie van het artikel 20 van het huidige KB dat handelt over 'beperkte verspreiding'. De opstellers wensen de markering 'beperkte verspreiding' wel degelijk te behouden maar niet de benaming daar dit verwarrend wordt geacht met het classificatieniveau 'BEPERKT'. De nieuwe benaming 'gevoelig niet geclassificeerd' is overgenomen uit NAVO documenten. Voor de duidelijkheid en de continuïteit werd geopteerd om de behandeling van "gevoelig niet geclassificeerd" in dit ontwerpbesluit behouden.

'Gevoelig niet geclassificeerd' is geen classificatieniveau. De beginselen van openbaarheid van bestuur zijn van toepassing op de documenten die deze markering dragen ».

Si le titre IV contient en effet des dispositions actualisant l'article 20 de l'arrêté royal du 24 mars 2000 qui prévoit une possibilité de « diffusion restreinte » de documents non classifiés, la section de législation ne distingue pas, dans la loi du 11 décembre 1998, le fondement juridique de celles-ci.

L'auteur du projet précisera quel est ce fondement juridique au préambule de l'arrêté en projet. À défaut, ce titre IV sera omis.

Article 113

Si cet article est maintenu ¹⁹, dès lors que l'alinéa 3 prévoit l'hypothèse de documents rédigés en anglais, à l'alinéa 4, il convient de prévoir les hypothèses où les documents sont rédigés dans une autre langue que le français, le néerlandais, l'allemand ou l'anglais.

Article 114

Dans la mesure où l'article examiné se borne à rappeler que des documents peuvent être soumis à des règles relatives au secret professionnel ou à une obligation de secret en vertu de la législation applicable, ou à des règles fixées par des dispositions contractuelles, il apparaît sans portée et sera omis.

Articles 115 à 119 (titre V)

Dès lors que le titre V contient des dispositions modificatives ou abrogatoires de l'arrêté royal du 24 mars 2000, ce titre sera intitulé « Modifications de l'arrêté royal du 24 mars 2000 portant exécution de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité ».

Par ailleurs, l'article 123 du projet, qui abroge la plupart des dispositions de cet arrêté royal et détermine lesquelles sont encore applicables, sera inséré dans ce titre V.

instelt (stukken tot staving van zijn beroep, elementen tot beoordeling van de gegrondheid van dat beroep) heeft de gemachtigde van de minister het volgende geantwoord:

“De ter beschikking gestelde geclassificeerde informatie is enkel nodig om de overheidsopdracht te kunnen uitvoeren. Toegang tot geclassificeerde informatie is afhankelijk van twee voorwaarden die cumulatief vervuld dienen te zijn. Deze zijn het hebben van een overeenstemmende veiligheidsmachtiging en de vereiste 'need to know' hebben. Indien de vennootschap niet geselecteerd werd, dan beschikt zij niet over de vereiste 'need to know' om kennis te kunnen nemen van de geclassificeerde informatie.

Er zal echter door de opstellers van het ontwerpbesluit een bepaling toegevoegd worden die de niet weerhouden kandidaat in staat stelt om zijn rechten uit te oefenen in het kader van een beroepsprocedure.”

Het verdient aanbeveling om het ontwerp aan te vullen op de manier die de gemachtigde van de minister heeft voorgesteld.

Artikel 104

Voor een betere overeenstemming met de Nederlandse tekst moet in het tweede lid van de Franse tekst het woord “recommandation” vervangen worden door het woord “proposition”.

Artikelen 112 tot 114 (titel IV)

Op een vraag over de rechtsgrond die de Koning ertoe machtigt om te voorzien in bepalingen betreffende niet-geclassificeerde informatie en om die informatie, in voorkomend geval, te voorzien van de vermelding “GEVOELIG NIET-GECLASSIFICEERD” heeft de gemachtigde van de minister het volgende geantwoord:

“Titel IV spreekt inderdaad over niet geclassificeerde gegevens. Deze bepalingen zijn echter een actualisatie van het artikel 20 van het huidige KB dat handelt over 'beperkte verspreiding'. De opstellers wensen de markering 'beperkte verspreiding' wel degelijk te behouden maar niet de benaming daar dit verwarrend wordt geacht met het classificatieniveau 'BEPERKT'. De nieuwe benaming 'gevoelig niet geclassificeerd' is overgenomen uit NAVO documenten. Voor de duidelijkheid en de continuïteit werd geopteerd om de behandeling van "gevoelig niet geclassificeerd" in dit ontwerpbesluit behouden.

'Gevoelig niet geclassificeerd' is geen classificatieniveau. De beginselen van openbaarheid van bestuur zijn van toepassing op de documenten die deze markering dragen.”

Hoewel titel IV inderdaad bepalingen bevat die een actualisatie zijn van artikel 20 van het koninklijk besluit van 24 maart 2002 dat voorziet in een mogelijkheid tot “beperkte verspreiding” van niet-geclassificeerde documenten, vindt de afdeling Wetgeving in de wet van 11 december 1998 geen rechtsgrond voor die bepalingen.

De steller van het ontwerp moet in de aanhef van het ontworpen besluit aangeven wat die rechtsgrond vormt. Zo niet, moet die titel IV weggelaten worden.

Artikel 113

Ook al wordt dit artikel behouden,¹⁹ doordat het derde lid in de mogelijkheid voorziet van in het Engels opgestelde documenten, dienen in het vierde lid de gevallen bepaald te worden waarin de documenten in een andere taal dan het Frans, het Nederlands, het Duits of het Engels opgesteld zijn.

Artikel 114

In zoverre het voorliggende artikel zich ertoe beperkt in herinnering te brengen dat documenten krachtens de toepasselijke wetgeving onder de regels inzake het beroepsgeheim of de geheimhoudingsverplichting kunnen vallen, of onder in contractuele bepalingen vastgelegde regels, blijkt het geen draagwijdte te hebben en moet het weggelaten worden.

Artikelen 115 tot 119 (titel V)

Aangezien titel V bepalingen bevat tot wijziging of tot opheffing van het koninklijk besluit van 24 maart 2000, moet het opschrift van die titel als volgt luiden: “Wijzigingen van het koninklijk besluit van 24 maart 2000 tot uitvoering van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen”.

Voorts moet artikel 123 van het ontwerp waarbij de meeste bepalingen van dat koninklijk besluit opgeheven worden en waarin bepaald wordt welke bepalingen nog van toepassing zijn, ingevoegd worden in die titel V.

Ce faisant, dans un but de sécurité juridique, l'auteur du projet s'assurera de la bonne articulation entre l'article 117 du projet, qui abroge l'article 30^{quater} de l'arrêté royal du 24 mars 2000, et l'article 123, lequel prévoit de manière contradictoire que l'arrêté royal du 24 mars 2000 est abrogé « à l'exception [...] du chapitre IIIbis qui comprend les articles 30bis à 30sexies [...] », ce qui laisse entendre que l'article 30^{quater} n'est pas abrogé.

Article 120

1. Dans le texte français, à l'alinéa 2, il y a lieu d'écrire « mais avant l'entrée en vigueur du présent arrêté [...] ».

2. Au même alinéa, il conviendra de corriger la référence à « l'article 18, alinéa 2 ou 3 » dès lors que s'il s'agit bien d'une référence à l'article 18 de l'arrêté royal examiné, celui-ci ne comporte qu'un seul alinéa.

Article 121

La déléguée du Ministre a justifié comme suit l'entrée en vigueur du projet prévue « le lendemain de sa publication au *Moniteur belge* » :

« Het ontwerpbesluit dient zo snel mogelijk in werking te treden. Bepaalde bepalingen van de Classificatiewet - zoals de bepalingen inzake BEPERKT - kunnen heden nog niet toegepast worden omdat het ontwerpbesluit nog niet in werking is getreden. Dit zorgt voor praktische moeilijkheden bij de toepassing van de Classificatiewet. Tien bijkomende dagen wachten heeft geen zin ».

Article 122

Il n'y a pas lieu de mentionner les mots « et secrétaires d'État »²⁰.

Le greffier,
Béatrice DRAPIER

Le président,
Patrick RONVAUX

Notes

* Par un courriel du 17 mai 2024.

1 Le Comité permanent R agit, pour la matière concernée par le projet, en tant qu'Autorité de protection des données.

2 Voir, à ce propos, les extraits suivants du préambule de la directive 2009/81/CE :

« (16) Le traité, à ses articles 30, 45, 46, 55 et 296, prévoit des exceptions spécifiques à l'application des principes qu'il édicte et, par conséquent, à l'application du droit qui en est dérivé. Il s'ensuit qu'aucune disposition de la présente directive ne devrait interdire d'imposer ou d'appliquer les mesures qui se révéleraient nécessaires à la sauvegarde des intérêts reconnus comme légitimes par ces dispositions du traité.

Cela signifie notamment que la passation de marchés qui relèvent du champ d'application de la présente directive peut en être exemptée si cela est justifié pour des raisons de sécurité publique ou nécessaire pour la protection des intérêts essentiels de la sécurité d'un État membre. Cela peut être le cas pour des marchés relevant à la fois de la défense et de la sécurité qui requièrent un tel niveau d'exigence en matière de sécurité d'approvisionnement ou dont la confidentialité et/ou l'importance pour la souveraineté nationale sont telles que même les dispositions spécifiques de la présente directive ne seraient pas suffisantes pour sauvegarder des intérêts essentiels de sécurité des États membres, dont la définition relève de la seule compétence des États membres.

(17) Toutefois, conformément à la jurisprudence de la Cour de justice des Communautés européennes, il convient d'interpréter la possibilité de recourir à de telles dérogations de manière à ne pas étendre leurs effets au-delà de ce qui est strictement nécessaire pour la protection des intérêts légitimes que ces articles permettent de sauvegarder. La non-application de la présente directive doit donc à la fois être proportionnée aux buts poursuivis et perturber le moins possible la libre circulation des marchandises et la libre prestation de services.

(18) [...] [D]ans le contexte spécifique des marchés de la défense et de la sécurité, les États membres conservent le pouvoir de décider si oui ou non leurs pouvoirs adjudicateurs ou entités adjudicatrices peuvent autoriser des agents économiques de pays tiers à participer aux procédures de passation des marchés [...].

(19) [...]

(20) Les marchés de défense et de sécurité contiennent souvent des informations classifiées que les dispositions législatives, réglementaires ou administratives en vigueur dans l'État membre concerné imposent, pour des raisons de sécurité, de protéger contre un accès non autorisé. Dans le domaine militaire, il existe dans les États membres des systèmes de classification de ces informations à des fins militaires. Cependant, dans le domaine de la sécurité non militaire, la pratique des États membres est plus variée lorsque d'autres informations doivent

Zodoende moet de steller van het ontwerp zich, ter wille van de rechtszekerheid, vergewissen van de goede samenhang tussen artikel 117 van het ontwerp, waarbij artikel 30^{quater} van het koninklijk besluit van 24 maart 2000 opgeheven wordt, en artikel 123 dat op tegenstrijdige wijze bepaalt dat het koninklijk besluit van 24 maart 2000 opgeheven wordt "met uitzondering van (...) hoofdstuk IIIbis dat de artikelen 30bis tot en met 30sexies omvat (...)", wat de indruk wekt dat artikel 30^{quater} niet opgeheven wordt.

Artikel 120

1. In het tweede lid van de Franse tekst schrijve men "mais avant l'entrée en vigueur du présent arrêté (...)".

2. In hetzelfde lid dient de verwijzing naar "artikel 18, tweede of derde lid" gecorrigeerd te worden, in de veronderstelling dat het wel degelijk gaat om een verwijzing naar artikel 18 van het voorliggende koninklijk besluit, dat slechts één lid omvat.

Artikel 121

De gemachtigde van de minister heeft de volgende verantwoording gegeven voor het feit dat het ontwerp in werking treedt "de dag volgend op de bekendmaking ervan in het *Belgisch Staatsblad*" :

"Het ontwerpbesluit dient zo snel mogelijk in werking te treden. Bepaalde bepalingen van de Classificatiewet - zoals de bepalingen inzake BEPERKT - kunnen heden nog niet toegepast worden omdat het ontwerpbesluit nog niet in werking is getreden. Dit zorgt voor praktische moeilijkheden bij de toepassing van de Classificatiewet. Tien bijkomende dagen wachten heeft geen zin."

Artikel 122

De woorden "en Staatssecretarissen" moeten niet vermeld worden.²⁰

De griffier,
Béatrice Drapier

De voorzitter,
Patrick Ronvaux

Nota's

* Bij e-mail van 17 mei 2024.

1 Wat de in het ontwerp behandelde aangelegenheid betreft, treedt het Vat Comité I op als Gegevensbeschermingsautoriteit.

2 Zie in dat verband de volgende uittreksels uit de preambule van richtlijn 2009/81/EG:

"(16) De artikelen 30, 45, 46, 55 en 296 van het Verdrag voorzien in specifieke uitzonderingen op de toepassing van de Verdragsbeginselen en, in het verlengde daarvan, op de toepassing van het van deze beginselen afgeleide recht. Dit heeft tot gevolg dat geen enkele bepaling van deze richtlijn het opleggen of toepassen mag verhinderen van de maatregelen die noodzakelijk blijken voor de vrijwaring van de door deze Verdragsbepalingen als rechtmatig erkende belangen.

Dit betekent met name dat de gunning van opdrachten die binnen het toepassingsgebied van deze richtlijn vallen, kan worden vrijgesteld van deze richtlijn, als dit verantwoord is om redenen van openbare veiligheid of nodig voor de bescherming van de essentiële veiligheidsbelangen van een lidstaat. Dit kan zowel het geval zijn voor opdrachten op het gebied van defensie als voor opdrachten op het gebied van veiligheid, waar zodanig strenge vereisten op het gebied van voorradingszekerheid nodig zijn of die zo vertrouwelijk en/of belangrijk voor de nationale soevereiniteit zijn dat zelfs de specifieke bepalingen van deze richtlijn niet volstaan om de essentiële veiligheidsbelangen van de lidstaten te vrijwaren, waarvan de bepaling een exclusieve verantwoordelijkheid van de lidstaten is.

(17) In overeenstemming met de rechtspraak van het Hof van Justitie van de Europese Gemeenschappen mag de mogelijkheid om van deze uitzonderingen gebruik te maken evenwel niet aldus worden uitgelegd dat de werking ervan verder gaat dan strikt noodzakelijk is ter bescherming van de rechtmatige belangen die deze bepalingen helpen te vrijwaren. Derhalve moet de niet-toepassing van deze richtlijn evenredig zijn met de nagestreefde doelstellingen en het vrije verkeer van goederen en het vrij verrichten van diensten zo min mogelijk belemmeren.

(18) (...) [I]n de specifieke context van defensie- en veiligheidsmarkten [behouden de lidstaten] de bevoegdheid (...) om te besluiten of hun aanbestedende dienst ondernemers van derde landen mag toestaan aan aanbestedingsprocedures deel te nemen. (...)

(19) (...)

(20) Opdrachten op defensie- en veiligheidsgebied bevatten vaak gerubriceerde gegevens die overeenkomstig de wettelijke of bestuursrechtelijke bepalingen die in de lidstaat in kwestie gelden, om veiligheidsredenen moeten worden beschermd tegen toegang door onbevoegden. Op militair gebied bestaan er in de lidstaten systemen voor de rubricering van dergelijke gegevens voor militaire doeleinden. Op het gebied van de niet-militaire veiligheid is de praktijk in de lidstaten echter minder eenduidig, wanneer andere gegevens op

également être protégées. Il convient donc de recourir à un concept qui prenne en compte la diversité des pratiques des États membres et qui permette d'englober les domaines militaire et non militaire [...].

En outre, l'article 296, paragraphe 1, point a), du traité donne aux États membres la possibilité d'exempter des dispositions de la présente directive des marchés dans les domaines de la défense et de la sécurité si l'application de ces dispositions les obligeait à fournir des renseignements dont ils estimeraient la divulgation contraire aux intérêts essentiels de leur sécurité. Cela peut être notamment le cas lorsque les marchés sont à ce point sensibles que leur existence même doit être tenue secrète ».

3 C.J.U.E., 30 novembre 1995, C-55/94, Gebhard, point 37.

4 Note de bas de page n° 1 du courrier cité : Artikel 1bis, 3°, wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, veiligheidsattesten, veiligheidsadviezen en de publiek geregeleerde dienst (Classificatiewet).

5 Note de bas de page n° 2 du courrier cité : Deze worden opgesomd in Artikel 3, § 1, Classificatiewet.

6 Note de bas de page n° 3 du courrier cité : Geclassificeerde opdracht: een opdracht waarbij geclassificeerde informatie door een administratieve overheid aan de onderneming wordt verstrekt of onder wiens gezag of instructie geclassificeerde informatie wordt gegenereerd.

7 Note de bas de page n° 4 du courrier cité : Artikel 1bis, 10°, b), Classificatiewet.

8 Soit les articles 9, 63, § 2, 4° et 5°, et 76 de l'arrêté royal du 23 janvier 2012 'relatif à la passation des marchés publics et de certains marchés de travaux, de fournitures et de services dans les domaines de la défense et de la sécurité'.

9 Voir l'avis 76.172/2 donné le 30 mai 2024 sur un projet d'arrêté royal 'relatif à la banque de données commune « Terrorisme, Extrémisme, processus de Radicalisation » (« T.E.R. »)' (obligation de communiquer des données à caractère personnel à l'autorité fédérale) et les nombreux avis dans le même sens cités à la note de bas de page n° 2 de cet avis ; voir aussi l'avis 75.110/2 donné le 27 février 2024 sur un avant-projet de loi 'modifiant la loi relative à la classification, aux habilitations de sécurité, attestations de sécurité, avis de sécurité et au service public réglementé' (Doc. parl., Chambre, 2023-2024, n° 55-3938/001, pp. 65-90).

10 Lequel est composé conformément à l'article 2 de l'arrêté royal du 22 décembre 2020 'portant création du Conseil national de sécurité, du Comité stratégique du renseignement et de la sécurité et du Comité de coordination du renseignement et de la sécurité', qui dispose comme il suit :

« Les membres du Conseil sont le Premier Ministre, qui préside le Conseil, les ministres ayant dans leurs attributions la Justice, la Défense nationale, l'Intérieur et les Affaires étrangères, et les vice Premiers Ministres qui n'ont pas ces matières dans leurs compétences.

Les Membres du Gouvernement qui ne sont pas membres du Conseil peuvent être invités par le Premier Ministre à y participer pour l'examen de dossiers qui les concernent particulièrement.

Le président du Comité de coordination du Renseignement et de la Sécurité (ci-après dénommé Comité de coordination) participe aux réunions du Conseil national de sécurité, avec voix consultative, sauf si le président du Conseil National de sécurité en décide autrement.

À la demande du président du Conseil national de sécurité ou sur initiative propre, le président du Comité de coordination peut être assisté par des membres du Comité de coordination, chaque fois que leur expertise est nécessaire pour l'examen de certains points de l'ordre du jour.

Les membres non permanents du Comité de coordination peuvent être invités par le Premier Ministre à participer au Conseil pour l'examen de dossiers qui les concernent particulièrement.

Des personnes qui, par leur fonction, peuvent fournir une contribution aux missions du Conseil, peuvent être invités par le Premier Ministre à participer à des réunions du Conseil, avec voix consultative ».

11 Note de bas de page n° 5 de l'avis cité : Voir l'arrêté royal du 22 décembre 2020 'portant création du Conseil national de sécurité, du Comité stratégique du renseignement et de la sécurité et du Comité de coordination du renseignement et de la sécurité'.

12 Avis 69.160/4 donné le 6 mai 2021 sur un avant-projet devenu la loi du 17 février 2022 'modifiant diverses dispositions en matière de communications électroniques en vue d'introduire des mesures de sécurité supplémentaires pour la fourniture de services mobiles 5G' (Doc. parl., Chambre, 2021-2022, n° 55-2317/001, pp. 46-59).

soortgelijke manier moeten worden beschermd. Het is derhalve aangewezen een concept te hanteren dat rekening houdt met de uiteenlopende werkwijzen die in de lidstaten worden gevolgd, en dat zowel het militaire als het niet-militaire gebied kan bestrijken. (....)

Bovendien biedt artikel 296, lid 1, onder a), van het Verdrag de lidstaten de mogelijkheid zowel opdrachten op het gebied van defensie als opdrachten op het gebied van veiligheid van de regels van deze richtlijn uit te sluiten, als toepassing van deze richtlijn hen zou verplichten informatie te verstrekken waarvan zij de bekendmaking strijdig achten met hun essentiële veiligheidsbelangen. Dit kan met name het geval zijn wanneer opdrachten zo gevoelig zijn dat zelfs het bestaan daarvan geheim moet worden gehouden."

3 HJEU 30 november 1995, C-55/94, Gebhard, punt 37.

4 Voetnoot 1 van de geciteerde brief: Artikel 1bis, 3°, wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, veiligheidsattesten, veiligheidsadviezen en de publiek geregeleerde dienst (Classificatiewet).

5 Voetnoot 2 van de geciteerde brief: Deze worden opgesomd in Artikel 3, § 1, Classificatiewet.

6 Voetnoot 3 van de geciteerde brief: Geclassificeerde opdracht: een opdracht waarbij geclassificeerde informatie door een administratieve overheid aan de onderneming wordt verstrekt of onder wiens gezag of instructie geclassificeerde informatie wordt gegenereerd.

7 Voetnoot 4 van de geciteerde brief: Artikel 1bis, 10°, b), Classificatiewet.

8 Namelijk de artikelen 9, 63, § 2, 4° en 5°, en 76 van het koninklijk besluit van 23 januari 2012 'plaatsing overheidsopdrachten en bepaalde opdrachten voor werken, leveringen en diensten op defensie- en veiligheidsgebied'.

9 Zie advies 76.172/2 van 30 mei 2024 over een ontwerp van koninklijk besluit 'betreffende de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R.")' (verplichting om persoonsgegevens mee te delen aan de federale overheid) en de talrijke adviezen in dezelfde zin die geciteerd worden in voetnoot 2 van dat advies; zie ook advies 75.110/2 van 27 februari 2024 over een voorontwerp van wet 'tot wijziging van de wet betreffende de classificatie, de veiligheidsmachtigingen, veiligheidsadviezen en publiek geregeleerde dienst' (Parl.St. Kamer 2023-24, nr. 55-3938/001, 65-90).

10 Die samengesteld wordt overeenkomstig artikel 2 van het koninklijk besluit van 22 december 2020 'tot oprichting van de Nationale Veiligheidsraad, het Strategisch Comité Inlichtingen en Veiligheid en het Coördinatiecomité Inlichtingen en Veiligheid', welke bepaling luidt als volgt:

"De leden van de Raad zijn de Eerste Minister, die de Raad voorziet, de ministers die Justitie, Landsverdediging, Binnenlandse Zaken en Buitenlandse Zaken binnen hun bevoegdheid hebben, en de Vice-eersteministers die geen van deze bevoegdheden hebben.

De Regeringsleden die geen lid zijn van de Raad, kunnen door de Eerste Minister worden uitgenodigd eraan deel te nemen voor het onderzoek van dossiers die hen in het bijzonder aanbelangen.

De voorzitter van het Coördinatiecomité Inlichtingen en Veiligheid (hierna genoemd Coördinatiecomité) neemt deel aan de vergaderingen van de Nationale Veiligheidsraad, met raadgevende stem, tenzij de voorzitter van de Nationale Veiligheidsraad daar anders over beslist.

Op verzoek van de voorzitter van de Nationale Veiligheidsraad of op eigen initiatief, kan de voorzitter van het Coördinatiecomité worden bijgestaan door leden van het Coördinatiecomité telkens hun expertise noodzakelijk is voor de bespreking van bepaalde agendapunten.

De niet-permanente leden van het Coördinatiecomité kunnen door de Eerste Minister worden uitgenodigd om deel te nemen aan de Raad voor het onderzoek van dossiers die hen in het bijzonder aanbelangen.

Personen die vanuit hun functie een bijdrage kunnen leveren aan de opdrachten van de Raad, kunnen door de Eerste Minister worden uitgenodigd om deel te nemen aan vergaderingen van de Raad, met raadgevende stem."

11 Voetnoot 5 van het geciteerde advies: Zie het koninklijk besluit van 22 december 2020 'tot oprichting van de Nationale Veiligheidsraad, het Strategisch Comité Inlichtingen en Veiligheid en het Coördinatiecomité Inlichtingen en Veiligheid'.

12 Advies 69.160/4 van 6 mei 2021 over een voorontwerp dat geleid heeft tot de wet van 17 februari 2022 'tot wijziging van diverse bepalingen inzake elektronische communicatie met het oog op de invoering van bijkomende beveiligingsmaatregelen voor de verstrekking van mobiele 5G-diensten' (Parl.St. Kamer 2021-22, nr. 55-2317/001, 46-59).

Voir également l'avis 25.704/2 donné le 21 mai 1997 sur un avant-projet devenu la loi du 11 décembre 1998 dans lequel la section de législation a observé ce qui suit :

« Qui plus est, en confiant à un Comité ministériel, — qui, en règle générale, ne peut être qu'un organe d'avis et de préparation de la politique gouvernementale, et non d'exécution des lois — le soin de déterminer la nature des données et les modalités de leur recueillement, le texte en projet heurte l'article 22 de la Constitution, lequel exige que les principes essentiels relatifs à ces questions soient inscrits dans un texte de loi » (Doc. parl., Chambre, 1996-1997, nos 49-1193/1 et 49-1194/1, p. 38, observation formulée sous l'observation générale n° 1).

13 Voir en ce sens l'avis 63.663/VR/V donné le 17 juillet 2018 sur un projet devenu l'arrêté royal du 25 octobre 2018 'limitant les jeux de hasard dans les établissements de jeux de hasard de classe III' et l'avis 76.366/2 donné le 12 juin 2024 sur un projet d'arrêté royal 'relatif au Conseil des bourgmestres'.

14 Ou, à tout le moins, la dernière modification en vigueur.

15 Principes de technique législative – Guide de rédaction des textes législatifs et réglementaires, www.raadvst-consetat.be, onglet « Technique législative », recommandation n° 27.

16 Avis 61.551/2 donné le 14 juin 2017 sur un avant-projet devenu la loi du 23 février 2018 'portant modification de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité' (Doc. parl., Chambre, 2017-2018, n° 54-2767/001, p. 34, observation formulée sous l'article 2).

17 Comme la section de législation l'a observé dans son avis 75.117/2 du 15 février 2024,

« [il] en va d'autant plus ainsi que le [RGPD] protège spécifiquement le traitement des données à caractère personnel 'à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques' [...], et que cette protection relève en outre, en l'espèce, du droit fondamental d'accès à l'information détenue par les autorités publiques, tel qu'il est consacré par l'article 32 de la Constitution et par la Convention du Conseil de l'Europe 'sur l'accès aux documents publics', signée à Tromsø le 18 juin 2009 [...].

Ce droit fondamental se déduit également de l'article 10 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales [...] et est donc aussi visé par l'article 85 du RGPD.

Dans cette mesure, des données à caractère personnel triées et archivées peuvent être conservées sans limitation de durée [...] » (avis 75.117/2 donné le 15 février 2024 sur un avant-projet de décret 'modifiant le décret du 4 décembre 2003 relatif à la création de l'Institut wallon de l'évaluation, de la prospective et de la statistique', Doc. parl., Parl. w., 2023—2024, n° 1656/1, pp. 27—30).

18 À l'instar de ce que prévoit l'article 27 de l'arrêté royal du 24 mars 2000.

19 Compte tenu de l'observation formulée sous le titre IV (articles 112 à 114).

20 Principes de technique législative – Guide de rédaction des textes législatifs et réglementaires, www.raadvst-consetat.be, onglet « Technique législative », recommandation n° 167 et formule F-4-7-2.

20 DECEMBRE 2024. — Arrêté royal portant exécution de la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, aux avis de sécurité et au service public réglementé

PHILIPPE, Roi des Belges,
A tous, présents et à venir, Salut.

Vu la Constitution, article 37 ;

Vu la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, aux avis de sécurité et au service public réglementé, l'article 1^{er}, modifié par la loi du 19 décembre 2023 ; l'article 1^{septies}, alinéa 4, inséré par la loi du 7 avril 2023 ; l'article 1^{octies}, § 2, inséré par la loi du 7 avril 2023 ; l'article 4, alinéa 6, modifié par la loi du 7 avril 2023 ; l'article 6, alinéa 2 ; l'article 7, § 1^{er}, alinéas 1^{er} et 2 et § 6, deuxième alinéa, modifié par la loi du 7 avril 2023 ; l'article 8, § 2, alinéa 2, modifié par la loi du 7 avril 2023 ; l'article 12, alinéa 2 ; l'article 17, alinéas 1^{er}, 2 et 4, modifié par la loi du 23 février 2018 et l'article 22, alinéas 1^{er} et 3 ;

Vu l'arrêté royal du 24 mars 2000 portant exécution de la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, attestations de sécurité et avis de sécurité ;

Vu l'avis de l'Inspection des Finances émis le 17 mars 2024 ;

Vu l'accord du Secrétaire d'Etat au Budget du 27 mars 2024 ;

Zie eveneens advies 25.704/2 van 21 mei 1997 over een voorontwerp dat geleid heeft tot de wet van 11 december 1998, waarin de afdeling Wetgeving het volgende heeft opgemerkt:

“Bovendien is de ontworpen tekst, doordat hij een Ministerieel Comité, — dat in de regel slechts een adviesorgaan kan zijn dat het beleid van de regering voorbereidt, doch geen uitvoering geeft aan wetten — belast met het bepalen van de aard van de gegevens en de wijze waarop ze ingewonnen worden, in strijd met artikel 22 van de Grondwet, dat voorschrijft dat de grondbeginselen betreffende die aangelegenheden in een wettekst worden opgenomen.” (Parl.St. Kamer 1996-97, nrs. 49-1193/1 en 49-1194/1, 38, opmerking gemaakt bij algemene opmerking 1).

13 Zie in dat verband advies 63.663/VR/V van 17 juli 2018 over een ontwerp dat geleid heeft tot het koninklijk besluit van 25 oktober 2018 'tot beperking van de kansspelen in de kansspelinrichtingen klasse III' en advies 76.366/2 van 12 juni 2024 over een ontwerp van koninklijk besluit 'met betrekking tot de Adviesraad burgemeesters'.

14 Of toch minstens de laatste nog van kracht zijnde wijziging.

15 Beginselen van de wetgevingstechniek – Handleiding voor het opstellen van wetgevende en reglementaire teksten, www.raadvst-consetat.be, tab “Wetgevingstechniek”, aanbeveling 27.

16 Advies 61.551/2 van 14 juni 2017 over een voorontwerp dat geleid heeft tot de wet van 23 februari 2018 'houdende wijziging van de wet van 11 december 1998, betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen' (Parl.St. Kamer 2017-18, nr. 54-2767/001, 34, opmerking in verband met artikel 2).

17 De afdeling Wetgeving heeft immers in advies 75.117/2 van 15 februari 2024 het volgende opgemerkt:

“Il en va d'autant plus ainsi que le [RGPD] protège spécifiquement le traitement des données à caractère personnel 'à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques' (...), et que cette protection relève en outre, en l'espèce, du droit fondamental d'accès à l'information détenue par les autorités publiques, tel qu'il est consacré par l'article 32 de la Constitution et par la Convention du Conseil de l'Europe 'sur l'accès aux documents publics', signée à Tromsø le 18 juin 2009 (...).

Ce droit fondamental se déduit également de l'article 10 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales [...] et est donc aussi visé par l'article 85 du RGPD.

Dans cette mesure, des données à caractère personnel triées et archivées peuvent être conservées sans limitation de durée [...]” (advies 75.117/2 van 15 februari 2024 over een voorontwerp van decreet 'tot wijziging het decreet van 4 december 2003 betreffende de oprichting van het Waals Instituut voor evaluatie, toekomstverwachting en statistiek', Parl.St. W.Parl. 2023—24, nr. 1656/1, 27—30).

18 Naar het voorbeeld van het bepaalde in artikel 27 van het koninklijk besluit van 24 maart 2000.

19 Gelet op de opmerking over titel IV (artikelen 112 tot 114).

20 Beginselen van de wetgevingstechniek – Handleiding voor het opstellen van wetgevende en reglementaire teksten, www.raadvst-consetat.be, tab “Wetgevingstechniek”, aanbeveling 167 en formule F-4-7-2.

20 DECEMBER 2024. — Koninklijk besluit tot uitvoering van de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, de veiligheidsadviezen en de publiek gereguleerde dienst

FILIP, Koning der Belgen,
Aan allen die nu zijn en hierna wezen zullen, Onze Groet.

Gelet op de Grondwet, artikel 37 ;

Gelet op de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, de veiligheidsadviezen en de publiek gereguleerde dienst, artikel 1^{er}, gewijzigd bij de wet van 19 december 2023; artikel 1^{septies}, vierde lid, ingevoegd bij de wet van 7 april 2023; artikel 1^{octies}, § 2, ingevoegd bij de wet van 7 april 2023; artikel 4, zesde lid, gewijzigd bij de wet van 7 april 2023; artikel 6, tweede lid; artikel 7, § 1, eerste en tweede lid en § 6, tweede lid, gewijzigd bij de wet van 7 april 2023; artikel 8, § 2, tweede lid, gewijzigd bij de wet van 7 april 2023; artikel 12, tweede lid; artikel 17, eerste, tweede en vierde lid, gewijzigd bij de wet van 23 februari 2018 en artikel 22, eerste en derde lid;

Gelet op het koninklijk besluit van 24 maart 2000 tot uitvoering van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen;

Gelet op het advies van de Inspectie van Financiën, gegeven op 17 maart 2024;

Gelet op de akkoordbevinding van de staatssecretaris van Begroting van 27 maart 2024;

Vu l'avis n° 008/CPR-ACC/2024 du Comité permanent de contrôle des services de renseignement et de sécurité émis le 22 juillet 2024 ;

Vu l'avis positif du Conseil national de Sécurité du 24 avril 2024 ;

Vu la communication de l'Organe de contrôle de l'information policière du 4 juin 2024, à la demande d'avis du 16 mai 2024, selon laquelle il ne donne pas d'avis sur le projet d'arrêté royal pour défaut de compétence ;

Vu l'avis du Collège des procureurs généraux près les cours d'appel, émis le 31 juillet 2024 ;

Vu la dispense d'analyse d'impact sur la base de l'article 8, § 2, 1° de la loi du 15 décembre 2013 portant des dispositions diverses concernant la simplification administrative ;

Vu l'avis n° 76.465/2 du Conseil d'Etat émis le 9 juillet 2024, en application de l'article 84, § 1^{er}, alinéa 1^{er}, 2°, des lois sur le Conseil d'Etat, coordonnées le 12 janvier 1973 ;

Considérant que cet arrêté royal relève des affaires courantes car il s'agit d'une affaire qui n'exige aucune initiative nouvelle de la part du Gouvernement et pour laquelle la continuité du pouvoir impose l'intervention du Pouvoir exécutif sous peine de créer une carence préjudiciable aux citoyens, telles que définies par la circulaire relative aux Affaires courantes du 27 mai 2024, adressée par le Premier Ministre aux Membres du Gouvernement ;

Sur la proposition de Notre Premier Ministre, du Ministre de la Justice, du Ministre de l'Intérieur, du Ministre de la Défense et de l'avis des ministres qui en ont délibéré en Conseil,

Nous avons arrêté et arrêtons :

TITRE I. — Définitions

Article 1^{er}. Pour l'application du présent arrêté, l'on entend par :

1° « la loi » : la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, aux avis de sécurité et au service public réglementé ;

2° « fonctionnaire dirigeant » : la personne à laquelle est confiée, par nomination définitive ou par mandat, la direction d'une administration publique, d'un organisme d'intérêt public ou d'une entreprise publique autonome ou son remplaçant ;

3° « compromission » : la situation dans laquelle des informations classifiées, à la suite d'une négligence, d'une brèche de sécurité ou d'une activité nuisible, ont perdu leur confidentialité, intégrité ou disponibilité, ou dans laquelle des services et moyens d'appui ont perdu leur intégrité ou disponibilité, en ce compris la perte, la divulgation à des personnes non autorisées, la modification non autorisée, la destruction d'une manière non autorisée ou le déni de service ;

4° « incident de sécurité » : un acte ou une omission, intentionnel ou non, contraire aux dispositions d'un accord international, de la réglementation de l'Union européenne, de la loi, du présent arrêté et des directives de l'Autorité nationale de Sécurité dans ce domaine, par laquelle des informations classifiées ou des services et moyens d'appui sont effectivement ou potentiellement mis en péril ;

5° « Autorité nationale de Sécurité » : l'autorité visée à l'article 1^{ter} de la loi ;

6° « Conseil national de Sécurité » : l'organe politique stratégique et de coordination créée par l'arrêté royal du 28 janvier 2015 portant création du Conseil national de sécurité, du Comité stratégique du renseignement et de la sécurité et du Comité de coordination du renseignement et de la sécurité ;

7° « sécurité industrielle » : l'application de mesures de protection en vue de prévenir, de détecter et de réparer la compromission d'informations classifiées lors des négociations précontractuelles et durant l'exécution d'un marché public ;

8° « titulaire » : une personne physique ou morale habilitée conformément au titre III, chapitre 5 du présent arrêté qui, sur base d'un besoin d'en connaître avéré, est en possession d'informations classifiées et à laquelle il incombe par conséquent d'en assurer la protection, conformément à la loi, au présent arrêté et aux directives de l'Autorité nationale de Sécurité ;

9° « porteur » : toute personne chargée de transporter des informations classifiées et en possession d'une habilitation de sécurité valable d'un niveau au moins équivalent à celui des informations transportées, mais qui n'a pas qualité pour prendre connaissance de leur contenu ;

Gelet op het advies nr. 008/VCI-BTA/202 van het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten, gegeven op 22 juli 2024;

Gelet op het positief advies van de Nationale Veiligheidsraad van 24 april 2024;

Gelet op de mededeling van het Controleorgaan op de politionele informatie van 4 juni 2024, op de vraag tot adviesverlening van 16 mei 2024, dat het geen advies verstrekt op het ontwerp van koninklijk besluit wegens onbevoegdheid;

Gelet op het advies van het College van procureurs-generaal bij de hoven van beroep, gegeven op 31 juli 2024;

Gelet op de vrijstelling van een impactanalyse op basis van artikel 8, § 2, 1°, van de wet van 15 december 2013 houdende diverse bepalingen inzake administratieve vereenvoudiging;

Gelet op het advies nr. 76.465/2 van de Raad van State, gegeven op 9 juli 2024 met toepassing van artikel 84, § 1, eerste lid, 2° van de wetten op de Raad van State, gecoördineerd op 12 januari 1973;

Overwegende dat dit koninklijk besluit valt binnen het kader van de lopende zaken, aangezien het gaat om een zaak waarvoor geen nieuw initiatief van de Regering is vereist en die met het oog op de continuïteit van het gezag door de Uitvoerende Macht moet worden behandeld, omdat anders een voor de burgers nadelig vacuüm zou ontstaan, zoals bepaald in de omzendbrief Lopende zaken van 27 mei 2024, die door de Eerste Minister aan de Regeringsleden werd gericht;

Op de voordracht van Onze Eerste Minister, de Minister van Justitie, de Minister van Binnenlandse Zaken, de Minister van Defensie en het advies van de in Raad vergaderde Ministers,

Hebben Wij besloten en besluiten Wij :

TITEL I. — Definities

Artikel 1. Voor de toepassing van dit besluit wordt verstaan onder:

1° "de wet": de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, de veiligheidsadviezen en de publiek gereguleerde dienst;

2° "leidend ambtenaar": de persoon aan wie, bij definitieve benoeming of bij mandaat, de leiding van een openbaar bestuur, een instelling van openbaar nut of een autonoom overheidsbedrijf toevertrouwd is of zijn plaatsvervanger;

3° "compromittering": de situatie waarin geclassificeerde informatie - ten gevolge van een nalatigheid, een inbreuk op de beveiliging of een schadelijke activiteit - hun vertrouwelijkheid, integriteit of beschikbaarheid hebben verloren, of waarin ondersteunende diensten en middelen hun integriteit of beschikbaarheid hebben verloren, met inbegrip van verlies, bekendmaking aan onbevoegde personen, ongeoorloofde wijziging, vernietiging op een ongeoorloofde manier, of ontzegging van dienst;

4° "veiligheidsincident": een handelen of nalaten, opzettelijk of niet, in strijd met de bepalingen van de toepasselijke internationale overeenkomst of regelgeving van de Europese Unie, de wet, het voorliggend besluit en de richtlijnen van de Nationale Veiligheidsoverheid in dit verband, waardoor geclassificeerde informatie of ondersteunende diensten en middelen feitelijk of mogelijk in gevaar komen;

5° "Nationale Veiligheidsoverheid": de in artikel 1^{ter} van de wet bedoelde overheid;

6° "Nationale Veiligheidsraad": het strategisch en coördinerend beleidsorgaan opgericht bij koninklijk besluit van 28 januari 2015 tot oprichting van de Nationale Veiligheidsraad, het Strategisch Comité Inlichtingen en Veiligheid en het Coördinatiecomité Inlichtingen en Veiligheid;

7° "industriële veiligheid": de toepassing van beschermende maatregelen om de compromittering van geclassificeerde informatie die tijdens precontractuele onderhandelingen en tijdens de uitvoering van overheidsopdrachten wordt aangewend te voorkomen, op te sporen en te herstellen;

8° "houder": een overeenkomstig titel III, hoofdstuk 5 van voorliggend besluit gemachtigde natuurlijk persoon of rechtspersoon van wie de noodzaak tot kennisname vaststaat en die geclassificeerde informatie in zijn bezit heeft en derhalve voor de bescherming daarvan verantwoordelijk is in overeenstemming met de wet, het voorliggend besluit en de richtlijnen van de Nationale Veiligheidsoverheid;

9° "drager": iedere persoon aangeduid voor het vervoeren van geclassificeerde informatie en die in het bezit is van een geldige veiligheidsmachtiging van een niveau dat minstens gelijkwaardig is aan de vervoerde informatie, maar die niet de hoedanigheid heeft om kennis te nemen van de inhoud van de informatie;

10° « organes » : tous les membres de l'organe d'administration, de la gestion journalière et toutes les autres personnes qui détiennent le pouvoir de gérer effectivement la personne morale, à savoir administrateurs, membres du conseil de surveillance, membres du conseil de direction, représentants permanents, personnes chargées de la gestion journalière et dirigeants de fait ;

11° « préposés » : toutes les personnes qui, dans le cadre d'une convention, à titre onéreux ou non, exécutent un rôle ou une tâche sous la direction et le contrôle d'une autre personne ;

12° « personne morale » : toute personne morale qui n'est pas une entité de droit public belge ;

13° « personne de contact pour la sécurité » : le fonctionnaire, le membre du personnel ou la personne contractuellement liée à l'entité, disposant de la nationalité belge et d'un avis de sécurité positif tel que défini à l'article 24 de la loi qui, dans une administration publique, un organisme d'intérêt public, une entreprise publique autonome ou une personne morale sans habilitation de sécurité, est désigné par le ministre ou son délégué, ou, à défaut de tutelle d'un ministre, le chef de cette administration publique, de cet organisme d'intérêt public ou de cette entreprise publique autonome, ou par l'organe d'administration de cette personne morale pour veiller à l'observation des règles de sécurité relatives à l'utilisation d'informations classifiées de niveau « RESTREINT » ;

14° « entité » : une organisation, avec ou sans responsabilité juridique, qui exerce une ou plusieurs activités spécifiques nécessitant l'utilisation d'informations classifiées ;

15° « autorité fonctionnelle d'un système de communication et d'information » : la personne ou l'entité responsable de l'élaboration, du développement, de l'entretien et/ou du fonctionnement d'un système de communication et d'information qui apporte un appui à un ou plusieurs processus.

TITRE II. — ROLES ET RESPONSABILITES

CHAPITRE 1. — L'officier de sécurité

Art. 2. En application de l'article 1bis, 15°, a) de la loi, les membres du Gouvernement fédéral et des gouvernements des entités fédérées désignent, dans la mesure où ils souhaitent utiliser des informations classifiées, un officier de sécurité au sein de leur cellule stratégique et au moins un officier de sécurité au sein de chaque administration publique relevant de leur autorité, dans laquelle des informations classifiées de niveau « CONFIDENTIEL » ou supérieur sont utilisées.

L'officier de sécurité est, si possible, remplacé par la personne dont le nom a été communiqué à l'autorité qui a désigné l'officier de sécurité, tel que visé à l'alinéa 1^{er}. Les conditions d'accès à ce remplacement sont les mêmes que celles exigées pour la fonction d'officier de sécurité déterminées par la loi et le présent arrêté.

Art. 3. Seules les personnes qui possèdent la nationalité belge peuvent exercer la fonction d'officier de sécurité.

Art. 4. L'Autorité nationale de Sécurité fixe les modalités du contrôle de l'exécution des missions de l'officier de sécurité.

CHAPITRE 2. — La personne de contact pour la sécurité

Art. 5. En ce qui concerne l'utilisation d'informations classifiées de niveau « RESTREINT », la personne de contact pour la sécurité :

1° est le point de contact permanent pour l'Autorité nationale de Sécurité et les autorités de sécurité visées à l'article 1quinquies de la loi, représente auprès de celles-ci la personne morale pour ce qui concerne tous les aspects de sécurité et est compétente pour prendre les mesures et décisions requises ;

2° est chargée de contrôler la conformité de la sécurité des informations classifiées susmentionnées, conformément aux mesures de protection décrites dans la loi, le présent arrêté et les directives de l'Autorité nationale de Sécurité ;

3° est chargée de prêter son concours lors des contrôles, des audits et des enquêtes effectués par l'Autorité nationale de Sécurité et les autorités de sécurité visées à l'article 1quinquies de la loi ;

4° est responsable des signalements et des enquêtes administratives internes relatifs aux incidents de sécurité et compromissions, ainsi que de prendre des mesures à cet égard, conformément aux instructions de l'autorité de sécurité compétente ;

10° "organen": alle leden van het bestuursorgaan, het dagelijks bestuur en alle andere personen die ten aanzien van de rechtspersoon werkelijke bestuursbevoegdheid hebben, zijnde bestuurders, leden van de raad van toezicht, leden van de directieraad, vaste vertegenwoordigers, personen belast met het dagelijks bestuur, en de feitelijke bestuurders;

11° "aangestelde": eenieder die in het kader van een overeenkomst, al dan niet ten bezwaarde titel, onder het gezag en toezicht van een andere persoon een rol of een taak uitvoert;

12° "rechtspersoon": elke rechtspersoon die geen Belgische publiekrechtelijke rechtspersoon is;

13° "contactpersoon voor de veiligheid" : de ambtenaar, het personeelslid of de persoon verbonden aan de entiteit door een contract, in het bezit van de Belgische nationaliteit en een positief veiligheidsadvies zoals bedoeld in artikel 24 van de wet, dat in de schoot van een openbaar bestuur, een instelling van openbaar nut, een autonoom overheidsbedrijf of een rechtspersoon zonder veiligheidsmachtiging door de minister of zijn gedelegeerde, of, bij ontstentenis van een minister met voorgedij, door het hoofd van dit openbaar bestuur, van deze instelling van openbaar nut, van dit autonoom overheidsbedrijf of door het bestuursorgaan van de rechtspersoon wordt aangewezen om te zorgen voor de inachtneming van de veiligheidsregels betreffende de aanwending van geclassificeerde informatie met het classificatieniveau "BEPERKT";

14° "entiteit": een organisatie met of zonder rechtspersoonlijkheid die een of meerdere bepaalde activiteiten uitvoert die de aanwending van geclassificeerde informatie vereisen;

15° "functionele autoriteit van een communicatie- en informatiesysteem": de persoon of entiteit die verantwoordelijk is voor het ontwerp, de ontwikkeling, het onderhoud en/of de werking van een communicatie- en informatiesysteem, waarmee één of meerdere processen worden ondersteund.

TITEL II. — ROLLEN EN VERANTWOORDELIJKHEDEN

HOOFDSTUK 1. — De veiligheidsofficier

Art. 2. In toepassing van artikel 1bis, 15°, a) van de wet, duiden de leden van de federale Regering en van de deelstatenregeringen, voor zover zij geclassificeerde informatie wensen aan te wenden, een veiligheidsofficier aan binnen hun beleidsceel en ten minste één veiligheidsofficier binnen elk openbaar bestuur dat onder hun gezag ressorteert, waarbinnen geclassificeerde informatie met het beschermingsniveau "VERTROUWELIJK" of hoger wordt aangewend.

De veiligheidsofficier wordt, indien mogelijk, vervangen door de persoon van wie de naam werd meegedeeld aan de overheid die de veiligheidsofficier heeft aangewezen, zoals bedoeld in het eerste lid. De voorwaarden van toegang voor deze vervanging zijn dezelfde als deze vereist voor de functie van veiligheidsofficier, zoals bepaald door de wet en voorliggend besluit.

Art. 3. De functie van veiligheidsofficier kan enkel worden uitgeoefend door personen die over de Belgische nationaliteit beschikken.

Art. 4. De Nationale Veiligheidsoverheid legt de nadere regels vast voor het toezicht op de uitvoering van de opdrachten van de veiligheidsofficier.

HOOFDSTUK 2. — De contactpersoon voor de veiligheid

Art. 5. De contactpersoon voor de veiligheid is voor wat betreft de aanwending van geclassificeerde informatie met het classificatieniveau "BEPERKT":

1° het vaste aanspreekpunt voor de Nationale Veiligheidsoverheid en de in artikel 1quinquies van de wet bedoelde veiligheidsoverheden en vertegenwoordigt hierbij de rechtspersoon voor wat betreft alle beveiligingsaspecten en is bevoegd tot het nemen van de vereiste maatregelen en beslissingen;

2° verantwoordelijk voor het toezicht houden op de deugdelijkheid van de beveiliging van voormelde geclassificeerde informatie conform de beschermingsmaatregelen zoals omschreven in de wet, het voorliggend besluit en de richtlijnen van de Nationale Veiligheidsoverheid;

3° verantwoordelijk voor het geven van volledige medewerking bij controles, audits en onderzoeken door de Nationale Veiligheidsoverheid en de in artikel 1quinquies van de wet bedoelde veiligheidsoverheden;

4° verantwoordelijk voor het melden en intern administratief onderzoeken van veiligheidsincidenten en compromitteringen, alsook het treffen van maatregelen dienaangaande, volgens de instructies van de bevoegde veiligheidsoverheid;

5° est chargée de rappeler régulièrement au personnel devant avoir accès aux informations classifiées de niveau « RESTREINT », les restrictions en matière d'utilisation des informations classifiées de niveau « RESTREINT » et les mesures de protection en vigueur.

Art. 6. La personne de contact pour la sécurité :

1° a pris connaissance des mesures de protection relatives aux informations classifiées de niveau « RESTREINT » ;

2° confirme par écrit à l'Autorité nationale de Sécurité selon le modèle établi par l'Autorité nationale de Sécurité, avoir entièrement compris les responsabilités et les mesures de protection imposées.

Art. 7. Si un officier de sécurité a déjà été désigné au sein de l'entité visée à l'article 1^{er}, 14°, aucune personne de contact pour la sécurité n'est désignée.

L'officier de sécurité exerce dans ce cas les missions de la personne de contact pour la sécurité, sans devoir être en possession d'un avis de sécurité positif, tel que visé à l'article 24 de la loi.

Art. 8. L'Autorité nationale de Sécurité fixe les modalités du contrôle de l'exécution des missions de la personne de contact pour la sécurité et peut déterminer des modalités complémentaires de désignation.

CHAPITRE 3. — *L'autorité fonctionnelle d'un système de communication et d'information*

Art. 9. L'autorité fonctionnelle d'un système de communication et d'information, telle que visée au titre III, chapitre 3 du présent arrêté :

1° prend contact, dans le cadre d'un projet d'approbation d'un système de communication et d'information, avec l'Autorité nationale de Sécurité afin de fixer les normes et exigences de sécurité pertinentes et de démarrer le processus d'approbation, en coopération avec l'officier de sécurité ou la personne de contact pour la sécurité ;

2° veille à ce que les mesures de sécurité répondent aux exigences de la loi, du présent arrêté et des directives de l'Autorité nationale de Sécurité et à ce que le système de communication et d'information ne traite aucune information classifiée avant approbation ;

3° évalue au moins une fois par an les mesures de protection mises en place dans un système de communication et d'information, en ce compris le plan de sécurité, et transmet cette évaluation à l'Autorité nationale de Sécurité, après avoir informé l'officier de sécurité ou la personne de contact pour la sécurité ;

4° consulte et tient informé l'officier de sécurité ou la personne de contact pour la sécurité sur des questions en lien avec la sécurité du système de communication et d'information ;

5° signale toute modification prévue du système de communication et d'information à l'Autorité nationale de Sécurité au moyen d'une déclaration de conformité, après avoir informé l'officier de sécurité ou la personne de contact pour la sécurité ;

6° avertit l'officier de sécurité ou la personne de contact pour la sécurité en cas d'incident de sécurité dans le système de communication et d'information indiquant que celui-ci ne peut plus protéger les informations classifiées de manière adéquate ;

7° prend, après consultation de l'officier de sécurité ou la personne de contact pour la sécurité, contact avec l'Autorité nationale de Sécurité, pour avis concernant l'approche à suivre, dans les 24h qui suivent un incident de sécurité ou la prise de connaissance d'informations dont il ressort que le système de communication et d'information n'est (en partie) plus apte à protéger adéquatement les informations classifiées ;

8° prête à tout moment son concours à l'Autorité nationale de Sécurité pour effectuer les tâches relatives à l'approbation et au contrôle du système de communication et d'information qui incombent à cette instance ;

9° prévoit les sensibilisations et formations nécessaires pour ses préposés.

5° verantwoordelijk voor het geregeld in herinnering brengen aan het personeel dat toegang moet krijgen tot geclassificeerde informatie van het niveau "BEPERKT" van de beperkingen op de aanwending van geclassificeerde informatie van het niveau "BEPERKT" en de van toepassing zijnde beschermingsmaatregelen.

Art. 6. De contactpersoon voor de veiligheid:

1° heeft kennis genomen van de beschermingsmaatregelen inzake geclassificeerde informatie met het classificatieniveau "BEPERKT";

2° bevestigt schriftelijk aan de Nationale Veiligheidsoverheid, conform het model opgesteld door de Nationale Veiligheidsoverheid, de opgelegde verantwoordelijkheden en beschermingsmaatregelen volledig te begrijpen.

Art. 7. Indien er in de schoot van de in artikel 1, 14° bedoelde entiteit reeds een veiligheidsofficier is aangewezen, wordt er geen contactpersoon voor de veiligheid aangesteld.

De veiligheidsofficier oefent in dat geval de opdrachten van de contactpersoon voor de veiligheid uit, zonder dat deze in het bezit moet worden gesteld van een positief veiligheidsadvies, zoals bedoeld in artikel 24 van de wet.

Art. 8. De Nationale Veiligheidsoverheid legt de nadere regels vast voor het toezicht op de uitvoering van de opdrachten van de contactpersoon voor de veiligheid en kan bijkomende modaliteiten bepalen voor de aanstelling.

HOOFDSTUK 3. — *De functionele autoriteit van een communicatie- en informatiesysteem*

Art. 9. De functionele autoriteit van een communicatie- en informatiesysteem, zoals bedoeld in titel III, hoofdstuk 3 van voorliggend besluit:

1° neemt in het kader van een project voor de goedkeuring van een communicatie- en informatiesysteem contact op met de Nationale Veiligheidsoverheid om de relevante beveiligingsnormen en -vereisten vast te stellen en het proces van goedkeuring te starten samen met de veiligheidsofficier of de contactpersoon voor de veiligheid;

2° waarborgt dat de beveiligingsmaatregelen voldoen aan de eisen van de wet, het voorliggend besluit en de richtlijnen van de Nationale Veiligheidsoverheid en dat het communicatie- en informatiesysteem geen geclassificeerde informatie behandelt voordat het is goedgekeurd;

3° evalueert ten minste éénmaal per jaar de beveiligingsmaatregelen die op een communicatie- en informatiesysteem worden toegepast, met inbegrip van het beveiligingsplan, en stuurt dit door naar de Nationale Veiligheidsoverheid, na de veiligheidsofficier of de contactpersoon voor de veiligheid te hebben geïnformeerd;

4° raadpleegt en houdt de veiligheidsofficier of de contactpersoon voor de veiligheid op de hoogte over kwesties in verband met de beveiliging van het communicatie- en informatiesysteem;

5° meldt elke geplande wijziging aan het communicatie- en informatiesysteem aan de Nationale Veiligheidsoverheid door middel van een conformiteitsverklaring, na de veiligheidsofficier of de contactpersoon voor de veiligheid te hebben geïnformeerd;

6° stelt de veiligheidsofficier of de contactpersoon voor de veiligheid in kennis wanneer zich in het communicatie- en informatiesysteem een veiligheidsincident voordoet waarbij wordt aangegeven dat het systeem geclassificeerde informatie niet langer passend kan beschermen;

7° neemt, na de veiligheidsofficier of de contactpersoon voor de veiligheid te hebben geraadpleegd, in geval van een veiligheidsincident of bij kennisname van informatie waaruit blijkt dat (een gedeelte van) het communicatie- en informatiesysteem niet meer in staat is om de geclassificeerde informatie adequaat te beschermen, binnen de 24 uur contact op met de Nationale Veiligheidsoverheid voor advies over de te volgen aanpak;

8° verleent de Nationale Veiligheidsoverheid te allen tijde volledige steun bij het vervullen van taken die deze instantie heeft met betrekking tot de goedkeuring van het communicatie- en informatiesysteem en het toezicht erop;

9° voorziet in de nodige sensibilisering en training voor zijn aangestelden.

TITRE III. — Informations classifiées**CHAPITRE 1. — Mesures de protection applicables lors de la classification et de la gestion d'informations classifiées****Section 1^{re}. — Disposition générale**

Art. 10. Les règles relatives à la procédure pour la classification, la modification du niveau de classification et la déclassification et aux mesures de protection inhérentes à la classification, contenues dans le présent arrêté, ne portent pas préjudice à la faculté de chaque ministre et du chef du Service Général du Renseignement et de la Sécurité des Forces armées en ce qui concerne la Défense, de prescrire des règles complémentaires d'ordre technique.

Section 2. — Personnes et autorités compétentes pour la classification, la modification du niveau de classification et la déclassification

Art. 11. Les personnes ou autorités, générant des informations classifiées sous l'autorité ou à l'instruction d'une autorité administrative, ainsi que le procureur fédéral et les magistrats qu'il délègue à cette fin et le procureur général qui représente le Collège des procureurs généraux dans le Comité de coordination du renseignement et de la sécurité, doivent être titulaires d'une habilitation de sécurité de niveau « SECRET » au minimum afin de procéder, conformément aux dispositions du présent arrêté et aux directives de l'Autorité nationale de Sécurité, à :

- 1° la classification;
- 2° la modification du niveau de classification;
- 3° la déclassification.

Les personnes ou personnes morales visées au premier alinéa attribuent un niveau de classification tel que défini à l'article 4 de la loi, sans toutefois attribuer un niveau de classification supérieur au niveau de l'habilitation de sécurité dont elles sont titulaires.

Art. 12. Seules les personnes suivantes, dans la mesure où elles possèdent une habilitation de sécurité du niveau de classification correspondante, sont habilitées à classer, modifier ou déclasser un niveau de classification « TRÈS SECRET » :

- 1° les membres permanents du Comité de coordination du renseignement et de la sécurité ;
- 2° le chef de la Défense et les officiers et fonctionnaires civils qu'il délègue à cette fin, qui sont au moins de niveau A, ainsi que les attachés de la Défense ;
- 3° le chef du Service général du Renseignement et de la Sécurité des Forces armées et les agents qu'il délègue à cette fin ;
- 4° l'administrateur général de la Sûreté de l'Etat et les agents qu'il délègue à cet effet ;
- 5° le commissaire général de la Police fédérale et les membres qu'il délègue à cet effet ;
- 6° le directeur général de l'Agence fédérale de Contrôle nucléaire ;
- 7° le secrétaire du Conseil des Ministres ;
- 8° la personne qui assure le secrétariat du Conseil national de Sécurité ;
- 9° le Président du Comité de Direction du Service public fédéral Affaires étrangères, Commerce extérieur et Coopération au Développement, les membres qu'il délègue à cet effet et les chefs des missions diplomatiques ou des postes consulaires ;
- 10° les fonctionnaires dirigeants désignés par le Conseil national de Sécurité ;
- 11° le procureur fédéral et les magistrats qu'il délègue à cet effet ;
- 12° le directeur et les membres de l'Organe de Coordination pour l'Analyse de la Menace compétents, désignés par celui-ci ;
- 13° le Comité permanent R, le chef de son Service d'Enquêtes, son greffier et le personnel ou les membres du personnel ou membres du Service d'Enquêtes de niveau A désignés à cet effet par le Comité.

TITEL III. — Geclassificeerde informatie**HOOFDSTUK 1. — De beschermingsmaatregelen van toepassing voor de classificatie en het beheer van geclassificeerde informatie****Afdeling 1. — Algemene bepaling**

Art. 10. De regels betreffende de procedure voor classificatie, het wijzigen van een classificatieniveau en de declassificatie, en de beschermingsmaatregelen verbonden aan de classificatie, vervat in dit besluit, doen geen afbreuk aan de mogelijkheid voor elke minister en de chef van de Algemene Dienst Inlichting en Veiligheid van de Krijgsmacht voor wat Defensie betreft, om bijkomende regels van technische aard voor te schrijven.

Afdeling 2. — Bevoegde personen en overheden voor het classificeren, de wijziging van het classificatieniveau en het declassificeren

Art. 11. De personen of overheden, die onder het gezag of instructie van een administratieve overheid geclassificeerde informatie genereren, evenals de federale procureur en de magistraten die hij hiertoe machtigt en de procureur-generaal die het college van procureurs-generaal vertegenwoordigt in het Coördinatiecomité voor Inlichting en Veiligheid, dienen houder te zijn van een veiligheidsmachtiging van ten minste het niveau "GEHEIM", om, overeenkomstig de wet, de bepalingen van voorliggend besluit en de richtlijnen van de Nationale Veiligheidsoverheid, over te gaan tot :

- 1° het classificeren;
- 2° het wijzigen van een classificatieniveau;
- 3° het declassificeren.

De in het eerste lid bedoelde personen of rechtspersonen kennen een classificatieniveau bedoeld in artikel 4 van de wet toe, zonder een hoger classificatieniveau toe te kennen dan het niveau van veiligheidsmachtiging waarvan zij houder zijn.

Art. 12. Enkel de volgende personen, voor zover ze in het bezit zijn van een veiligheidsmachtiging van het overeenstemmende classificatieniveau, zijn gemachtigd het classificatieniveau "ZEER GEHEIM" te classificeren, te wijzigen of te declassificeren:

- 1° de permanente leden van het Coördinatiecomité voor inlichting en veiligheid;
- 2° de chef Defensie en de door hem hiertoe gemachtigde officieren en burgerambtenaren die ten minste het niveau A hebben en de Defensie-attachés;
- 3° de chef van de Algemene Dienst Inlichting en Veiligheid van de Krijgsmacht en de agenten die hij hiertoe machtigt;
- 4° de administrateur-generaal van de Veiligheid van de Staat en de agenten die hij hiertoe machtigt;
- 5° de commissaris-generaal van de Federale Politie en de leden die hij hiertoe machtigt;
- 6° de directeur-generaal van het Federaal Agentschap voor Nucleaire Controle;
- 7° de secretaris van de Ministerraad;
- 8° de persoon die het secretariaat verzekert van de Nationale Veiligheidsraad;
- 9° de Voorzitter van het directiecomité van de Federale Overheidsdienst Buitenlandse Zaken, Buitenlandse Handel en Ontwikkelingssamenwerking, de leden die hij hiertoe machtigt en de hoofden van de diplomatieke zendingen of de consulaire posten;
- 10° de leidende ambtenaren aangeduid door de Nationale Veiligheidsraad;
- 11° de federale procureur en de magistraten die hij hiertoe machtigt;
- 12° de directeur en de bevoegde leden van het Coördinatieorgaan voor de dreigingsanalyse die door hem worden aangewezen;
- 13° het Vast Comité I, het hoofd van zijn Dienst Enquêtes, zijn griffier en de hiertoe door het Comité aangeduide personeelsleden of leden van de Dienst Enquêtes van het niveau A.

Section 3. — Gestion des informations classifiées

Sous-section 1. — Disposition générale

Art. 13. L'Autorité nationale de Sécurité peut déterminer des mesures supplémentaires de nature administrative et technique pour la gestion des informations classifiées.

Sous-section 2. — Marquages

Art. 14. Les autorités et personnes compétentes pour classifier, modifier le niveau de classification ou déclassifier veillent à ce que les informations classifiées soient marquées conformément aux dispositions du présent arrêté et à ce que ces marquages soient clairement visibles.

Une modification d'un niveau de classification ou une déclassification est également clairement marquée sur les informations classifiées.

Art. 15. Le niveau de classification d'informations classifiées ne peut être ni modifié ni déclassifié sans l'autorisation écrite de l'autorité d'origine, de même que les marquages visés aux articles 16, 17, 18 et 20 ne peuvent pas être modifiés ou supprimés.

Art. 16. L'autorité ou la personne compétente indique clairement et correctement le niveau de classification sur les informations classifiées, conformément aux alinéas 2 et 3, et les éventuelles restrictions de diffusion conformément à l'article 18.

Chaque page d'un document classifié est numérotée et marquée du niveau de classification attribué au document et porte la mention « TRÈS SECRET », « SECRET », « CONFIDENTIEL » ou « RESTREINT », ou la mention « ZEER GEHEIM », « GEHEIM », « VERTROUWELIJK » ou « BEPERKT », selon que le document est rédigé en français ou en néerlandais.

La mention visée à l'alinéa 2 doit être suivie de la mention « (Wet 11.12.1998) » ou de la mention « (Loi 11.12.1998) », selon que le document est rédigé en néerlandais ou en français.

Si le document est rédigé dans une langue autre que le néerlandais ou le français, le marquage en néerlandais ou en français doit être complété par son équivalent international en langue anglaise repris dans le tableau comparatif de l'annexe 1.

À défaut d'un marquage adéquat et complet, conformément aux alinéas 1^{er} à 4 ainsi qu'à l'article 20, le titulaire du document prend contact par écrit avec l'autorité ou la personne compétente pour demander une correction.

A défaut d'une correction, le document en question sera considéré comme non-classifié.

Art. 17. Des parties distinctes d'un même document peuvent requérir des niveaux de classification différents et être marquées en conséquence, y compris si elles sont traitées sous forme électronique.

Art. 18. Il est possible d'apposer des marquages supplémentaires, tels que :

1° des restrictions d'utilisation ou d'accès;

2° la date ou l'événement spécifique au-delà duquel le niveau de classification sera revu ou abrogé.

Art. 19. § 1^{er}. Les informations classifiées échangées dans le cadre de conventions ou de traités internationaux qui lient la Belgique, sont protégées par le niveau de classification belge correspondant, mentionné dans le tableau comparatif de l'annexe 1.

§ 2. Sous réserve des conventions et traités internationaux visés au paragraphe 1^{er}, les informations classifiées échangées dans un cadre international par le Service général du Renseignement et de la Sécurité des Forces armées, le Ministère de la Défense ou par d'autres services publics fédéraux sont, pour ce qui concerne ces services, protégées par le niveau de classification belge correspondant comme déterminé dans les accords conclus à cet effet.

§ 3. Le cas échéant, le niveau de classification belge correspondant ainsi que des marquages supplémentaires seront apposés sur ces informations classifiées.

Afdeling 3. — Beheer van geclassificeerde informatie

Onderafdeling 1. — Algemene bepaling

Art. 13. De Nationale Veiligheidsoverheid kan bijkomende maatregelen van administratieve en technische aard bepalen voor het beheer van geclassificeerde informatie.

Onderafdeling 2. — Markeringen

Art. 14. De bevoegde overheden en personen voor het classificeren, wijzigen van een classificatieniveau en het declassificeren zorgen ervoor dat geclassificeerde informatie overeenkomstig de bepalingen van voorliggend besluit wordt gemarkeerd en dat deze markering duidelijk zichtbaar is.

Een wijziging van het classificatieniveau of een declassificatie wordt eveneens duidelijk zichtbaar gemarkeerd op de geclassificeerde informatie.

Art. 15. Zonder dat de overheid van oorsprong er schriftelijk in heeft toegestemd, wordt het classificatieniveau van geclassificeerde informatie niet gewijzigd of gedeclineerd, noch worden de in de artikelen 16, 17, 18 en 20 bedoelde markeringen gewijzigd of verwijderd.

Art. 16. Het classificatieniveau wordt duidelijk en correct aangegeven door de bevoegde overheid of persoon op de geclassificeerde informatie overeenkomstig het tweede en derde lid en de eventuele verspreidingsbeperkingen overeenkomstig artikel 18.

Elke pagina van een geclassificeerd document wordt genummerd en gemarkeerd met het classificatieniveau dat aan het document wordt toegekend en draagt de vermelding "ZEER GEHEIM", "GEHEIM", "VERTROUWELIJK", "BEPERKT" of de vermelding "TRÈS SECRET", "SECRET", "CONFIDENTIEL" of "RESTREINT", naar gelang het document in het Nederlands of het Frans is opgesteld.

De in het tweede lid bedoelde vermelding moet gevolgd worden door de vermelding "(Wet 11.12.1998)" of door de vermelding "(Loi 11.12.1998)", naar gelang het document in het Nederlands of het Frans is opgesteld.

Indien het document in een andere taal dan het Nederlands of het Frans is opgesteld, moet de markering in het Nederlands of het Frans worden aangevuld met het internationaal equivalent in de Engelse taal dat wordt vermeld in de vergelijkende tabel van bijlage 1.

Bij gebrek aan een correcte en volledige markering overeenkomstig het eerste tot het vierde lid en overeenkomstig artikel 20, neemt de houder van het document schriftelijk contact op met de bevoegde overheid of persoon om een correctie te vragen.

Bij gebrek aan een correctie, wordt het desbetreffende document als niet-geclassificeerd beschouwd.

Art. 17. Afzonderlijke delen van een bepaald document kunnen verschillende classificaties vereisen en kunnen dienovereenkomstig gemarkeerd worden, ook wanneer ze elektronisch worden verwerkt.

Art. 18. Aanvullende markeringen zijn mogelijk, zoals:

1° beperkingen voor het gebruik of de toegang;

2° de datum of de specifieke gebeurtenis waarna het classificatieniveau wordt herzien of opgeheven.

Art. 19. § 1. De geclassificeerde informatie die uitgewisseld wordt in het kader van internationale overeenkomsten of verdragen die België binden, zijn beschermd met het overeenstemmende Belgische classificatieniveau bedoeld in de vergelijkende tabel van bijlage 1.

§ 2. Onder voorbehoud van de internationale overeenkomsten of verdragen die België binden bedoeld in paragraaf 1, wordt de geclassificeerde informatie uitgewisseld in een internationaal kader door de Algemene Dienst Inlichting en Veiligheid van de Krijgsmacht, het Ministerie van Landsverdediging, of door andere federale overheidsdiensten, voor wat deze diensten betreft, beschermd met het overeenstemmende Belgische classificatieniveau zoals bepaald in overeenkomsten die hiertoe werden afgesloten.

§ 3. Waar nodig wordt deze geclassificeerde informatie gemarkeerd met het overeenstemmende Belgische classificatieniveau en aanvullende markeringen.

Sous-section 3. — Déclassification du niveau de classification « RESTREINT »

Art. 20. Les informations classifiées au niveau de classification « RESTREINT » indiqueront une date de finalisation et resteront classifiées pendant maximum dix ans après cette date, à moins qu'une date ne soit expressément indiquée sous la mention « RESTREINT » à partir de laquelle ces informations sont automatiquement déclassifiées. Cette dernière date ne peut pas dépasser dix ans après la date de finalisation de l'information classifiée au niveau « RESTREINT ».

L'article 7, § 5, de la loi s'applique aux informations classifiées de niveau « RESTREINT » émanant d'une autorité d'origine étrangère ou supranationale ainsi qu'aux informations classifiées mixtes.

Sous-section 4. — Classification ou déclassification collectives

Art. 21. Des pièces existantes peuvent faire l'objet d'une classification ou déclassification collectives suite à la décision expresse de l'autorité d'origine.

La classification ou la déclassification collectives consistent à attribuer ou à abroger un degré de classification général à un ensemble de documents, à un fichier ou à un ensemble de dossiers identifiables par sujet, sur quelque support que ce soit, sans procéder à la classification ou à la déclassification détaillées pour chaque document, fiche ou dossier.

Les dispositions de la sous-section 2 ne s'appliquent pas aux documents classifiés en vertu des alinéas 1^{er} et 2.

Sous-section 5. — Enregistrement

Art. 22. L'enregistrement indique sans équivoque le titulaire clairement identifié auquel les informations classifiées sont attribuées.

Art. 23. Par dérogation à l'article 22, les informations classifiées de niveau « RESTREINT » ne sont pas enregistrées. Par la seule prise de connaissance de ces informations, le titulaire assume la responsabilité de la protection de ces informations classifiées, conformément à la loi, au présent arrêté et aux directives de l'Autorité nationale de Sécurité, après avoir été informé par l'autorité d'origine des restrictions d'utilisation des informations classifiées de niveau « RESTREINT » et des mesures de protection applicables.

Lorsqu'elles entrent dans l'entité ou sortent de cette entité, les informations classifiées de niveau « CONFIDENTIEL » ou « SECRET » sont toujours enregistrées dans un registre spécialement prévu à cet effet.

Les informations classifiées de niveau « TRÈS SECRET » sont toujours enregistrées dans un registre spécialement prévu à cet effet, distinct du registre visé à l'alinéa 2.

Les informations classifiées de niveau « CONFIDENTIEL » qui sont imprimées par un membre du personnel de l'entité et qui ne sortent pas de l'entité, ne sont pas enregistrées.

Les projets de textes, les documents de travail et les impressions personnelles d'informations classifiées de niveau « SECRET », s'ils ne sortent pas de l'entité, ne doivent pas être enregistrés pendant 5 jours ouvrables. Une fois que ce délai de 5 jours ouvrables à compter de l'impression du document est écoulé, il convient de les détruire ou de les enregistrer.

Les registres non-électroniques visés aux alinéas 2 et 3 peuvent aussi être tenus sous une forme électronique qui remplit les conditions relatives au niveau de classification « CONFIDENTIEL » au moins, conformément à la loi, au présent arrêté et aux directives de l'Autorité nationale de Sécurité.

Art. 24. L'utilisation d'informations classifiées dans un système de communication et d'information approuvé doit être enregistrée au moyen de processus internes à ce système de communication et d'information.

Art. 25. Les titulaires des informations classifiées de niveau « SECRET » ou « TRÈS SECRET » en connaissent la localisation.

Onderafdeling 3. — Declassificatie van het classificatieniveau "BEPERKT"

Art. 20. Geclassificeerde informatie met het classificatieniveau "BEPERKT" vermeldt een datum van finalisatie en blijft gedurende maximum tien jaar geclassificeerd na deze datum, tenzij er uitdrukkelijk een datum wordt vermeld onder de vermelding "BEPERKT" vanaf wanneer dit classificatieniveau automatisch wordt gedeclineerd. Deze laatste datum mag niet meer dan tien jaar bedragen na de finalisatie van de geclassificeerde informatie.

Voor wat betreft geclassificeerde informatie met het classificatieniveau "BEPERKT" die uitgaat van een buitenlandse of supranationale overheid van oorsprong en de gemengde geclassificeerde informatie, geldt artikel 7, § 5 van de wet.

Onderafdeling 4. — Collectief classificeren of declassificeren

Art. 21. Bestaande stukken kunnen het voorwerp uitmaken van het collectief classificeren of declassificeren na de uitdrukkelijke beslissing hiertoe van de overheid van oorsprong.

Het collectief classificeren of declassificeren bestaat uit de toekenning of opheffing van een algemeen classificatieniveau aan een geheel van documenten, een bestand of een geheel van dossiers die identificeerbaar zijn per onderwerp, op om het even welke drager, zonder over te gaan tot het gedetailleerd classificeren of declassificeren voor elk document, bestand of dossier.

De bepalingen van onderafdeling 2 zijn niet van toepassing op de krachtens het eerste en het tweede lid geclassificeerde documenten.

Onderafdeling 5. — Registratie

Art. 22. De registratie stelt ondubbelzinnig een duidelijk geïdentificeerde houder vast aan wie de geclassificeerde informatie is toegevoegd.

Art. 23. In afwijking van artikel 22, wordt geclassificeerde informatie met het classificatieniveau "BEPERKT" niet geregistreerd. De houder neemt door de enkele kennisname van deze informatie de verantwoordelijkheid op zich voor de bescherming van deze geclassificeerde informatie in overeenstemming met de wet, het voorliggend besluit en de richtlijnen van de Nationale Veiligheidsoverheid nadat hij door de overheid van oorsprong werd geïnformeerd over de beperkingen op de aanwending van de geclassificeerde informatie van het classificatieniveau "BEPERKT" en de van toepassing zijnde beschermingsmaatregelen.

Geclassificeerde informatie met het classificatieniveau "VERTROUWELIJK" of "GEHEIM" wordt steeds geregistreerd in een speciaal daartoe bestemd register wanneer het bij de entiteit aankomt of deze verlaat.

Geclassificeerde informatie met het classificatieniveau "ZEER GEHEIM" wordt steeds in een speciaal daartoe bestemd register geregistreerd, gescheiden van het register bedoeld in het tweede lid.

Geclassificeerde informatie met het classificatieniveau "VERTROUWELIJK" die wordt afgedrukt door een personeelslid van de entiteit en die de entiteit niet verlaat, wordt niet geregistreerd.

Ontwerpteksten, werkdocumenten en persoonlijke afdrucken van geclassificeerde informatie met het classificatieniveau "GEHEIM" moeten gedurende vijf werkdagen niet worden geregistreerd indien ze de entiteit niet verlaten. Op het moment dat er vijf werkdagen zijn verstreken sinds het document werd afgedrukt, dient het ofwel te worden vernietigd ofwel te worden geregistreerd.

De niet-elektronische registers vermeld in het tweede en het derde lid, kunnen aangehouden worden in elektronische vorm, die voldoet aan de voorwaarden voor wat betreft minstens het classificatieniveau "VERTROUWELIJK" in overeenstemming met de wet, het voorliggend besluit en de richtlijnen van de Nationale Veiligheidsoverheid.

Art. 24. De aanwending van geclassificeerde informatie in een goedgekeurd communicatie- en informatiesysteem moet geregistreerd worden door middel van processen binnen dit communicatie- en informatiesysteem.

Art. 25. De houders van de geclassificeerde informatie met het classificatieniveau "GEHEIM" of "ZEER GEHEIM" kennen de plaats ervan.

Sous-section 6. — Reproduction et traduction

Art. 26. La reproduction ou la traduction, partielle ou complète, d'une pièce classifiée « TRÈS SECRET » ne peut avoir lieu sans l'accord écrit préalable exprès de l'autorité d'origine.

Art. 27. Lorsque l'autorité d'origine de documents classifiés du niveau « SECRET » ou inférieur n'a pas imposé de restrictions à leur reproduction ou à leur traduction, lesdits documents peuvent être reproduits ou traduits sur instruction du titulaire.

Art. 28. Les mesures de protection applicables au document original le sont aussi à ses reproductions et à ses traductions.

Sous-section 7. — Transmission et transport

Art. 29. L'information classifiée doit être transmise selon les modalités suivantes :

1° par porteur, sous double enveloppe fermée, le niveau de classification ne figurant que sur l'enveloppe intérieure ; ou

2° par voie électronique, sous la protection de systèmes approuvés par l'Autorité nationale de Sécurité et conformément aux mesures de protection applicables au niveau de classification correspondant aux informations classifiées.

L'Autorité nationale de Sécurité fixe les conditions supplémentaires de nature administrative et technique que cette double enveloppe fermée et ce porteur doivent remplir.

Art. 30. Les informations classifiées de niveau « RESTREINT » peuvent également être envoyées par pli recommandé à la poste, avec accusé de réception, sous double enveloppe fermée. Le niveau de classification ne peut figurer que sur l'enveloppe intérieure.

Art. 31. Les informations classifiées peuvent être transmises sur des supports électroniques conformément à la politique de sécurité de l'Autorité nationale de Sécurité.

Art. 32. Pour la circulation interne d'informations classifiées de niveau « CONFIDENTIEL » ou supérieur au sein d'une entité, celles-ci sont portées sous pli fermé par porteur ou par son titulaire.

L'entité au sein de laquelle circule des informations classifiées de niveau « RESTREINT » est responsable de la mise en place de toutes les mesures de sécurité possibles afin d'en empêcher la consultation inappropriée.

Les informations classifiées peuvent être transportées au sein de l'entité par le titulaire, à la condition que toutes les mesures de sécurité possibles afin d'en empêcher la consultation inappropriée soient effectivement mises en place.

Sous-section 8. — Destruction

Art. 33. Les dispositions de la présente sous-section sont applicables sans préjudice :

1° de l'article 25 de la loi ;

2° des articles 21 et 21/1 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité ;

3° de l'article 5 de la loi du 24 juin 1955 relative aux archives ; et,

4° des articles 132 à 137 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

Le titulaire et l'autorité d'origine d'informations classifiées vérifient régulièrement si la détention des informations classifiées ou de leurs copies présente toujours une utilité et s'il n'y a pas lieu de procéder à leur destruction.

Art. 34. Le titulaire d'informations classifiées de niveau « TRÈS SECRET » ne procède jamais à leur destruction, mais les retourne toujours à leur autorité d'origine.

L'autorité d'origine dresse un procès-verbal de la destruction et de son objet. Ce procès-verbal est signé par ceux qui ont détruit les informations et l'officier de sécurité.

Onderafdeling 6. — Reproductie en vertaling

Art. 26. De gehele of gedeeltelijke reproductie of vertaling van een stuk met het classificatieniveau "ZEER GEHEIM" gebeurt enkel na het uitdrukkelijk schriftelijk voorafgaandelijk akkoord van de overheid van oorsprong.

Art. 27. Indien de overheid van oorsprong op documenten met het classificatieniveau "GEHEIM" of lager geen waarschuwing met betrekking tot de reproductie of het vertalen heeft aangebracht, kunnen deze documenten op instructie door de houder worden gereproduceerd of vertaald.

Art. 28. De beschermingsmaatregelen die voor het originele document gelden, zijn ook van toepassing op de reproducties en de vertalingen.

Onderafdeling 7. — Verzending en vervoer

Art. 29. Geclassificeerde informatie moet op volgende manieren worden doorgezonden:

1° onder dubbele gesloten omslag bij drager waarbij het classificatieniveau enkel kan worden vermeld op de binnenomslag; of

2° met elektronische middelen, beschermd door systemen die zijn goedgekeurd door de Nationale Veiligheidsoverheid en overeenkomstig de toepasselijke beschermingsmaatregelen van het overeenstemmende classificatieniveau van de geclassificeerde informatie.

De bijkomende voorwaarden van administratieve en technische aard waaraan de dubbele gesloten omslag en de drager moeten voldoen worden bepaald door de Nationale Veiligheidsoverheid.

Art. 30. Geclassificeerde informatie met het classificatieniveau "BEPERKT" kan ook verzonden worden via een ter post aangetekende zending met ontvangstmelding onder dubbele gesloten omslag. Het classificatieniveau mag enkel worden vermeld op de binnenomslag.

Art. 31. Geclassificeerde informatie kan worden overgebracht op elektronische dragers overeenkomstig het veiligheidsbeleid van de Nationale Veiligheidsoverheid.

Art. 32. Voor de interne rondzending binnen een entiteit van geclassificeerde informatie met het classificatieniveau "VERTROUWELIJK" of hoger wordt de geclassificeerde informatie onder gesloten omslag gedragen door een drager of door de houder.

De entiteit waarbinnen geclassificeerde informatie met het classificatieniveau "BEPERKT" wordt rondgestuurd is verantwoordelijk voor het nemen van alle mogelijke beschermingsmaatregelen tegen het niet-geëigend inkijken ervan.

Geclassificeerde informatie kan binnen de entiteit worden rondgedragen door de houder, op voorwaarde dat alle mogelijke beschermingsmaatregelen tegen het niet-geëigend inkijken ervan effectief worden genomen.

Onderafdeling 8. — Vernietiging

Art. 33. De bepalingen van voorliggende onderafdeling zijn van toepassing onverminderd:

1° artikel 25 van de wet;

2° de artikelen 21 en 21/1 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten;

3° artikel 5 van de Archiefwet van 24 juni 1995; en

4° de artikelen 132 tot 137 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens.

De houder en de overheid van oorsprong van geclassificeerde informatie gaan regelmatig na of het houden van de geclassificeerde informatie of de kopieën ervan nog enig nut heeft en er niet moet overgegaan worden tot de vernietiging ervan.

Art. 34. Geclassificeerde informatie met het classificatieniveau "ZEER GEHEIM" wordt nooit zelf vernietigd door de houder ervan, maar steeds teruggestuurd naar de overheid van oorsprong van de geclassificeerde informatie.

De overheid van oorsprong stelt een proces-verbaal op dat de vernietiging en haar voorwerp vermeldt. Dit proces-verbaal wordt ondertekend door diegene die de informatie heeft vernietigd en de veiligheidsofficier.

Art. 35. Les informations classifiées de niveau « SECRET » ou inférieur, ainsi que leurs copies, peuvent être détruites par l'autorité d'origine, le titulaire ou l'officier de sécurité du titulaire ou, le cas échéant, par la personne de contact pour la sécurité en cas d'informations classifiées, ou de copies, de niveau « RESTREINT ».

Cette autorité d'origine, ce titulaire ou officier de sécurité enregistre la destruction d'informations classifiées de niveau « CONFIDENTIEL » ou « SECRET » dans le registre visé à l'article 23.

Sous-section 9. — Incidents de sécurité et compromission

Art. 36. En cas d'incident de sécurité concernant des informations classifiées, l'officier de sécurité ou, le cas échéant, la personne de contact pour la sécurité des informations classifiées concernées en sont immédiatement avertis.

L'officier de sécurité ou, le cas échéant, la personne de contact pour la sécurité procède à une enquête administrative interne et avertit simultanément la personne qui dirige l'administration, la cellule stratégique, le service, l'organisme ou l'entreprise où il est désigné, ainsi que l'Autorité nationale de Sécurité.

Si nécessaire, l'Autorité nationale de Sécurité informe l'autorité d'origine des informations classifiées.

Art. 37. L'officier de sécurité signale une compromission d'informations classifiées de niveau « CONFIDENTIEL » ou supérieur à l'Autorité nationale de Sécurité immédiatement, qui en informe l'autorité d'origine.

En cas d'incident de sécurité ou de compromission dont la surveillance est due à l'officier de sécurité ou à la personne de contact pour la sécurité, la direction de l'entité à laquelle appartient l'officier de sécurité ou la personne de contact pour la sécurité est tenue d'en informer l'Autorité nationale de Sécurité immédiatement après en avoir pris connaissance.

Art. 38. L'officier de sécurité ou, le cas échéant, la personne de contact pour la sécurité transmet chaque année, avant le 15 mars, un aperçu des incidents de sécurité et des compromissions au cours de l'année précédente à l'Autorité nationale de Sécurité.

CHAPITRE 2. — Mesures de protection physique

Section 1. — Dispositions générales

Art. 39. L'Autorité nationale de Sécurité détermine les mesures de protection physique minimales supplémentaires de nature administrative et technique pour l'utilisation d'informations classifiées au sein et en dehors des zones visées à l'article 42.

Art. 40. Les mesures de protection physique visent à prévenir l'utilisation inappropriée d'informations classifiées en :

1° garantissant que les informations classifiées sont traitées et stockées conformément à la loi, au présent arrêté et aux directives de l'Autorité nationale de Sécurité ;

2° permettant d'établir une distinction entre les membres du personnel au regard de l'accès aux informations classifiées sur la base de leur besoin d'en connaître et, le cas échéant, de leur niveau d'habilitation de sécurité ;

3° dissuadant, en empêchant et en détectant les actes non autorisés ;

4° empêchant ou en retardant toute intrusion par la ruse ou par la force.

Art. 41. Les informations classifiées de niveau « TRÈS SECRET » ne peuvent être consultées que dans la zone sécurisée, telle que visée à l'article 42, 2°.

Les informations classifiées de niveau « CONFIDENTIEL » ou « SECRET » ne peuvent être consultées en dehors des zones visées à l'article 42.

En cas de consultation d'informations classifiées dans la zone administrative, telle que visée à l'article 42, 1°, il est strictement nécessaire que toutes les précautions possibles soient prises afin d'écarter tout risque de consultation ou d'écoute inappropriée.

Les informations classifiées de niveau « RESTREINT » peuvent être consultées en dehors des zones visées à l'article 42, si et seulement si toutes les précautions nécessaires ont été prises afin d'écarter tout risque de consultation ou d'écoute inappropriée.

Art. 35. Geclassificeerde informatie met het classificatieniveau "GEHEIM" en lager, evenals de kopieën ervan, kunnen vernietigd worden door de overheid van oorsprong, de houder of de veiligheids-officier van de houder of in voorkomend geval door de contactpersoon voor de veiligheid in het geval van geclassificeerde informatie met het classificatieniveau "BEPERKT" of de kopieën daarvan.

Deze overheid van oorsprong, de houder of veiligheids-officier registreert de vernietiging van de geclassificeerde informatie met het classificatieniveau "VERTROUWELIJK" of GEHEIM in het register bedoeld in artikel 23.

Onderafdeling 9. — Veiligheidsincident en compromittering

Art. 36. In geval van een veiligheidsincident betreffende geclassificeerde informatie, worden de veiligheids-officier of in voorkomend geval de contactpersoon voor de veiligheid van de desbetreffende geclassificeerde informatie onmiddellijk verwittigd.

De veiligheids-officier of in voorkomend geval de contactpersoon voor de veiligheid gaat over tot een intern administratief onderzoek en brengt tegelijkertijd de persoon die het bestuur, de beleids-cel, de dienst, de instelling of het bedrijf leidt waar hij is aangeduid, op de hoogte, evenals de Nationale Veiligheidsoverheid.

De Nationale Veiligheidsoverheid informeert zo nodig de overheid van oorsprong van de geclassificeerde informatie.

Art. 37. Een compromittering van geclassificeerde informatie met het classificatieniveau "VERTROUWELIJK" of hoger wordt onmiddellijk door de veiligheids-officier gerapporteerd aan de Nationale Veiligheidsoverheid, die de overheid van oorsprong informeert.

In het geval van een veiligheidsincident of compromittering te wijten aan de veiligheids-officier of de contactpersoon voor de veiligheid, moet de directie van de entiteit waartoe de veiligheids-officier of de contactpersoon voor de veiligheid behoort de Nationale Veiligheidsoverheid onmiddellijk informeren nadat deze er van op de hoogte werd gesteld.

Art. 38. De veiligheids-officier of in voorkomend geval de contactpersoon voor de veiligheid maakt jaarlijks vóór 15 maart een overzicht van de veiligheidsincidenten en compromitteringen van het afgelopen jaar over aan de Nationale Veiligheidsoverheid.

HOOFDSTUK 2. — De fysieke beschermingsmaatregelen

Afdeling 1. — Algemene bepalingen

Art. 39. De bijkomende minimale fysieke beschermingsmaatregelen van administratieve en technische aard voor de aanwending van geclassificeerde informatie binnen en buiten de zones zoals bedoeld in artikel 42 worden bepaald door de Nationale Veiligheidsoverheid.

Art. 40. Fysieke beschermingsmaatregelen zijn bedoeld om de niet-geëigende aanwending van geclassificeerde informatie te voorkomen door:

1° ervoor te zorgen dat geclassificeerde informatie wordt verwerkt en opgeslagen in overeenstemming met de wet, het voorliggend besluit en de richtlijnen van de Nationale Veiligheidsoverheid;

2° op basis van het "noodzaak tot kennisname"-beginsel, en in voorkomend geval, van hun niveau van veiligheidsmachtiging, een onderscheid tussen personeelsleden mogelijk te maken wat de toegang tot geclassificeerde informatie betreft;

3° acties waarvoor geen toestemming is verleend, af te schrikken, tegen te houden en op te sporen;

4° het binnendringen door list of geweld te verhinderen of te vertragen.

Art. 41. De geclassificeerde informatie met het classificatieniveau "ZEER GEHEIM" wordt enkel geraadpleegd in de beveiligde zone, zoals bedoeld in artikel 42, 2°.

De geclassificeerde informatie met het classificatieniveau "VERTROUWELIJK" of "GEHEIM" wordt niet geraadpleegd buiten de zones die worden vermeld in artikel 42.

Indien de geclassificeerde informatie wordt geraadpleegd in de administratieve zone, zoals bedoeld in artikel 42, 1°, is het strikt noodzakelijk dat alle mogelijke voorzorgsmaatregelen in acht worden genomen opdat er geen risico tot het niet-geëigend inkijken of af luisteren is.

De geclassificeerde informatie met het classificatieniveau "BEPERKT" kan worden geraadpleegd buiten de zones die worden vermeld in artikel 42, maar enkel en alleen als alle nodige voorzorgsmaatregelen in acht worden genomen opdat er geen risico tot het niet-geëigend inkijken of af luisteren is.

Section 2. — Zones administratives et sécurisées

Art. 42. Sans préjudice de l'article 39, deux types de zones physiquement protégées sont créés, afin de protéger physiquement les informations classifiées, au sein d'une installation physique:

- 1° la zone administrative ; et
- 2° la zone sécurisée.

Art. 43. Les zones administratives doivent au moins répondre aux conditions suivantes :

1° un périmètre défini est établi de façon visible afin de permettre le contrôle des personnes et, dans la mesure du possible, des véhicules ;

2° seules les personnes qui y ont été spécifiquement autorisées par le chef de l'entité ou son remplaçant en vue d'accomplir un rôle ou une tâche spécifique peuvent pénétrer dans cette zone sans être escortées par une personne habilitée ;

3° si le chef de l'entité ou son remplaçant autorise d'autres personnes à pénétrer dans cette zone, celles-ci sont toujours escortées par une personne habilitée.

Art. 44. § 1^{er}. Les zones sécurisées doivent au moins répondre aux conditions suivantes :

1° un périmètre défini et protégé est établi de façon visible avec un système de contrôle d'accès ;

2° sans préjudice des compétences propres des autorités judiciaires, seules les personnes titulaires d'une habilitation de sécurité conforme et qui ont été spécifiquement autorisées par le chef de l'entité ou son remplaçant à pénétrer dans la zone sur la base de leur besoin d'en connaître ou afin d'y accomplir un rôle ou une tâche spécifique, peuvent accéder à cette zone sans être escortées par une personne habilitée ;

3° les personnes qui ne sont pas titulaires d'une habilitation de sécurité conforme, et qui n'ont pas été spécifiquement autorisées par le chef de l'entité ou son remplaçant à pénétrer dans la zone sur la base de leur besoin d'en connaître ou en vue d'y accomplir un rôle ou une tâche spécifique, sont toujours escortées par une personne habilitée ;

4° les visiteurs sont enregistrés dans un registre des visites.

§ 2. Les autorités d'origine visées à l'article 12 sont habilitées, en collaboration avec leur officier de sécurité, à établir des zones sécurisées.

Art. 45. Si l'officier de sécurité estime que l'installation physique répond aux exigences pour être approuvée à partir du niveau de classification « CONFIDENTIEL », il envoie une déclaration de conformité à l'Autorité nationale de Sécurité.

Art. 46. L'Autorité nationale de Sécurité vérifie la déclaration de conformité et peut effectuer une enquête de terrain à cet effet.

Art. 47. § 1^{er}. L'Autorité nationale de Sécurité notifie sa décision concernant l'approbation de l'installation physique à partir du niveau de classification « CONFIDENTIEL » à l'officier de sécurité.

§ 2. La décision d'approbation de l'installation physique a une durée de validité de cinq ans au maximum.

Une demande de renouvellement de cette décision peut être introduite entre le troisième et le sixième mois avant la date d'expiration de sa validité par l'officier de sécurité auprès de l'Autorité nationale de Sécurité, conformément à l'article 45.

§ 3. En l'absence de décision définitive de l'Autorité nationale de Sécurité dans le cas du paragraphe 2, alinéa 2, l'Autorité nationale de Sécurité accorde une approbation à titre provisoire de sorte que l'installation physique concernée puisse continuer à être utilisée dans l'attente d'une décision définitive de l'Autorité nationale de Sécurité.

Art. 48. Tout changement apporté à l'installation physique doit être immédiatement signalé à l'Autorité nationale de Sécurité.

L'Autorité nationale de Sécurité vérifie le changement et, si elle l'estime nécessaire, peut procéder à une nouvelle enquête de terrain.

L'Autorité nationale de Sécurité notifie à l'officier de sécurité sa décision d'approbation de l'installation physique.

Afdeling 2. — Administratieve en beveiligde zones

Art. 42. Onverminderd artikel 39, worden voor de fysieke bescherming van geclassificeerde informatie twee soorten fysiek beschermde zones binnen een fysieke installatie ingesteld:

- 1° de administratieve zone; en
- 2° de beveiligde zone.

Art. 43. Administratieve zones moeten minstens aan volgende voorwaarden voldoen:

1° er wordt een duidelijk omschreven afscheiding ingesteld waar personen en indien mogelijk voertuigen kunnen worden gecontroleerd;

2° enkel personen die door het hoofd van de entiteit of zijn plaatsvervanger specifiek zijn geautoriseerd met het oog op het vervullen van een specifieke rol of taak, hebben toegang tot deze zone zonder begeleiding van een gemachtigd persoon;

3° wanneer aan andere personen de toegang tot deze zone wordt verleend door het hoofd van de entiteit of zijn plaatsvervanger, worden deze altijd begeleid door een gemachtigd persoon.

Art. 44. § 1. Beveiligde zones moeten minstens aan volgende voorwaarden voldoen:

1° er wordt een duidelijk omschreven, beschermde afscheiding ingesteld met een toegangscontrolesysteem;

2° onverminderd de eigen bevoegdheden van de gerechtelijke overheden, hebben enkel personen die beschikken over een overeenkomstige veiligheidsmachtiging en specifiek geautoriseerd zijn door het hoofd van de entiteit of zijn plaatsvervanger om de zone te betreden op basis van zijn noodzaak tot kennisname of met het oog op het vervullen van een specifieke rol of taak, toegang tot deze zone zonder begeleiding van een gemachtigd persoon;

3° de personen die niet beschikken over de overeenstemmende veiligheidsmachtiging, en niet specifiek zijn geautoriseerd door het hoofd van de entiteit of zijn plaatsvervanger om de zone te betreden op basis van zijn noodzaak tot kennisname of met het oog op het vervullen van een specifieke rol of taak, worden altijd begeleid door een gemachtigd persoon;

4° de bezoekers worden geregistreerd in een bezoekersregister.

§ 2. De in artikel 12 bedoelde overheden van oorsprong zijn gemachtigd, via hun veiligheidsofficier, beveiligde zones in te stellen.

Art. 45. Indien de veiligheidsofficier van oordeel is dat de fysieke installatie vanaf het classificatieniveau "VERTROUWELIJK" voldoet aan de eisen om te worden goedgekeurd, stuurt hij een conformiteitsverklaring door naar de Nationale Veiligheidsoverheid.

Art. 46. De Nationale Veiligheidsoverheid verifieert de conformiteitsverklaring en kan daartoe een terreinonderzoek uitvoeren.

Art. 47. § 1. De Nationale Veiligheidsoverheid brengt zijn beslissing betreffende de goedkeuring van de fysieke installatie vanaf het classificatieniveau "VERTROUWELIJK" ter kennis van de veiligheids-officier.

§ 2. De beslissing tot goedkeuring van de fysieke installatie heeft een geldigheidsduur van maximum vijf jaar.

Tussen de drie en de zes maanden vóór het einde van de geldigheidsduur kan een hernieuwing van deze beslissing worden aangevraagd door de veiligheidsofficier bij de Nationale Veiligheidsoverheid overeenkomstig artikel 45.

§ 3. Bij gebrek aan een definitieve beslissing van de Nationale Veiligheidsoverheid in het geval van paragraaf 2, tweede lid, kent de Nationale Veiligheidsoverheid een tijdelijke goedkeuring toe, zodat de desbetreffende fysieke installatie verder kan gebruikt worden in afwachting van een definitieve beslissing van de Nationale Veiligheidsoverheid.

Art. 48. Iedere wijziging aan de fysieke installatie dient onverwijld gemeld te worden aan de Nationale Veiligheidsoverheid.

De Nationale Veiligheidsoverheid verifieert de wijziging en kan, indien hij dit nodig acht, een nieuw terreinonderzoek uitvoeren.

De Nationale Veiligheidsoverheid brengt zijn beslissing betreffende de goedkeuring van de wijziging aan de fysieke installatie ter kennis aan de veiligheidsofficier.

CHAPITRE 3. — *Mesures de protection des systèmes de communication et d'information pour les informations classifiées*

Art. 49. L'Autorité nationale de Sécurité détermine les mesures de protection minimales supplémentaires de nature administrative et technique des systèmes de communication et d'information pour les informations classifiées.

Art. 50. Sans préjudice du chapitre 4 du titre III, l'officier de sécurité ou la personne de contact pour la sécurité évalue si un système de communication et d'information offre les garanties suffisantes, définies à l'article 8, § 4, alinéa 2, de la loi, pour utiliser des informations classifiées.

Si l'officier de sécurité ou la personne de contact pour la sécurité estime que le système de communication et d'information répond aux exigences pour utiliser des informations classifiées, il envoie une déclaration de conformité, attestant que les garanties sont remplies, ainsi que la documentation nécessaire à l'Autorité nationale de Sécurité.

Cette déclaration de conformité est signée tant par l'autorité fonctionnelle du système de communication et d'information que par l'officier de sécurité ou la personne de contact pour la sécurité.

Art. 51. L'Autorité nationale de Sécurité vérifie la déclaration de conformité. A cet effet, l'Autorité nationale de Sécurité peut utiliser la documentation technique ou, le cas échéant, demander une documentation technique supplémentaire.

Art. 52. Pour les systèmes de communication et d'information utilisant des informations classifiées de niveau « RESTREINT », l'Autorité nationale de Sécurité peut demander à l'entité de soumettre le système de sécurité concerné à des tests de sécurité afin de vérifier que les garanties suffisantes sont atteintes en termes de confidentialité, d'intégrité, de disponibilité, d'authenticité et de non-répudiation de ces systèmes et des informations qu'ils contiennent. De surcroît, l'Autorité nationale de Sécurité peut vérifier que les mesures techniques et non techniques sont correctement implémentées, intégrées et configurées.

Pour les systèmes de communication et d'information utilisant des informations classifiées de niveau « CONFIDENTIEL » ou supérieur, l'Autorité nationale de Sécurité demande à l'entité de soumettre le système concerné à des tests de sécurité afin de vérifier que les garanties suffisantes sont atteintes en termes de confidentialité, d'intégrité, de disponibilité, d'authenticité et de non-répudiation de ces systèmes et des informations qu'ils contiennent. De surcroît, l'Autorité nationale de Sécurité vérifie que les mesures techniques et non techniques sont correctement implémentées, intégrées et configurées.

Art. 53. § 1^{er}. L'Autorité nationale de Sécurité notifie sa décision concernant l'approbation du système de communication et d'information à l'autorité fonctionnelle du système de communication et d'information et à l'officier de sécurité ou la personne de contact pour la sécurité.

§ 2. La décision d'approbation du système de communication et d'information dispose d'une durée de validité de trois ans au maximum.

Une demande de renouvellement de cette décision peut être introduite entre le sixième et le septième mois avant la date d'expiration de sa validité par l'officier de sécurité ou la personne de contact pour la sécurité auprès de l'Autorité nationale de Sécurité, conformément à l'article 50.

§ 3. En l'absence de décision définitive de l'Autorité nationale de Sécurité dans le cas du paragraphe 2, alinéa 2, l'Autorité nationale de Sécurité accorde une prolongation à titre provisoire de sorte que le système de communication et d'information concerné puisse continuer à être utilisé dans l'attente d'une décision définitive de l'Autorité nationale de Sécurité.

CHAPITRE 4. — *Mesures de protection relatives au matériel cryptographique destiné au traitement d'informations classifiées*

Section 1^{re}. — Généralités

Art. 54. L'Autorité nationale de Sécurité fixe les exigences minimales administratives et techniques en termes d'évaluation, d'approbation, d'utilisation, y compris le compte cryptographique, de transport, de partage, de conservation, de gestion, y compris la production des clés cryptographiques, et de destruction du matériel cryptographique destiné au traitement des informations classifiées.

HOOFDSTUK 3. — *De beschermingsmaatregelen van communicatie- en informatiesystemen voor geclassificeerde informatie*

Art. 49. De bijkomende minimale beschermingsmaatregelen van administratieve en technische aard van communicatie- en informatiesystemen voor geclassificeerde informatie worden bepaald door de Nationale Veiligheidsoverheid.

Art. 50. Onverminderd hoofdstuk 4 van titel III, beoordeelt de veiligheidsofficier of de contactpersoon voor de veiligheid of een communicatie- en informatiesysteem voldoende garanties biedt, zoals bepaald in artikel 8, § 4, tweede lid van de wet, om geclassificeerde informatie aan te wenden.

Indien de veiligheidsofficier of de contactpersoon voor de veiligheid van oordeel is dat het communicatie- en informatiesysteem voldoet aan de eisen om geclassificeerde informatie aan te wenden, stuurt hij een conformiteitsverklaring om te bevestigen dat aan de garanties is voldaan, alsook de vereiste documentatie door naar de Nationale Veiligheidsoverheid.

Deze conformiteitsverklaring wordt ondertekend door zowel de functionele autoriteit van het communicatie- en informatiesysteem als de veiligheidsofficier of de contactpersoon voor de veiligheid.

Art. 51. De Nationale Veiligheidsoverheid verifieert de conformiteitsverklaring. De Nationale Veiligheidsoverheid kan hiervoor de technische documentatie gebruiken of desgevallend bijkomende technische documentatie opvragen.

Art. 52. Voor communicatie- en informatiesystemen die geclassificeerde informatie met het classificatieniveau "BEPERKT" aanwenden, kan de Nationale Veiligheidsoverheid de entiteit verzoeken om het desbetreffende systeem te onderwerpen aan beveiligingstests om na te gaan of voldoende garanties zijn bereikt ten aanzien van de vertrouwelijkheid, de integriteit, de beschikbaarheid, de authenticiteit en de niet-weerlegbaarheid van deze systemen en van de informatie die ze bevatten. Tevens kan de Nationale Veiligheidsoverheid nagaan of de technische en niet-technische maatregelen correct zijn geïmplementeerd, geïntegreerd en geconfigureerd.

Voor communicatie- en informatiesystemen die geclassificeerde informatie met het classificatieniveau "VERTROUWELIJK" of hoger aanwenden, verzoekt de Nationale Veiligheidsoverheid de entiteit om het desbetreffende systeem te onderwerpen aan beveiligingstests om na te gaan of voldoende garanties zijn bereikt ten aanzien van de vertrouwelijkheid, de integriteit, de beschikbaarheid, de authenticiteit en de niet-weerlegbaarheid van deze systemen en van de informatie die ze bevatten. Tevens gaat de Nationale Veiligheidsoverheid na of de technische en niet-technische maatregelen correct zijn geïmplementeerd, geïntegreerd en geconfigureerd.

Art. 53. § 1. De Nationale Veiligheidsoverheid brengt zijn beslissing betreffende de goedkeuring van het communicatie- en informatiesysteem ter kennis van de functionele autoriteit van het communicatie- en informatiesysteem en de veiligheidsofficier of de contactpersoon voor de veiligheid.

§ 2. De beslissing tot goedkeuring van het communicatie- en informatiesysteem heeft een geldigheidsduur van maximum drie jaar.

Tussen de zes en de zeven maanden vóór het einde van de geldigheidsduur kan een hernieuwing van deze beslissing worden aangevraagd door de veiligheidsofficier of de contactpersoon voor de veiligheid bij de Nationale Veiligheidsoverheid overeenkomstig artikel 50.

§ 3. Bij gebrek aan een definitieve beslissing van de Nationale Veiligheidsoverheid in het geval van paragraaf 2, tweede lid, kent de Nationale Veiligheidsoverheid een tijdelijke verlenging toe, zodat het desbetreffende communicatie- en informatiesysteem verder kan gebruikt worden in afwachting van een definitieve beslissing van de Nationale Veiligheidsoverheid.

HOOFDSTUK 4. — *De beschermingsmaatregelen verbonden aan cryptografisch materiaal voor de behandeling van geclassificeerde informatie*

Afdeling 1. — Algemeen

Art. 54. De minimale administratieve en technische vereisten voor de evaluatie, de goedkeuring, het gebruik, waaronder de cryptografische account, het transport, de verdeling, de bewaring, het beheer, met inbegrip van de productie van cryptografische sleutels, en de vernietiging van cryptografisch materiaal voor de behandeling van geclassificeerde informatie worden bepaald door de Nationale Veiligheidsoverheid.

Art. 55. Seuls les produits cryptographiques approuvés par l'Autorité nationale de Sécurité peuvent être utilisés pour stocker, traiter et transmettre des informations classifiées.

Art. 56. L'Autorité nationale de Sécurité est l'unique point de contact entre les autorités fonctionnelles d'un système de communication et d'information et les titulaires de comptes cryptographiques de produits cryptographiques destinés au traitement d'informations classifiées, d'une part, et les autorités internationales, d'autre part.

Section 2. — Procédure d'approbation de produits cryptographiques

Art. 57. Si l'autorité fonctionnelle d'un système de communication et d'information estime que le produit cryptographique offre les garanties suffisantes pour fournir des services de sécurité, tel que défini à l'article 8, § 4, alinéa 3 de la loi, il introduit une demande d'approbation auprès de l'Autorité nationale de Sécurité.

Art. 58. Le produit cryptographique est évalué par l'Autorité nationale de Sécurité ou à la demande de l'Autorité nationale de Sécurité par :

1° le Service général du Renseignement et de la Sécurité des Forces armées ; ou

2° un autre organisme conformément à la politique de sécurité de l'Autorité nationale de Sécurité.

Les instances visées au premier alinéa dressent un rapport d'évaluation.

L'Autorité nationale de Sécurité apprécie le rapport d'évaluation.

Art. 59. Pour les produits cryptographiques utilisant des informations classifiées, l'Autorité nationale de Sécurité demande à l'autorité fonctionnelle d'un système de communication et d'information de soumettre le produit concerné à des tests de sécurité afin de vérifier qu'il offre les garanties suffisantes quant à la fourniture de services de sécurité, en particulier sur le plan de la confidentialité, de l'intégrité, de la disponibilité, de l'authenticité et de la non-répudiation.

Art. 60. L'Autorité nationale de Sécurité peut demander à un autre pays ou à une autre instance de procéder à une seconde évaluation.

Art. 61. Un produit cryptographique obtient l'approbation de l'Autorité nationale de Sécurité sur la base d'une évaluation satisfaisante des garanties quant à la fourniture de services de sécurité, en particulier sur le plan de la confidentialité, de l'intégrité, de la disponibilité, de l'authenticité et de la non-répudiation.

L'Autorité nationale de Sécurité notifie sa décision concernant l'approbation du produit cryptographique à l'autorité fonctionnelle d'un système de communication et d'information.

La décision d'approbation du produit cryptographique a une validité de trois ans au maximum. Une demande de prorogation de cette décision peut être introduite jusqu'à six mois avant la date d'expiration de sa validité.

Art. 62. L'Autorité nationale de Sécurité tient un registre des produits cryptographiques qu'elle a approuvés.

Art. 63. L'autorité fonctionnelle d'un système de communication et d'information procède au moins une fois par an à une analyse des menaces relatives aux éventuelles compromissions du produit cryptographique approuvé et la transmet à l'Autorité nationale de Sécurité.

Section 3. — Gestion et distribution du matériel cryptographique

Art. 64. Une entité souhaitant utiliser du matériel cryptographique pour les informations classifiées doit être en possession d'un compte cryptographique délivrée par l'Autorité nationale de Sécurité et doit en outre appliquer les mesures de protection énoncées à l'article 7, § 1^{er} de la loi.

Une demande de compte cryptographique doit être introduite auprès de l'Autorité nationale de Sécurité.

L'Autorité nationale de Sécurité fixe les conditions auxquelles un compte cryptographique doit répondre.

Art. 65. Le possesseur d'un compte cryptographique tient un registre du matériel cryptographique qu'il gère.

Art. 55. Het bewaren, verwerken en doorsturen van geclassificeerde informatie via elektronische middelen gebeurt enkel mits het gebruik van door de Nationale Veiligheidsoverheid goedgekeurde cryptografische producten.

Art. 56. De Nationale Veiligheidsoverheid is het enige contactpunt tussen enerzijds functionele autoriteiten van een communicatie- en informatiesysteem en houders van een cryptografische account van cryptografische producten voor de behandeling van geclassificeerde informatie en anderzijds internationale autoriteiten.

Afdeling 2. — Goedkeuringsprocedure voor cryptografische producten

Art. 57. Indien de functionele autoriteit van een communicatie- en informatiesysteem van oordeel is dat het cryptografisch product voldoende garanties biedt voor het verlenen van beveiligingsdiensten, zoals bepaald in artikel 8, § 4, derde lid van de wet, stuurt hij een verzoek tot goedkeuring door naar de Nationale Veiligheidsoverheid.

Art. 58. Het cryptografisch product wordt geëvalueerd door de Nationale Veiligheidsoverheid of op vraag van de Nationale Veiligheidsoverheid door:

1° de Algemene Dienst Inlichting en Veiligheid van de Krijgsmacht; of

2° een door haar aangewezen andere instantie overeenkomstig het veiligheidsbeleid van de Nationale Veiligheidsoverheid.

De in het eerste lid vermelde instanties stellen een evaluatierapport op.

De Nationale Veiligheidsoverheid beoordeelt het evaluatierapport.

Art. 59. Voor cryptografische producten die geclassificeerde informatie aanwenden, verzoekt de Nationale Veiligheidsoverheid de functionele autoriteit van een communicatie- en informatiesysteem om het desbetreffende product te onderwerpen aan beveiligingstests om na te gaan of voldoende garanties zijn bereikt voor het verlenen van beveiligingsdiensten, in het bijzonder op het vlak van de vertrouwelijkheid, de integriteit, de beschikbaarheid, de authenticiteit en de niet-weerlegbaarheid.

Art. 60. De Nationale Veiligheidsoverheid kan een ander land of een andere instantie verzoeken om een tweede evaluatie uit te voeren.

Art. 61. Goedkeuring van een cryptografisch product wordt door de Nationale Veiligheidsoverheid verleend op basis van een bevredigende beoordeling betreffende de garanties voor het verlenen van beveiligingsdiensten, in het bijzonder op het vlak van de vertrouwelijkheid, de integriteit, de beschikbaarheid, de authenticiteit en de niet-weerlegbaarheid.

De Nationale Veiligheidsoverheid brengt zijn beslissing betreffende de goedkeuring van het cryptografisch product ter kennis van de functionele autoriteit van een communicatie- en informatiesysteem.

De beslissing tot goedkeuring van het cryptografisch product heeft een geldigheidsduur van maximum drie jaar. Tot zes maanden vóór het einde van de geldigheidsduur kan een hernieuwing van deze beslissing worden aangevraagd.

Art. 62. De Nationale Veiligheidsoverheid houdt een register bij van de door haar goedgekeurde cryptografische producten.

Art. 63. De functionele autoriteit van een communicatie- en informatiesysteem voert minstens jaarlijks een dreigingsanalyse uit met betrekking tot mogelijke compromitteringen van het goedgekeurd cryptografisch product en bezorgt deze aan de Nationale Veiligheidsoverheid.

Afdeling 3. — Beheer en verdeling van cryptografisch materiaal

Art. 64. Een entiteit die cryptografisch materiaal wenst te gebruiken voor geclassificeerde informatie, moet in het bezit zijn van een cryptografische account afgeleverd door de Nationale Veiligheidsoverheid en moet eveneens voldoen aan de in artikel 7, § 1 van de wet vernoemde beschermingsmaatregelen.

Een aanvraag tot het bekomen van een cryptografische account wordt ingediend bij de Nationale Veiligheidsoverheid.

De voorwaarden waaraan een cryptografische account moet voldoen worden vastgelegd door de Nationale Veiligheidsoverheid.

Art. 65. De bezitter van een cryptografische account houdt een register bij van het cryptografisch materiaal dat hij beheert.

Art. 66. L'Autorité nationale de Sécurité tient un registre du matériel cryptographique qu'elle a distribué.

Section 4. — Situations d'urgence

Art. 67. Les informations classifiées de niveau de classification « RESTREINT » ou « CONFIDENTIEL » peuvent être transmises au moyen d'un produit cryptographique approuvé pour un niveau de classification inférieur ou sans cryptage, lorsque les circonstances exceptionnelles suivantes se produisent simultanément :

(a) une crise, un conflit ou une situation de guerre menace d'éclater ou a éclaté ; et

(b) il est d'une importance capitale de recevoir les informations rapidement, le cryptage n'est pas disponible et l'on estime que les informations classifiées concernées arriveront trop tardivement pour neutraliser la menace.

Art. 68. Dans des circonstances exceptionnelles, lorsqu'il est capital d'agir rapidement, que le cryptage est indisponible et que l'on estime que les informations classifiées concernées arriveront trop tardivement pour neutraliser la menace, les informations de niveau « RESTREINT » peuvent être transmises sans avoir été cryptées.

Art. 69. Lorsque les articles 67 et 68 sont invoqués, l'officier de sécurité de l'entité qui a transmis les informations classifiées établit ensuite un rapport. Ce rapport est transmis à l'autorité d'origine.

CHAPITRE 5. — Mesures de protection relatives aux personnes physiques ou morales

Section 1^{re}. — Habilitation de sécurité pour les personnes physiques

Sous-section 1. — Généralités

Art. 70. § 1^{er}. Les personnes de nationalité belge qui, dans les limites strictes d'un besoin d'en connaître, ont besoin d'accéder à des informations classifiées à partir du niveau « CONFIDENTIEL » peuvent se voir octroyer une habilitation de sécurité aux conditions prévues par la loi, le présent arrêté et la directive du Conseil national de sécurité, telles que mentionnées à l'article 18, alinéa 5 de la loi.

§ 2. Il en va de même pour les personnes de nationalité étrangère, à condition qu'il s'agisse de ressortissants d'un pays avec lequel la Belgique a conclu un accord en matière d'échange et de protection mutuelle d'informations classifiées, d'où il ressort que :

1° le service de renseignement et de sécurité belge compétent peut effectuer une enquête, conformément aux conditions prévues par la loi, le présent arrêté et la directive du Conseil national de Sécurité visée à l'article 18, alinéa 5 de la loi, ou que les autorités de sécurité visées à l'article 1^{quinièmes} de la loi peuvent, le cas échéant, octroyer une habilitation de sécurité ; ou

2° l'habilitation de sécurité étrangère peut être reconnue par l'Autorité nationale de Sécurité ou par les autorités de sécurité visées à l'article 1^{quinièmes} de la loi.

§ 3. Par dérogation au paragraphe 2, les ressortissants d'un Etat membre de l'Espace économique européen ou de la Confédération suisse qui, dans les limites strictes du besoin d'en connaître, doivent nécessairement avoir accès à des informations classifiées à partir du niveau de classification « CONFIDENTIEL », peuvent se voir délivrer une habilitation de sécurité par l'Autorité nationale de Sécurité ou l'une des autorités visées à l'article 1^{quinièmes} de la loi, si le service de renseignement et de sécurité belge compétent peut effectuer l'enquête de sécurité, conformément aux conditions prévues par la loi, le présent arrêté et la directive du Conseil national de Sécurité, telles que visées à l'article 18, alinéa 5 de la loi.

Sous-section 2. — Procédure de demande

Art. 71. § 1^{er}. Sans préjudice de l'article 93, la demande d'habilitation de sécurité, dûment motivée et signée par l'autorité ou la personne visée au § 2, est adressée, par l'intermédiaire de l'officier de sécurité, à l'Autorité nationale de Sécurité ou, le cas échéant, à l'une des autorités visées à l'article 1^{quinièmes} de la loi.

§ 2. Pour les membres de la cellule stratégique d'un ministre ou d'un secrétaire d'Etat, la demande est signée par le directeur de la cellule stratégique dont relève le membre de la cellule stratégique concerné.

Pour les membres du personnel des administrations publiques, des organismes d'intérêt public ou des entreprises publiques autonomes, la demande est signée par le fonctionnaire dirigeant dont dépend le membre du personnel concerné.

Art. 66. De Nationale Veiligheidsoverheid houdt een register bij van het door haar verdeelde cryptografisch materiaal.

Afdeling 4. — Noodsituaties

Art. 67. Geclassificeerde informatie met het classificatieniveau "BEPERKT" of "VERTROUWELIJK" kan door middel van een voor een lager classificatieniveau goedgekeurd cryptografisch product of zonder versleuteling worden doorgestuurd, wanneer de volgende uitzonderlijke omstandigheden zich tegelijk voordoen :

(a) het gaat om een dreigende of uitgebroken crisis, conflict of oorlogssituatie; en

(b) het van uitermate belang is dat de informatie spoedig wordt ontvangen, encryptie niet beschikbaar is en wanneer men van oordeel is dat de desbetreffende geclassificeerde informatie te laat zal komen om de dreiging te neutraliseren.

Art. 68. In uitzonderlijke omstandigheden, wanneer snelheid van uitermate belang is, encryptie niet beschikbaar is en wanneer men van oordeel is dat de desbetreffende geclassificeerde informatie te laat zal komen om de dreiging te neutraliseren, kan informatie met het classificatieniveau "BEPERKT" onversleuteld worden doorgestuurd.

Art. 69. Indien gebruik wordt gemaakt van artikel 67 of artikel 68, wordt nadien een verslag opgesteld door de veiligheidsofficier van de entiteit die de geclassificeerde informatie heeft verzonden. Dit verslag wordt doorgestuurd naar de overheid van oorsprong.

HOOFDSTUK 5. — De beschermingsmaatregelen gerelateerd aan natuurlijke personen en rechtspersonen

Afdeling 1. — De veiligheidsmachtiging voor natuurlijke personen

Onderafdeling 1. — Algemeen

Art. 70. § 1. Personen met de Belgische nationaliteit die, binnen de strikte grenzen van een noodzaak tot kennisname, toegang nodig hebben tot geclassificeerde informatie vanaf het classificatieniveau "VERTROUWELIJK", kunnen een machtiging krijgen volgens de voorwaarden bepaald in de wet, het voorliggend besluit en de richtlijn van de Nationale Veiligheidsraad, zoals vermeld in artikel 18, vijfde lid van de wet.

§ 2. Hetzelfde geldt voor personen met een buitenlandse nationaliteit op voorwaarde dat zij onderdaan zijn van een land waarmee België een overeenkomst inzake de uitwisseling en de wederzijdse bescherming van geclassificeerde informatie heeft afgesloten, waaruit blijkt dat :

1° de bevoegde Belgische inlichtingen- en veiligheidsdienst het onderzoek kan voeren overeenkomstig de voorwaarden vermeld in de wet, het voorliggend besluit en de richtlijn van de Nationale Veiligheidsraad, zoals vermeld in artikel 18, vijfde lid van de wet of de in artikel 1^{quinièmes} van de wet bedoelde veiligheidsoverheden in voorkomend geval een veiligheidsmachtiging kunnen toekennen; of

2° de buitenlandse veiligheidsmachtiging kan worden erkend door de Nationale Veiligheidsoverheid of de in artikel 1^{quinièmes} van de wet bedoelde veiligheidsoverheden.

§ 3. In afwijking van paragraaf 2 kunnen onderdanen van een lidstaat van de Europese Economische ruimte of de Zwitserse Bondsstaat, die binnen de strikte grenzen van een noodzaak tot kennisname, toegang nodig hebben tot geclassificeerde informatie vanaf het classificatieniveau "VERTROUWELIJK", een veiligheidsmachtiging krijgen van de Nationale Veiligheidsoverheid of de in artikel 1^{quinièmes} van de wet bedoelde veiligheidsoverheden, indien de bevoegde Belgische inlichtingen- en veiligheidsdienst het onderzoek kan voeren overeenkomstig de voorwaarden vermeld in de wet, het voorliggend besluit en de richtlijn van de Nationale Veiligheidsraad, zoals vermeld in artikel 18, vijfde lid van de wet.

Onderafdeling 2. — Aanvraagprocedure

Art. 71. § 1. Onverminderd artikel 93, wordt de aanvraag om een veiligheidsmachtiging, met redenen gemotiveerd en ondertekend door de in paragraaf 2 bedoelde overheid of persoon, via de veiligheidsofficier aan de Nationale Veiligheidsoverheid of, in voorkomend geval, aan één van de in artikel 1^{quinièmes} van de wet bedoelde overheden, gericht.

§ 2. Voor de leden van de beleidscel van een minister of een staatssecretaris wordt de aanvraag ondertekend door de directeur van de beleidscel waarvan het betrokken lid van de beleidscel afhangt.

Voor de personeelsleden van openbare besturen, instellingen van openbaar nut of autonome overheidsbedrijven wordt de aanvraag ondertekend door de leidend ambtenaar waarvan het betrokken personeelslid afhangt.

Au sein du Ministère de la Défense, la demande est signée par l'autorité investie des pouvoirs de chef de corps.

Pour les membres du personnel de la police fédérale, la demande est signée par le commissaire général, le directeur général ou par le directeur dont le membre du personnel relève, ou par la personne qu'ils délèguent à cette fin.

Pour les membres du personnel de la police locale, la demande est signée par le chef de corps ou par la personne qu'il délègue à cet effet.

Pour les organes et préposés des personnes morales autres que celles citées à l'alinéa 2, la demande est signée par la ou les personnes qui assurent la direction de la personne morale dûment habilitée.

Pour le travailleur indépendant sans personnalité juridique, qui travaille exclusivement pour un seul et même donneur d'ordre sur le lieu d'exploitation dans le cadre d'un marché classifié, la demande peut être signée par les personnes mentionnées aux alinéas 2 ou 6, même si ce travailleur indépendant ne relève pas de l'autorité du donneur d'ordre.

Pour un travailleur indépendant doté de la personnalité juridique, dont le siège social est situé en Belgique, qui travaille exclusivement pour un seul et même donneur d'ordre sur le lieu d'exploitation dans le cadre d'un marché public classifié, la demande peut être signée par les personnes mentionnées aux alinéas 2 ou 6, même si ce travailleur indépendant ne relève pas de l'autorité du donneur d'ordre.

Dans les autres cas, la demande est signée par l'autorité directement concernée ou par la personne qui requiert une habilitation de sécurité.

§ 3. Dès que la demande d'habilitation de sécurité est acceptée par l'Autorité nationale de Sécurité ou les autorités de sécurité visées à l'article 1^{quinq}uies de la loi, elle en informe l'officier de sécurité, par écrit, dans les plus brefs délais.

L'officier de sécurité transmet aux personnes qui requièrent une habilitation de sécurité les documents requis par l'article 17 de la loi.

Sous-section 3. — Appréciation de la recevabilité de la demande

Art. 72. L'officier de sécurité vérifie que l'ensemble des documents visés à l'article 17, alinéa 3, de la loi sont dûment complétés par les personnes qui requièrent une habilitation de sécurité.

Si des documents font défaut ou s'ils ne sont pas dûment complétés, l'officier de sécurité en informe les personnes qui requièrent une habilitation de sécurité et leur demande de transmettre les documents manquants ou de compléter les documents dans les plus brefs délais. Le délai de quinze jours visé à l'article 73 ne prend pas cours tant que les documents manquants ou complétés n'ont pas été envoyés à l'officier de sécurité.

Art. 73. Dès la réception des documents visés à l'article 17, alinéa 3, de la loi dûment complétés, l'officier de sécurité dispose d'un délai de quinze jours pour les transmettre à l'Autorité nationale de Sécurité ou aux autorités de sécurité visées à l'article 1^{quinq}uies de la loi.

Art. 74. L'Autorité nationale de Sécurité ou les autorités de sécurité visées à l'article 1^{quinq}uies de la loi vérifient que l'ensemble des documents visés à l'article 17, alinéa 3 de la loi ont été transmis et dûment complétés par les personnes qui requièrent une habilitation de sécurité.

Si des documents font défaut ou n'ont pas été dûment complétés ou si les motifs de la demande ne sont pas suffisamment précis, corrects ou convaincants, la demande est déclarée irrecevable. L'Autorité nationale de Sécurité ou les autorités de sécurité visées à l'article 1^{quinq}uies de la loi en informent l'officier de sécurité, qui à son tour avertit les personnes qui requièrent l'habilitation de sécurité.

Lorsque la demande est déclarée recevable par l'Autorité nationale de Sécurité ou les autorités de sécurité visées à l'article 1^{quinq}uies de la loi, l'officier de sécurité en est informé et l'Autorité nationale de Sécurité ou les autorités de sécurité visées à l'article 1^{quinq}uies de la loi transmettent immédiatement les documents visés à l'article 17, alinéa 3 de la loi ainsi que la demande d'enquête de sécurité à effectuer au service de renseignement et de sécurité compétent.

Binnen het Ministerie van Landsverdediging wordt de aanvraag ondertekend door de overheid die bekleed is met de bevoegdheden van korpscommandant.

Voor de personeelsleden van de federale politie wordt de aanvraag ondertekend door de commissaris-generaal, de directeur-generaal of de directeur onder wie het betrokken personeelslid ressorteert, of door de persoon die zij aanwijzen.

Voor de personeelsleden van de lokale politie wordt de aanvraag ondertekend door de korpschef of door de persoon die zij aanwijzen.

Voor de organen en de aangestelden van andere rechtspersonen dan die genoemd in het tweede lid, wordt de aanvraag ondertekend door de persoon of de personen die het bestuur van de naar behoren gemachtigde rechtspersoon verzekeren.

Voor de zelfstandige zonder rechtspersoonlijkheid, die exclusief voor één en dezelfde opdrachtgever werkzaam is op de plaats van de uitbatingsetel in het kader van een geclassificeerde overheidsopdracht, kan de aanvraag ondertekend worden door de personen vermeld in het tweede of zesde lid, ook al ressorteert deze zelfstandige niet onder het werkgeversgezag van de opdrachtgever.

Voor de zelfstandige met rechtspersoonlijkheid, waarvan de statutaire zetel in België is gevestigd, die exclusief voor één en dezelfde opdrachtgever werkzaam is op de plaats van de uitbatingsetel in het kader van een geclassificeerde overheidsopdracht, kan de aanvraag ondertekend worden door de personen vermeld in het tweede of zesde lid, ook al ressorteert deze zelfstandige niet onder het werkgeversgezag van de opdrachtgever.

In de andere gevallen wordt de aanvraag door de rechtstreeks betrokken overheid of de persoon die een veiligheidsmachtiging behoeft ondertekend.

§ 3. Van zodra de aanvraag om een veiligheidsmachtiging door de Nationale Veiligheidsoverheid of de in artikel 1^{quinq}uies van de wet bedoelde veiligheids-overheden is aanvaard, brengt zij de veiligheids-officier hiervan zo snel mogelijk schriftelijk op de hoogte.

De veiligheids-officier bezorgt aan de personen die een veiligheids-machtiging behoeven de in artikel 17 van de wet vereiste documenten.

Onderafdeling 3. — Beoordeling van de ontvankelijkheid van de aanvraag

Art. 72. De veiligheids-officier controleert of alle in artikel 17, derde lid, van de wet bedoelde documenten volledig zijn ingevuld door de personen die een veiligheidsmachtiging behoeven.

Indien documenten ontbreken of indien de documenten niet volledig werden ingevuld, informeert de veiligheids-officier de personen die een veiligheidsmachtiging behoeven hierover met het verzoek onverwijld de ontbrekende documenten op te sturen of de documenten verder aan te vullen. De in artikel 73, bedoelde termijn van vijftien dagen neemt geen aanvang zolang de ontbrekende of vervolledigde documenten niet zijn opgestuurd aan de veiligheids-officier.

Art. 73. Vanaf de ontvangst van de volledig ingevulde documenten, bedoeld in artikel 17, derde lid, van de wet, beschikt de veiligheids-officier over een termijn van vijftien dagen om ze naar de Nationale Veiligheidsoverheid of de in artikel 1^{quinq}uies van de wet bedoelde veiligheids-overheden te zenden.

Art. 74. De Nationale Veiligheidsoverheid of de in artikel 1^{quinq}uies van de wet bedoelde veiligheids-overheden controleren of alle in artikel 17, derde lid, van de wet bedoelde documenten werden toegestuurd en volledig zijn ingevuld door de personen die een veiligheidsmachtiging behoeven.

Indien documenten ontbreken of niet volledig werden ingevuld of wanneer de motieven in de aanvraag niet voldoende concreet, correct of overtuigend zijn, wordt de aanvraag als onontvankelijk beschouwd. De veiligheids-officier wordt hierover geïnformeerd door de Nationale Veiligheidsoverheid of de in artikel 1^{quinq}uies van de wet bedoelde veiligheids-overheden, die op zijn beurt de personen die een veiligheids-machtiging behoeven informeert.

Indien de aanvraag door de Nationale Veiligheidsoverheid of de in artikel 1^{quinq}uies van de wet bedoelde veiligheids-overheden als onontvankelijk wordt beschouwd, wordt de veiligheids-officier hierover geïnformeerd en stuurt de Nationale Veiligheidsoverheid of de in artikel 1^{quinq}uies van de wet bedoelde veiligheids-overheden de in artikel 17, derde lid, van de wet bedoelde documenten en de aanvraag om een veiligheids-onderzoek uit te voeren onverwijld door aan de bevoegde inlichtingen- en veiligheidsdienst.

Art. 75. Si la demande est signée par l'autorité directement concernée ou par la personne qui requiert une habilitation de sécurité, telle que visée à l'article 71, § 2, alinéa 9, la procédure décrite aux articles 72, 73 et 74 est effectuée directement auprès de l'Autorité nationale de Sécurité ou des autorités de sécurité visées à l'article 1^{quinq}uies de la loi, et non par l'intermédiaire de l'officier de sécurité.

Sous-section 4. — Enquête de sécurité

Art. 76. A dater de la transmission visée aux articles 74, alinéa 3, et 75, le service de renseignement et de sécurité transmet les résultats de son enquête de sécurité à l'Autorité nationale de Sécurité ou aux autorités de sécurité visées à l'article 1^{quinq}uies de la loi, dans un délai de :

1° deux mois, s'il s'agit d'une enquête de sécurité dans le cadre d'une habilitation de sécurité de niveau « CONFIDENTIEL » ;

2° trois mois, s'il s'agit d'une enquête de sécurité dans le cadre d'une habilitation de sécurité de niveau « SECRET » ;

3° six mois, s'il s'agit d'une enquête de sécurité dans le cadre d'une habilitation de sécurité de niveau « TRÈS SECRET ».

Ces délais peuvent être prorogés pour une durée maximale de trois mois lorsque le service de renseignement et de sécurité doit recueillir des informations à l'étranger.

Art. 77. Le modèle des documents visés à l'article 17, alinéas 1^{er} et 2, de la loi, est repris dans les annexes 2 à 5.

Art. 78. L'accord ou le retrait prévus à l'article 16 de la loi s'effectue par l'envoi électronique d'un formulaire d'accord à l'officier de sécurité.

S'il n'est pas possible de procéder via un envoi électronique, cet envoi se fait selon les modalités prévues à l'article 17, alinéa 2 de la loi.

Sous-section 5. — Décision concernant l'habilitation de sécurité

Art. 79. Dès la réception des résultats de l'enquête de sécurité, l'Autorité nationale de Sécurité ou les autorités de sécurité visées à l'article 1^{quinq}uies de la loi disposent d'un délai d'un mois pour statuer sur la demande d'habilitation de sécurité et transmettre la décision à l'officier de sécurité.

Art. 80. Dès la réception de la décision de l'Autorité nationale de Sécurité ou des autorités de sécurité visées à l'article 1^{quinq}uies de la loi, l'officier de sécurité dispose d'un délai de quinze jours pour notifier cette décision à la personne pour laquelle l'habilitation de sécurité est demandée.

Dans le cas visé à l'article 71, § 2, alinéa 9, l'Autorité nationale de Sécurité ou les autorités de sécurité visées à l'article 1^{quinq}uies de la loi notifient la décision à l'autorité directement concernée ou à la personne qui requiert une habilitation de sécurité dans un délai d'un mois et quinze jours.

Sous-section 6. — Durée de validité de l'habilitation de sécurité

Art. 81. L'habilitation de sécurité pour les personnes physiques est délivrée pour une période de cinq ans maximum.

Cette période peut être raccourcie en raison d'éléments recueillis lors de l'enquête de sécurité ou en raison d'une demande d'habilitation de sécurité de plus courte durée. Toute durée de validité inférieure à cinq ans est mentionnée dans la notification de la décision d'octroi de l'habilitation de sécurité par l'Autorité nationale de Sécurité ou des autorités de sécurité visées à l'article 1^{quinq}uies de la loi.

Le délai de cinq ans ou le délai réduit visé à l'alinéa 2 prennent cours à la date de la décision d'octroi de l'habilitation de sécurité par l'Autorité nationale de Sécurité ou des autorités de sécurité visées à l'article 1^{quinq}uies de la loi.

Sous-section 7. — Enquête de sécurité complémentaire

Art. 82. La personne titulaire d'une habilitation de sécurité est tenue de signaler à l'officier de sécurité, de sa propre initiative, les événements survenus dans sa sphère privée, qui entraînent une modification des données indiquées dans le questionnaire de base visé à l'article 17, alinéa 1^{er}, de la loi.

L'employeur de la personne titulaire de l'habilitation de sécurité est également tenu de signaler à l'officier de sécurité tout élément troublant dans le comportement de la personne concernée qui est inconciliable avec les garanties de discrétion, de loyauté et d'intégrité.

Art. 75. Indien de aanvraag door de rechtstreeks betrokken overheid of de persoon die een veiligheidsmachtiging behoeft, is ondertekend, zoals vermeld in artikel 71, § 2, negende lid, wordt de in artikelen 72, 73 en 74 vermelde procedure rechtstreeks gevoerd met de Nationale Veiligheidsoverheid of de in artikel 1^{quinq}uies van de wet bedoelde veiligheidsdiensten en niet via de veiligheidsofficier.

Onderafdeling 4. — Het veiligheidsonderzoek

Art. 76. Vanaf de in artikel 74, derde lid, en artikel 75, bedoelde overzending, bezorgt de inlichtingen- en veiligheidsdienst de resultaten van zijn onderzoek aan de Nationale Veiligheidsoverheid of de in artikel 1^{quinq}uies van de wet bedoelde veiligheidsdiensten, binnen:

1° twee maanden als het gaat om een veiligheidsonderzoek voor een veiligheidsmachtiging van het niveau "VERTROUWELIJK";

2° drie maanden als het gaat om een veiligheidsonderzoek voor een veiligheidsmachtiging van het niveau "GEHEIM";

3° zes maanden als het gaat om een veiligheidsonderzoek voor een veiligheidsmachtiging van het niveau "ZEER GEHEIM".

Die termijnen kunnen met ten hoogste drie maanden worden verlengd wanneer de inlichtingen- en veiligheidsdienst inlichtingen moet inwinnen in het buitenland.

Art. 77. Het model van de in artikel 17, eerste en tweede lid, van de wet bedoelde documenten is opgenomen in bijlagen 2 tot 5.

Art. 78. De in artikel 16 van de wet voorziene instemming of intrekking gebeurt door het elektronisch versturen van het instemmingsformulier naar de veiligheidsofficier.

Indien een elektronische verzending niet mogelijk is, gebeurt de verzending op de wijze bepaald in artikel 17, tweede lid van de wet.

Onderafdeling 5. — De beslissing betreffende de veiligheidsmachtiging

Art. 79. Zodra de Nationale Veiligheidsoverheid of de in artikel 1^{quinq}uies van de wet bedoelde veiligheidsdiensten de resultaten van het veiligheidsonderzoek hebben ontvangen, hebben ze één maand de tijd om zich over de aanvraag om een veiligheidsmachtiging uit te spreken en de beslissing aan de veiligheidsofficier over te zenden.

Art. 80. Zodra de veiligheidsofficier de beslissing van de Nationale Veiligheidsoverheid of de in artikel 1^{quinq}uies van de wet bedoelde veiligheidsdiensten heeft ontvangen, heeft hij vijftien dagen de tijd om deze beslissing ter kennis te brengen van de persoon voor wie de veiligheidsmachtiging is gevraagd.

In het in artikel 71, § 2, negende lid, bedoelde geval, brengt de Nationale Veiligheidsoverheid of de in artikel 1^{quinq}uies van de wet bedoelde veiligheidsdiensten de beslissing ter kennis van de rechtstreeks betrokken overheid of de persoon die een veiligheidsmachtiging behoeft binnen een termijn van één maand en vijftien dagen.

Onderafdeling 6. — Geldigheidsduur van de veiligheidsmachtiging

Art. 81. De veiligheidsmachtiging voor natuurlijke personen wordt toegestaan voor een periode van maximum vijf jaar.

Deze periode kan ingekort worden omwille van de tijdens het veiligheidsonderzoek bekomen elementen of omdat een veiligheidsmachtiging van kortere duur werd gevraagd. Elke geldigheidsduur korter dan vijf jaar moet vermeld worden in de notificatie van de beslissing van de Nationale Veiligheidsoverheid of de in artikel 1^{quinq}uies van de wet bedoelde veiligheidsdiensten tot het toekennen van de veiligheidsmachtiging.

De termijn van vijf jaar of de in het tweede lid bedoelde ingekorte termijn begint te lopen vanaf de datum van de beslissing van de Nationale Veiligheidsoverheid of de in artikel 1^{quinq}uies van de wet bedoelde veiligheidsdiensten tot het toekennen van de veiligheidsmachtiging.

Onderafdeling 7. — Tussentijds veiligheidsonderzoek

Art. 82. De persoon in het bezit van een veiligheidsmachtiging dient zelf uit eigen beweging aan de veiligheidsofficier gebeurtenissen uit zijn privésfeer te melden, indien het gaat om een wijziging van de gegevens die worden vermeld in de basisvragenlijst, zoals bedoeld in artikel 17, eerste lid van de wet.

De werkgever van de persoon die de veiligheidsmachtiging bezit moet aan de veiligheidsofficier elk verontrustend element signaleren betreffende het gedrag van de betrokkene dat onverzoenbaar is met de garanties inzake geheimhouding, loyauteit en integriteit.

Si la personne titulaire d'une habilitation de sécurité n'a pas retiré son consentement et que, pendant la durée de l'habilitation de sécurité, des éléments visés aux alinéas 1 et 2 sont signalés par l'officier de sécurité, le titulaire de l'habilitation de sécurité ou son employeur, l'Autorité nationale de Sécurité ou les autorités de sécurité visées à l'article 1^{qu}inques de la loi peuvent charger le service de renseignement et de sécurité compétent de procéder à une enquête de sécurité complémentaire.

L'officier de sécurité est chargé du suivi des signalements d'éléments relatifs aux personnes titulaires d'une habilitation de sécurité susceptibles de conduire à un réexamen de l'habilitation de sécurité tel que visé à l'article 16, § 3, de la loi.

Section 2. — Habilitation de sécurité pour les personnes morales

Sous-section 1. — Généralités

Art. 83. Toute personne morale peut être autorisée à accéder à des informations classifiées pour autant que le besoin d'en connaître soit reconnu par l'Autorité nationale de Sécurité ou les autorités de sécurité visées à l'article 1^{qu}inques de la loi et que cette personne morale dispose d'une habilitation de sécurité pour les personnes morales, à l'exception des informations classifiées de niveau « RESTREINT » pour lesquelles aucune habilitation de sécurité n'est requise.

Art. 84. Seules les personnes morales dont le siège social se situe en Belgique peuvent être habilitées dans le cadre des marchés publics qui impliquent, nécessitent et/ou contiennent des informations classifiées de niveau « CONFIDENTIEL » ou supérieur.

Les personnes morales dont le siège social n'est pas situé en Belgique peuvent également être habilitées dans le cadre de marchés publics classifiés du niveau « CONFIDENTIEL » au moins, dans la mesure où ces personnes morales disposent d'une habilitation de sécurité pour personnes morales qui peut être reconnue par l'Autorité nationale de Sécurité ou les autorités de sécurité visées à l'article 1^{qu}inques de la loi sur la base des accords relatifs à l'échange et à la protection mutuelle des informations classifiées liant la Belgique.

Pour ce qui concerne les marchés publics qui impliquent, nécessitent et/ou contiennent des informations classifiées du niveau « CONFIDENTIEL » au moins, l'administrateur ICT doit être en possession d'une habilitation de sécurité du niveau fixé conformément à la politique de sécurité de l'Autorité nationale de Sécurité.

Pour ce qui concerne les marchés publics qui impliquent, nécessitent et/ou contiennent des informations classifiées de niveau « RESTREINT », l'Autorité nationale de Sécurité détermine la nécessité d'une habilitation de sécurité pour l'administrateur ICT et, le cas échéant, son niveau.

Sous-section 2. — Procédure de demande

Art. 85. § 1. Sans préjudice de l'article 93, l'administrateur d'une personne morale remet à l'Autorité nationale de Sécurité ou, le cas échéant, à l'une des autorités visées à l'article 1^{qu}inques de la loi, le dossier d'habilitation comprenant au moins :

1° le questionnaire de base, mentionné à l'article 17 de la loi, rempli par le candidat officier de sécurité et son remplaçant éventuel ;

2° les documents justificatifs qui lui ont été remis par l'officier de sécurité du pouvoir adjudicateur ;

3° le questionnaire de base, mentionné à l'article 17 de la loi, rempli par toutes les personnes physiques appartenant aux organes de la personne morale, ainsi qu'une vue d'ensemble de tous les actionnaires ou associés qui exercent le contrôle de droit ou de fait sur la personne morale.

Toutes les personnes physiques appartenant aux organes sont tenus d'introduire une demande d'habilitation.

Au moins un des membres de l'organe d'administration doit :

1° avoir la nationalité belge ;

2° faire l'objet d'une enquête de sécurité effectuée par un des services de renseignement et de sécurité conformément à la loi, au présent arrêté et aux directives du Conseil national de Sécurité, telle que visée à l'article 18, alinéa 5 de la loi ; et

3° se voir octroyer une habilitation de sécurité à l'issue de l'enquête de sécurité effectuée.

Indien de persoon in het bezit van een veiligheidsmachtiging zijn toestemming niet heeft ingetrokken en tijdens de looptijd van de veiligheidsmachtiging elementen zoals bedoeld in het eerste en het tweede lid worden signaleerd door de veiligheidsofficier, de persoon in het bezit van de veiligheidsmachtiging of diens werkgever, kan de Nationale Veiligheidsoverheid of de in artikel 1^{qu}inques van de wet bedoelde veiligheidsdiensten de bevoegde inlichtingen- en veiligheidsdienst belasten met een tussentijds veiligheidsonderzoek.

De veiligheidsofficier is belast met de nazorg voor de melding van elementen in verband met personen die een veiligheidsmachtiging hebben ontvangen, en die kunnen leiden tot herziening van de veiligheidsmachtiging, zoals bedoeld in artikel 16, § 3 van de wet.

Afdeling 2. — De veiligheidsmachtiging voor rechtspersonen

Onderafdeling 1. — Algemeen

Art. 83. Iedere rechtspersoon kan toegang krijgen tot geclassificeerde informatie, indien de noodzaak tot kennisname wordt erkend door de Nationale Veiligheidsoverheid of de in artikel 1^{qu}inques van de wet bedoelde veiligheidsdiensten en deze rechtspersoon beschikt over een veiligheidsmachtiging voor rechtspersonen, met uitzondering voor de geclassificeerde informatie van het niveau « BEPERKT » waar geen enkele veiligheidsmachtiging voor is vereist.

Art. 84. Enkel rechtspersonen waarvan de statutaire zetel in België is gevestigd, kunnen gemachtigd worden in het kader van overheidsopdrachten die betrekking hebben op geclassificeerde informatie van het niveau « VERTROUWELIJK » of hoger of deze informatie noodzakelijk maken en/of bevatten.

Rechtspersonen waarvan de statutaire zetel niet in België is gevestigd, kunnen eveneens gemachtigd worden in het kader van geclassificeerde overheidsopdrachten van minstens het niveau « VERTROUWELIJK », voor zover deze rechtspersonen beschikken over een veiligheidsmachtiging voor rechtspersonen die door de Nationale Veiligheidsoverheid of de in artikel 1^{qu}inques van de wet bedoelde veiligheidsdiensten kan worden erkend op basis van de overeenkomsten inzake de uitwisseling en de wederzijdse bescherming van geclassificeerde informatie die België binden.

Voor wat betreft overheidsopdrachten die betrekking hebben op geclassificeerde informatie van minstens het niveau « VERTROUWELIJK » of deze informatie noodzakelijk maken en/of bevatten, moet de ICT-beheerder in het bezit zijn van een veiligheidsmachtiging waarvan het niveau wordt bepaald overeenkomstig het veiligheidsbeleid van de Nationale Veiligheidsoverheid.

Voor wat betreft overheidsopdrachten die betrekking hebben op geclassificeerde informatie van het niveau « BEPERKT » of deze noodzakelijk maken en/of bevatten, bepaalt de Nationale Veiligheidsoverheid de noodzaak van een veiligheidsmachtiging voor de ICT-beheerder en desgevallend het niveau ervan.

Onderafdeling 2. — Aanvraagprocedure

Art. 85. § 1. Onverminderd artikel 93, bezorgt de bestuurder van een rechtspersoon aan de Nationale Veiligheidsoverheid of, in voorkomend geval, aan één van de in artikel 1^{qu}inques van de wet bedoelde overheden het habilitatiedossier, minstens bestaande uit :

1° de door de kandidaat-veiligheidsofficier en zijn eventuele vervanger ingevulde basisvragenlijst, die wordt vermeld in artikel 17 van de wet ;

2° de rechtvaardigingsdocumenten die hem werden overhandigd door de veiligheidsofficier van de aanbestedende overheid ;

3° de door alle fysieke personen die tot de organen van de rechtspersoon behoren ingevulde basisvragenlijst, die wordt vermeld in artikel 17 van de wet, evenals een volledig zicht op alle aandeelhouders of vennoten die in rechte of in feite de controle over de rechtspersoon uitoefenen.

Alle fysieke personen die tot de organen behoren moeten een aanvraag tot machtiging indienen.

Minstens één van de leden van het bestuursorgaan moet :

1° over de Belgische nationaliteit beschikken ;

2° onderworpen kunnen worden aan een veiligheidsonderzoek uitgevoerd door één van de inlichtingen- en veiligheidsdiensten overeenkomstig de wet, het voorliggend besluit en de richtlijn van de Nationale Veiligheidsraad, zoals vermeld in artikel 18, vijfde lid van de wet ; en

3° een veiligheidsmachtiging kunnen worden toegekend na het uitgevoerde veiligheidsonderzoek.

§ 2. L'Autorité nationale de Sécurité ou les autorités de sécurité visées à l'article 1^{qu}inques de la loi déterminent pour la personne morale visée à la présente section le nombre de personnes physiques appartenant aux organes qui doivent être titulaires d'une habilitation de sécurité, dont au moins la moitié doit être titulaire d'une habilitation de sécurité.

§ 3. La personne chargée de la gestion journalière de la personne morale doit résider et être domiciliée en Belgique.

Sous-section 3. — Appréciation de la recevabilité de la demande

Art. 86. L'Autorité nationale de Sécurité ou les autorités de sécurité visées à l'article 1^{qu}inques de la loi vérifient que toutes les données mentionnées à l'article 85, paragraphe 1^{er}, ont été envoyées.

Si des données sont manquantes ou incorrectement remplies, le candidat officier de sécurité de la personne morale sera invité à les compléter.

Art. 87. L'Autorité nationale de Sécurité ou les autorités de sécurité visées à l'article 1^{qu}inques de la loi déclarent la demande recevable ou irrecevable et en informent le candidat officier de sécurité.

Si la demande est recevable, l'Autorité nationale de Sécurité ou les autorités de sécurité visées à l'article 1^{qu}inques de la loi transmettent sans délai la demande d'ouverture d'une enquête de sécurité au service de renseignement et de sécurité compétent, ainsi que les informations mentionnées à l'article 85, paragraphe 1^{er}.

Sous-section 4. — Enquête de sécurité

Art. 88. L'article 76 est applicable à ces demandes.

Sous-section 5. — Décision concernant l'habilitation de sécurité

Art. 89. Dès la réception des résultats de l'enquête de sécurité, l'Autorité nationale de Sécurité ou les autorités de sécurité visées à l'article 1^{qu}inques de la loi disposent d'un délai d'un mois pour statuer sur la demande d'habilitation de sécurité et transmettre leur décision à l'officier de sécurité.

Art. 90. Dès la réception de la décision de l'Autorité nationale de Sécurité ou d'une autorité de sécurité visée à l'article 1^{qu}inques de la loi par l'officier de sécurité, celui-ci dispose d'un délai de quinze jours pour notifier cette décision aux organes mentionnés à l'article 85, § 1^{er}, alinéa 1, 3^o.

Sous-section 6. — Durée de validité de l'habilitation de sécurité

Art. 91. L'article 81 s'applique aux décisions d'octroi d'une habilitation de sécurité pour les personnes morales.

Sous-section 7. — Autres tâches de l'officier de sécurité dans le cadre de la présente section

Art. 92. La personne morale est tenue, par l'intermédiaire de l'officier de sécurité, de communiquer immédiatement et par écrit à l'Autorité nationale de Sécurité, les éléments suivants :

1° les modifications ayant un impact sur la politique de sécurité de la personne morale ;

2° les modifications prévues dans la propriété/l'actionariat et la direction de la personne morale ;

3° les nominations prévues d'administrateurs n'ayant pas la nationalité belge ou la coopération envisagée avec des sociétés ou des autorités étrangères.

4° tout élément d'intérêt inconciliable avec les garanties de discrétion, de loyauté et d'intégrité.

L'officier de sécurité est chargé du suivi de la notification de tous les éléments susceptibles d'aboutir à un réexamen de l'habilitation de sécurité visée à l'article 16, § 3 de la loi.

Section 3. — Habilitations de sécurité en vue d'un accès à l'étranger

Art. 93. La personne morale ou physique qui souhaite, dans un but scientifique, industriel ou économique, avoir accès à des informations classifiées ou à une zone sécurisée à l'étranger, doit introduire auprès de l'Autorité nationale de Sécurité une demande motivée d'obtention d'une habilitation de sécurité et doit y joindre l'invitation écrite des autorités étrangères compétentes.

§ 2. De Nationale Veiligheidsoverheid of de in artikel 1^{qu}inques van de wet bedoelde veiligheidsoverheden bepalen voor de rechtspersoon bedoeld in deze afdeling hoeveel fysieke personen die tot de organen behoren houder moeten zijn van een veiligheidsmachtiging, waarbij minstens de helft houder moet zijn van een veiligheidsmachtiging.

§ 3. De persoon aan wie het dagelijks bestuur van de rechtspersoon werd opgedragen moet in België verblijven en er gedomicilieerd zijn.

Onderafdeling 3. — Beoordeling van de ontvankelijkheid van de aanvraag

Art. 86. De Nationale Veiligheidsoverheid of de in artikel 1^{qu}inques van de wet bedoelde veiligheidsoverheden controleren of alle in artikel 85, paragraaf 1 vermelde gegevens werden toegestuurd.

Indien gegevens ontbreken of niet correct werden ingevuld, wordt de kandidaat-veiligheidsofficier van de rechtspersoon gevraagd om de gegevens te vervolledigen.

Art. 87. De Nationale Veiligheidsoverheid of de in artikel 1^{qu}inques van de wet bedoelde veiligheidsoverheden verklaren de aanvraag ontvankelijk of onontvankelijk en informeren de kandidaat-veiligheidsofficier hierover.

Ingeval de aanvraag ontvankelijk is, wordt de aanvraag om een veiligheidsonderzoek op te starten door de Nationale Veiligheidsoverheid of de in artikel 1^{qu}inques van de wet bedoelde veiligheidsoverheden onverwijld doorgestuurd aan de bevoegde inlichtingen- en veiligheidsdienst, samen met de gegevens vermeld in artikel 85, paragraaf 1.

Onderafdeling 4. — Het veiligheidsonderzoek

Art. 88. Het artikel 76 is van toepassing op deze aanvragen.

Onderafdeling 5. — De beslissing betreffende de veiligheidsmachtiging

Art. 89. Zodra de Nationale Veiligheidsoverheid of de in artikel 1^{qu}inques van de wet bedoelde veiligheidsoverheden de resultaten van het veiligheidsonderzoek hebben ontvangen, hebben ze één maand de tijd om zich over de aanvraag om een veiligheidsmachtiging uit te spreken en hun beslissing aan de veiligheidsofficier over te zenden.

Art. 90. Zodra de veiligheidsofficier de beslissing van de Nationale Veiligheidsoverheid of één van de in artikel 1^{qu}inques van de wet bedoelde veiligheidsoverheden heeft ontvangen, heeft hij vijftien dagen de tijd om deze beslissingen ter kennis te brengen aan de organen vermeld in artikel 85, § 1, eerste lid, 3^o.

Onderafdeling 6. — Geldigheidsduur van de veiligheidsmachtiging

Art. 91. Artikel 81 is van toepassing op de beslissingen tot toekenning van een veiligheidsmachtiging voor rechtspersonen.

Onderafdeling 7. — Overige taken van de veiligheidsofficier in het kader van deze afdeling

Art. 92. De rechtspersoon is verplicht om via de veiligheidsofficier onverwijld aan de Nationale Veiligheidsoverheid het volgende schriftelijk mee te delen:

1° wijzigingen die impact hebben op het veiligheidsbeleid van de rechtspersoon;

2° voorgenomen wijzigingen in eigendom/aandeelhouderschap en bestuur van de rechtspersoon;

3° voorgenomen benoemingen van bestuurders die niet beschikken over de Belgische nationaliteit of voorgenomen samenwerking met buitenlandse bedrijven of overheden;

4° elk verontrustend element dat onverzoeikbaar is met de garanties inzake geheimhouding, loyauteit en integriteit.

De veiligheidsofficier is belast met de nazorg voor de melding van alle elementen die kunnen leiden tot een herziening van de veiligheidsmachtiging zoals bedoeld in artikel 16, § 3 van de wet.

Afdeling 3. — Veiligheidsmachtigingen met het oog op toegang in het buitenland

Art. 93. De rechtspersoon of natuurlijke persoon die voor een wetenschappelijk, industrieel of economisch doel toegang wil krijgen tot geclassificeerde informatie of tot een beveiligde zone in het buitenland, moet bij de Nationale Veiligheidsoverheid een met redenen omklede aanvraag om een veiligheidsmachtiging indienen en moet hiertoe de schriftelijke uitnodiging voorleggen van de bevoegde buitenlandse overheidsinstanties.

Dès que la demande d'habilitation de sécurité a été acceptée, l'Autorité nationale de Sécurité en informe l'officier de sécurité dans les plus brefs délais. Celui-ci remet alors à la personne concernée tous les documents requis.

S'il n'y a pas d'officier de sécurité compétent à l'égard de la personne concernée, l'Autorité nationale de Sécurité informe directement celle-ci de sa décision et lui transmet, contre accusé de réception, les documents requis.

Art. 94. L'habilitation de sécurité délivrée conformément à l'article 93 concerne exclusivement l'accès aux lieux où sont situés des organismes publics étrangers, en ce compris des installations militaires, des entreprises étrangères ou des institutions étrangères d'enseignement supérieur.

CHAPITRE 6. — *Mesures de protection liées aux marchés publics qui impliquent, nécessitent et/ou contiennent des informations classifiées*

Art. 95. Les mesures de protection minimales supplémentaires de nature administrative et technique associées aux marchés publics qui impliquent, nécessitent et/ou contiennent des informations classifiées sont déterminées par l'Autorité nationale de Sécurité sous réserve de l'application de la loi du 13 août 2011 relative aux marchés publics et à certains marchés de travaux, de fournitures et de services dans le domaine de la défense et de la sécurité.

Art. 96. Dans le cadre des autres marchés publics (qu'ils soient attribués en vertu d'un accord-cadre ou non), aucun accès ne peut être accordé à des informations classifiées, sauf en cas de nécessité et à moins que les mesures de protection nécessaires ne soient prises à l'égard de l'adjudicataire et de tous les collaborateurs concernés de ce dernier, conformément à la loi, au présent arrêté et aux directives de l'Autorité nationale de Sécurité.

Art. 97. Un pouvoir adjudicateur peut passer des marchés pour des tâches qui impliquent ou nécessitent l'utilisation d'informations classifiées par des entités industrielles ou autres.

A cette fin, le pouvoir adjudicateur doit faire usage de la loi du 13 août 2011 relative aux marchés publics et à certains marchés de travaux, de fournitures et de services dans le domaine de la défense et de la sécurité.

Art. 98. Lors de l'attribution de marchés classifiés à des entités industrielles ou autres, le pouvoir adjudicateur veille au respect des normes minimales de sécurité industrielle, telles que définies dans la loi et le présent arrêté ainsi que dans les directives de l'Autorité nationale de Sécurité et dans le marché public classifié.

Art. 99. L'Autorité nationale de Sécurité vérifie que toutes les mesures de protection nécessaires liées aux marchés publics ont été prises pour protéger les informations classifiées lors de la phase de prospection, la procédure d'attribution ainsi que pendant l'exécution d'un marché public classifié.

Art. 100. L'Autorité nationale de Sécurité vérifie que :

1° les adjudicataires enregistrés sur le territoire qui participent à des marchés publics impliquant, nécessitant et/ou contenant des informations classifiées de niveau « CONFIDENTIEL » ou supérieur ou aux contrats de sous-traitance y afférents pendant l'exécution des marchés ou au stade précontractuel, disposent d'une habilitation de sécurité pour les personnes morales octroyée au niveau de classification correspondant ;

2° le personnel des adjudicataires ou des sous-traitants qui doit avoir accès à des informations classifiées de niveau « CONFIDENTIEL » ou supérieur pour l'exécution d'un marché public classifié dispose d'une habilitation de sécurité pour les personnes physiques du niveau de classification correspondant ;

3° les adjudicataires enregistrés sur le territoire qui participent à des marchés publics qui se rapportent à des informations classifiées ou impliquant, nécessitant et/ou contenant des informations classifiées de niveau « CONFIDENTIEL » ou supérieur, ou aux contrats de sous-traitance y afférents pendant l'exécution des marchés ou au stade précontractuel, disposent d'une installation physique approuvée ;

4° les adjudicataires enregistrés sur le territoire qui participent à des marchés publics ou qui se rapportent à des informations classifiées ou impliquant, nécessitant et/ou contenant des informations classifiées, ou aux contrats de sous-traitance y afférents pendant l'exécution des marchés ou au stade précontractuel, disposent d'un système de communication et d'information approuvé ;

Van zodra de aanvraag om een veiligheidsmachtiging is aanvaard, brengt de Nationale Veiligheidsoverheid de veiligheidsofficier hiervan zo snel mogelijk op de hoogte. Deze laatste geeft dan aan de betrokken persoon alle vereiste documenten.

Indien er ten aanzien van de betrokken persoon geen bevoegde veiligheidsofficier is, brengt de Nationale Veiligheidsoverheid de betrokken persoon rechtstreeks op de hoogte van haar beslissing en maakt hem, tegen ontvangstmelding, de vereiste documenten over.

Art. 94. De overeenkomstig artikel 93 afgegeven veiligheidsmachtiging heeft uitsluitend betrekking op de toegang tot plaatsen waar buitenlandse overheidsinstellingen, met inbegrip van militaire installaties, buitenlandse bedrijven en buitenlandse instellingen voor hoger onderwijs, gevestigd zijn.

HOOFDSTUK 6. — *De beschermingsmaatregelen verbonden aan overheidsopdrachten die betrekking hebben op geclassificeerde informatie of deze noodzakelijk maken en/of bevatten*

Art. 95. De bijkomende minimale beschermingsmaatregelen van administratieve en technische aard verbonden aan de overheidsopdrachten die betrekking hebben op geclassificeerde informatie of deze informatie noodzakelijk maken en/of bevatten, worden bepaald door de Nationale Veiligheidsoverheid onder voorbehoud van de toepassing van de wet van 13 augustus 2011 inzake overheidsopdrachten en bepaalde opdrachten voor werken, leveringen en diensten op defensie- en veiligheidsgebied.

Art. 96. In het kader van overige overheidsopdrachten (al dan niet toegekend in het kader van een raamovereenkomst), mag geen toegang verleend worden tot geclassificeerde informatie, tenzij dit noodzakelijk is en de nodige beschermingsmaatregelen in overeenstemming met de wet, het voorliggend besluit en de richtlijnen van de Nationale Veiligheidsoverheid getroffen worden met betrekking tot de opdrachtnemer en alle betrokken medewerkers van de opdrachtnemer.

Art. 97. Een aanbestedende overheid kan opdrachten plaatsen voor taken die de aanwending van geclassificeerde informatie door industriële of andere entiteiten behelzen of vereisen.

De aanbestedende overheid moet hiervoor gebruik maken van de wet van 13 augustus 2011 inzake overheidsopdrachten en bepaalde opdrachten voor werken, leveringen en diensten op defensie- en veiligheidsgebied.

Art. 98. De aanbestedende overheid zorgt er voor dat aan de minimumnormen voor industriële veiligheid, zoals bepaald in de wet en voorliggend besluit, evenals in de richtlijnen van de Nationale Veiligheidsoverheid en in de geclassificeerde overheidsopdracht, is voldaan bij het plaatsen van geclassificeerde opdrachten bij industriële of andere entiteiten.

Art. 99. De Nationale Veiligheidsoverheid verifieert dat alle beschermingsmaatregelen verbonden aan overheidsopdrachten werden genomen die nodig zijn voor de bescherming van geclassificeerde informatie tijdens de prospectiefase, de gunningsprocedure en de uitvoering van een geclassificeerde opdracht.

Art. 100. De Nationale Veiligheidsoverheid verifieert dat:

1° de op het grondgebied geregistreerde opdrachtnemers die deelnemen aan overheidsopdrachten die betrekking hebben op geclassificeerde informatie van het niveau "VERTROUWELIJK" of hoger of deze informatie noodzakelijk maken en/of bevatten, of deze in onderaanneming tijdens de uitvoering van de opdrachten of in de precontractuele fase, beschikken over een veiligheidsmachtiging voor rechtspersonen in overeenstemming met het overeenkomstige classificatieniveau;

2° het personeel van opdrachtnemers of van de entiteiten in onderaanneming dat voor de uitvoering van een geclassificeerde overheidsopdracht toegang moet hebben tot geclassificeerde informatie van het niveau "VERTROUWELIJK" of hoger over een veiligheidsmachtiging voor personen beschikt met het dienovereenkomstige classificatieniveau;

3° de op het grondgebied geregistreerde opdrachtnemers die deelnemen aan overheidsopdrachten die betrekking hebben op geclassificeerde informatie van het niveau "VERTROUWELIJK" of hoger of deze informatie noodzakelijk maken en/of bevatten, of deze in onderaanneming tijdens de uitvoering van de opdrachten of in de precontractuele fase, beschikken over een goedgekeurde fysieke installatie;

4° de op het grondgebied geregistreerde opdrachtnemers die deelnemen aan overheidsopdrachten die betrekking hebben op geclassificeerde informatie of deze informatie noodzakelijk maken en/of bevatten, of deze in onderaanneming tijdens de uitvoering van de opdrachten of in de precontractuele fase, beschikken over een goedgekeurd communicatie- en informatiesysteem;

5° les personnes morales qui ne sont pas enregistrées sur le territoire disposent d'une habilitation de sécurité valide pour les personnes morales, délivrée par les autorités compétentes du pays tiers et reconnue par l'Autorité nationale de Sécurité sur la base des accords et traités internationaux liant la Belgique en la matière.

Art. 101. En ce qui concerne les informations classifiées générées ou traitées par l'adjudicataire, le pouvoir adjudicateur exerce les droits de l'autorité d'origine, à moins que le pouvoir adjudicateur en ait disposé autrement dans le contrat.

Après l'exécution du marché, toutes les informations classifiées doivent être restituées au pouvoir adjudicateur dans les 15 jours ouvrables suivant le terme du contrat et aucune copie de ces informations ne peut être conservée.

Art. 102. Les candidats ou soumissionnaires qui n'ont pas été retenus et auxquels des informations classifiées ont été communiquées ou produites au cours de la procédure doivent les restituer au pouvoir adjudicateur dans un délai de 15 jours ouvrables à compter de la notification de leur non-sélection et ne peuvent conserver aucune copie de ces informations, sauf s'ils en ont encore besoin dans le cadre d'une procédure de litige. Dans ce cas, ils retourneront les informations classifiées à la fin de la période de recours et aucune copie de ces informations ne pourra être conservée.

CHAPITRE 7. — Contrôle

Art. 103. L'Autorité nationale de Sécurité exerce le contrôle :

1° afin de veiller à l'application (permanente) des mesures de protection minimales requises ;

2° afin de sensibiliser les fonctionnaires dirigeants, les dirigeants des personnes morales, les officiers de sécurité et les personnes de contact pour la sécurité à l'évolution de l'environnement en termes de risques et, au sens large, d'attirer l'attention de l'organisation sur l'importance des mesures de protection ;

3° afin de recommander des contre-mesures au cas où la confidentialité, l'intégrité, la disponibilité, l'authenticité et la non-répudiation des systèmes risquent de ne plus être garanties ;

4° afin de sensibiliser en permanence à la vigilance en matière de sécurité ;

5° dans le cadre de la procédure de demande d'habilitation de sécurité.

Art. 104. L'Autorité nationale de Sécurité exerce son contrôle au moyen :

1° d'informations demandées à l'entité contrôlée, qui est tenue de mettre sans délai à la disposition de l'Autorité nationale de Sécurité, à la demande de celle-ci, toutes les informations pertinentes sur les mesures de protection mises en œuvre et de coopérer pleinement ;

2° d'informations recueillies dans le cadre des enquêtes de terrain, en particulier lors d'un contrôle ou une inspection sur place.

Les membres de l'Autorité nationale de Sécurité chargés d'effectuer des enquêtes de terrain sont nommés par le ministre de la Justice sur proposition de l'administrateur général de la Sûreté de l'État. Lors de leur nomination, ils reçoivent une carte de légitimation dont le modèle est déterminé par le ministre de la Justice. Cette carte ne peut être utilisée que dans le cadre des enquêtes de terrain et doit immédiatement être restituée à l'autorité qui l'a délivrée, une fois le mandat terminé.

Les membres du Service général du Renseignement et de la Sécurité des Forces armées chargés d'effectuer des enquêtes de terrain en ce qui concerne la Défense, tel que définie à l'article 1^{er}quinquies, alinéas 2 et 3 de la loi, se voient délivrer, lors de leur nomination, une carte de légitimation dont le modèle est déterminé par le ministre de la Défense. Cette carte ne peut être utilisée que dans le cadre d'enquêtes de terrain et doit être restituée immédiatement à l'autorité qui l'a délivrée, une fois le mandat terminé.

5° rechtspersonen die niet zijn geregistreerd op het grondgebied beschikken over een geldige veiligheidsmachtiging voor rechtspersonen, afgeleverd door de bevoegde autoriteiten van het derde land en erkend door de Nationale Veiligheidsoverheid op grond van de internationale overeenkomsten en verdragen die België ter zake binden.

Art. 101. Wat betreft geclassificeerde informatie die door de opdrachtnemer wordt gegenereerd of verwerkt, oefent de aanbestedende overheid de rechten van de overheid van oorsprong uit, tenzij de aanbestedende overheid dit anders heeft bepaald in het contract.

Na uitvoering van de opdracht moet alle geclassificeerde informatie binnen de vijftien werkdagen na de beëindiging ervan teruggestuurd worden naar de aanbestedende overheid en mag er geen kopie worden bijgehouden van deze informatie.

Art. 102. Kandidaten of inschrijvers die niet zijn geselecteerd en aan wie tijdens de procedure geclassificeerde informatie werd verstrekt of deze hebben gegenereerd, moeten deze informatie terugsturen naar de aanbestedende overheid binnen de vijftien werkdagen na betekening van hun niet-selectie en mogen geen kopie bijhouden van deze informatie, tenzij zij deze informatie nog nodig hebben in het kader van een geschillenprocedure. In dat geval sturen zij de geclassificeerde informatie terug na afloop van de beroepstermijn en mag er geen kopie worden bijgehouden van deze informatie.

HOOFDSTUK 7. — Toezicht

Art. 103. Het toezicht wordt door de Nationale Veiligheidsoverheid uitgeoefend:

1° om te verzekeren dat de vereiste minimum beschermingsmaatregelen (blijvend) worden toegepast;

2° om de leidende ambtenaren, de hoofden van rechtspersonen, de veiligheidsfunctionarissen en de contactpersonen voor de veiligheid bewust te maken van de veranderende risico-omgeving en, in de ruime zin, de organisatie te wijzen op het belang van de beschermingsmaatregelen;

3° om tegenmaatregelen aan te bevelen in geval de vertrouwelijkheid, de integriteit, de beschikbaarheid, de authenticiteit en de niet-weerlegbaarheid van de systemen dreigt niet meer gegarandeerd te worden;

4° om blijvend te sensibiliseren op het vlak van veiligheidsbewustzijn;

5° als onderdeel van de procedure tot het aanvragen van een veiligheidsmachtiging.

Art. 104. De Nationale Veiligheidsoverheid oefent het toezicht uit door middel van:

1° informatie die wordt opgevraagd bij de gecontroleerde entiteit, die gehouden is om onverwijld op vraag van de Nationale Veiligheidsoverheid alle relevante informatie over de uitgevoerde beschermingsmaatregelen ter beschikking te stellen van de Nationale Veiligheidsoverheid en haar volledige medewerking te verlenen;

2° informatie die wordt verworven tijdens een terreinonderzoek, met name een controle of inspectie ter plaatse.

De leden van de Nationale Veiligheidsoverheid belast met het uitvoeren van terreinonderzoeken worden aangesteld door de minister van Justitie, op voordracht van de administrateur-generaal van de Veiligheid van de Staat. Bij hun aanstelling krijgen zij een legitimatiekaart waarvan het model wordt bepaald door de minister van Justitie. Die kaart mag alleen gebruikt worden in het kader van terreinonderzoeken en moet onmiddellijk worden terugbezorgd aan de overheid die haar heeft afgegeven, zodra de aanstelling is beëindigd.

De leden van de Algemene Dienst Inlichting en Veiligheid van de Krijgsmacht belast met het uitvoeren van terreinonderzoeken voor wat betreft Defensie, zoals omschreven in artikel 1^{er}quinquies, tweede en derde lid van de wet, krijgen bij hun aanstelling een legitimatiekaart waarvan het model wordt bepaald door de minister van Defensie. Die kaart mag alleen gebruikt worden in het kader van terreinonderzoeken en moet onmiddellijk worden terugbezorgd aan de overheid die haar heeft afgegeven, zodra de aanstelling is beëindigd.

Art. 105. L'Autorité nationale de Sécurité visite l'entité contrôlée, de façon annoncée ou non, en vue d'évaluer la mise en œuvre des mesures de protection prévues par la loi, le présent arrêté et les directives de l'Autorité nationale de Sécurité.

L'Autorité nationale de Sécurité communique un contrôle annoncé au moins un mois à l'avance à l'officier de sécurité de l'entité contrôlée, afin de permettre à ce dernier de prendre les mesures administratives nécessaires pour faciliter le contrôle. En l'absence d'officier de sécurité ou son remplaçant, l'Autorité nationale de Sécurité annonce ce contrôle au fonctionnaire dirigeant, aux personnes assurant la direction de l'entité contrôlée ou à la personne de contact pour la sécurité.

Art. 106. Lors de l'exécution d'une enquête de terrain, qu'elle soit annoncée ou non, les membres de l'Autorité nationale de Sécurité et du Service général du Renseignement et de la Sécurité des Forces armées peuvent se prévaloir des compétences suivantes, notamment :

1° s'entretenir avec toute personne potentiellement concernée par la protection des informations classifiées de l'entité contrôlée, en tenant compte des tâches de sécurité spécifiques dont elle est responsable ;

2° consulter toutes les pièces, tous les registres, documents et objets utiles au contrôle et liés à la protection des informations classifiées concernées ;

3° effectuer des contrôles ponctuels sur la manière de protéger les informations classifiées au sein de l'entité ;

4° visiter les différentes zones et implantations où des informations classifiées sont utilisées ;

5° consulter les informations pertinentes dans les systèmes de communication et d'information (en ce compris la sécurité du système, les données de configuration et les fichiers logs).

Art. 107. En cas de violation des mesures de protection, telles que prévues par la loi, le présent arrêté et les directives de l'Autorité nationale de Sécurité, l'Autorité nationale de Sécurité peut procéder à la suspension immédiate ou au retrait de l'approbation si la gravité de la situation le justifie.

Art. 108. Au plus tard deux mois à compter du premier jour ouvrable suivant le contrôle, l'Autorité nationale de Sécurité met le rapport avec ses constatations à la disposition de l'officier de sécurité de l'entité contrôlée.

Le rapport comprend :

1° les constatations relatives à l'application des mesures de protection minimales par l'entité concernée ;

2° le cas échéant, les exigences obligatoires à mettre en œuvre si les mesures de protection minimales ne sont pas respectées ;

3° le cas échéant, des recommandations si les mesures de protection minimales ont été respectées mais que la sécurité peut être améliorée.

En l'absence d'un officier de sécurité ou de son remplaçant, l'officier de l'Autorité nationale de Sécurité met ce rapport à la disposition du fonctionnaire dirigeant, des personnes assurant la direction de l'entité contrôlée ou de la personne de contact pour la sécurité.

Art. 109. Au plus tard quinze jours ouvrables à dater de la prise de connaissance du rapport, l'entité contrôlée transmet, le cas échéant, une proposition de mesures correctives à l'Autorité nationale de Sécurité, en indiquant le délai de mise en œuvre.

Art. 110. Le cas échéant, l'Autorité nationale de Sécurité indique sans délai à l'entité contrôlée si ces mesures correctives sont suffisantes ou si des mesures correctives supplémentaires s'imposent.

Art. 111. L'entité contrôlée prend les mesures correctives nécessaires, sous peine de suspension ou de retrait de l'habilitation de sécurité pour les personnes morales.

Art. 105. De Nationale Veiligheidsoverheid bezoekt de gecontroleerde entiteit, al dan niet aangekondigd, voor een beoordeling van de implementatie van de beschermingsmaatregelen, zoals vastgelegd in de wet, voorliggend besluit en de richtlijnen van de Nationale Veiligheidsoverheid.

Een aangekondigde controle wordt door de Nationale Veiligheidsoverheid minstens één maand op voorhand aangekondigd bij de veiligheidsofficier van de gecontroleerde entiteit, opdat deze de nodige administratieve maatregelen kan treffen om de controle te faciliteren. Bij gebreke aan een veiligheidsofficier of zijn vervanger, kondigt de Nationale Veiligheidsoverheid deze controle aan bij de leidend ambtenaar, de personen die het bestuur van de gecontroleerde entiteit verzekeren of de contactpersoon voor de veiligheid.

Art. 106. Bij het uitvoeren van een terreinonderzoek, al dan niet aangekondigd, kan er door de leden van de Nationale Veiligheidsoverheid en de Algemene Dienst Inlichting en Veiligheid van de Krijgsmacht beroep worden gedaan op volgende bevoegdheden, onder meer:

1° een onderhoud met elke mogelijke betrokkene bij de bescherming van de geclassificeerde informatie van de gecontroleerde entiteit, rekening houdende met de specifieke beveiligingstaken waarvoor zij verantwoordelijk zijn;

2° de inzage van alle stukken, registers, documenten en voorwerpen die nuttig zijn voor de controle en die in verband staan met de bescherming van de desbetreffende geclassificeerde informatie;

3° het uitvoeren van steekproeven betreffende de manier waarop de geclassificeerde informatie wordt beschermd binnen de entiteit;

4° het bezoeken van verschillende zones en vestigingen waar geclassificeerde informatie wordt aangewend;

5° het bekijken van relevante informatie in de communicatie- en informatiesystemen (onder meer de beveiliging van het systeem, de configuratiegegevens en de logbestanden).

Art. 107. In geval van schendingen van de beschermingsmaatregelen, zoals bepaald in de wet, in voorliggend besluit en de richtlijnen van de Nationale Veiligheidsoverheid, die dermate ernstig zijn, kan de Nationale Veiligheidsoverheid overgaan tot de onmiddellijke schorsing of intrekking van de goedkeuring.

Art. 108. Ten laatste twee maanden vanaf de eerste werkdag nadat de controle heeft plaatsgevonden, stelt de Nationale Veiligheidsoverheid het verslag met haar vaststellingen ter beschikking van de veiligheidsofficier van de gecontroleerde entiteit.

Het verslag bevat:

1° de vaststellingen betreffende de toepassing van de minimum beschermingsmaatregelen door de desbetreffende entiteit;

2° in voorkomend geval de verplicht uit te voeren vereisten indien de minimum beschermingsmaatregelen niet worden gerespecteerd;

3° in voorkomend geval aanbevelingen indien de minimum beschermingsmaatregelen zijn gerespecteerd, maar er ruimte is tot verbetering van de veiligheid.

Bij gebrek aan een veiligheidsofficier of zijn vervanger, stelt de Nationale Veiligheids-officier dit verslag ter beschikking van de leidend ambtenaar, de personen die het bestuur van de gecontroleerde entiteit verzekeren of de contactpersoon voor de veiligheid.

Art. 109. Ten laatste vijftien werkdagen vanaf de kennisname van het verslag door de gecontroleerde entiteit, stuurt deze in voorkomend geval een voorstel tot corrigerende maatregelen door aan de Nationale Veiligheidsoverheid met vermelding van de termijn van uitvoering.

Art. 110. De Nationale Veiligheidsoverheid laat in voorkomend geval onverwijld aan de gecontroleerde entiteit weten of deze corrigerende maatregelen voldoende zijn of dat er bijkomende corrigerende maatregelen vereist zijn.

Art. 111. De gecontroleerde entiteit neemt op straffe van intrekking of schorsing van de veiligheidsmachtiging voor rechtspersonen de nodige corrigerende maatregelen.

TITRE IV. — Dispositions transitoires et finales

Art. 112. Les pièces classifiées avant l’entrée en vigueur, le 1^{er} juin 2000, de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité et revêtues de la mention « TRÈS SECRET », « SECRET » ou « CONFIDENTIEL » sont réputées porter le degré de classification correspondant prévu à l’article 4 de la loi.

Les pièces classifiées après l’entrée en vigueur, le 1^{er} juin 2000, de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité, mais avant l’entrée en vigueur du présent arrêté, marquées de la mention « TRÈS SECRET », « SECRET » ou « CONFIDENTIEL » et d’une référence à la loi qui ne respecte pas pleinement les exigences de forme énoncées à l’article 16, alinéa 2 ou 3, sont réputées porter le degré de classification correspondant prévu à l’article 4 de la loi.

Art. 113. Les documents revêtus de la mention “DIFFUSION RESTREINTE (AR 24.03.2000)” avant l’entrée en vigueur du présent arrêté conservent cette mention. Cette mention ne peut en aucun cas être assimilée au degré de classification « RESTREINT », tel que prévu par l’article 4, alinéa 5 de la loi, étant donné que les mesures de protection telles que définies dans la loi et le présent arrêté ne s’appliquent pas aux documents portant la mention « DIFFUSION RESTREINTE (AR 24.03.2000) ».

Sans préjudice d’autres dispositions légales ou réglementaires spécifiques aux informations non classifiées, les informations non-classifiées, rédigées en français, dont une autorité ou une personne souhaite restreindre la diffusion aux personnes qualifiées pour en prendre connaissance sans attacher à cette limitation les effets juridiques prévus par la loi, peuvent être revêtues, à compter de l’entrée en vigueur du présent arrêté, de la mention « SENSIBLE NON CLASSIFIÉ (AR 20.12.2024) » et non plus de la mention « DIFFUSION RESTREINTE (AR 24.03.2000) ».

Lorsque les documents sont rédigés dans une autre langue que le néerlandais ou le français, les documents dont une autorité ou une personne souhaite restreindre la diffusion aux personnes qualifiées pour en prendre connaissance sans attacher à cette limitation les effets juridiques prévus par la loi, peuvent être revêtus, à compter de l’entrée en vigueur du présent arrêté, de la mention « SENSITIVE NON-CLASSIFIED (RD 20.12.2024) ».

Art. 114. Le présent arrêté entre en vigueur le 1^{er} février 2025.

Art. 115. L’arrêté royal du 24 mars 2000 portant exécution de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité est abrogé.

Art. 116. Nos Ministres sont chargés, chacun en ce qui le concerne, de l’exécution du présent arrêté.

Donné à Bruxelles, le 20 décembre 2024.

PHILIPPE

Par le Roi :

Le Ministre de la Justice,
P. VAN TIGCHELT

La Ministre de la Défense,
L. DEDONDER

La Ministre de l’Intérieur,
A. VERLINDEN

TITEL IV. — Overgangs- en slotbepalingen

Art. 112. De stukken geclassificeerd voor de inwerkingtreding van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen op 1 juni 2000 gemerkt met de vermelding “ZEER GEHEIM”, “GEHEIM”, of “VERTROUWELIJK” worden geacht gemerkt te zijn met het overeenstemmend classificatieniveau voorzien in artikel 4 van de wet.

De stukken geclassificeerd na de inwerkingtreding van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen op 1 juni 2000 maar voor de inwerkingtreding van onderhavig besluit gemerkt met de vermelding “ZEER GEHEIM”, “GEHEIM”, of “VERTROUWELIJK” en een verwijzing naar de wet die niet volledig overeenstemt met de vormelijke vereisten vermeld in artikel 16, tweede of derde lid worden geacht gemerkt te zijn met het overeenstemmend classificatieniveau voorzien in artikel 4 van de wet.

Art. 113. De documenten, vóór de inwerkingtreding van voorliggend besluit, voorzien van de vermelding “BEPERKTE VERSPREIDING (KB 24.03.2000)”, blijven deze vermelding behouden. Deze vermelding kan op geen enkele manier gelijkgesteld worden met het classificatieniveau “BEPERKT”, zoals bepaald in artikel 4, vijfde lid van de wet, gezien op documenten met de vermelding “BEPERKTE VERSPREIDING (KB 24.03.2000)” niet de beschermingsmaatregelen vermeld in de wet en voorliggend besluit van toepassing zijn.

Onverminderd andere specifieke wettelijke of reglementaire bepalingen betreffende niet-geclassificeerde informatie, kan de niet-geclassificeerde informatie, opgesteld in het Nederlands, waarvan een overheid of persoon de verspreiding wil beperken tot de personen die bevoegd zijn om er kennis van te nemen, zonder aan deze beperking de juridische gevolgen te verbinden voorzien door de wet, vanaf de inwerkingtreding van voorliggend besluit worden voorzien van de vermelding “GEVOELIG NIET-GECLASSIFICEERD (KB 20.12.2024)” en niet langer met de vermelding “BEPERKTE VERSPREIDING (KB 24.03.2000)”.

Indien het document in een andere taal dan het Nederlands of het Frans is opgesteld, kunnen de documenten waarvan een overheid of persoon de verspreiding wil beperken tot de personen die bevoegd zijn om er kennis van te nemen, zonder aan deze beperking de juridische gevolgen te verbinden voorzien door de wet, vanaf de inwerkingtreding van voorliggend besluit worden voorzien van de vermelding “SENSITIVE NON-CLASSIFIED (RD 20.12.2024)”.

Art. 114. Dit besluit treedt in werking op 1 februari 2025.

Art. 115. Het koninklijk besluit van 24 maart 2000 tot uitvoering van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, wordt opgeheven.

Art. 116. Onze Ministers zijn, ieder wat hem betreft, belast met de uitvoering van dit besluit.

Gegeven te Brussel, 20 december 2024.

FILIP

Van Koningswege :

De Minister van Justitie,
P. VAN TIGCHELT

De Minister van Defensie,
L. DEDONDER

De Minister van Binnenlandse Zaken,
A. VERLINDEN

Art. N1. Bijlage 1

Concordantie van de classificatieniveaus in toepassing van internationale overeenkomsten of verdragen die België binden, en het Belgische classificatieniveau.

België In het Nederlands: In het Frans: Optioneel voor int. gebruik markering aanvullen met:	ZEER GEHEIM (Wet 1.12.1998) TRÈS SECRET (Loi 11.12.1998) BE TOP SECRET	GEHEIM (Wet 1.12.1998) SECRET (Loi 11.12.1998) BE SECRET	VERTROUWELIJK (Wet 1.12.1998) CONFIDENTIEL (Loi 11.12.1998) BE CONFIDENTIAL	BEPERKT (Wet 1.12.1998) RESTREINT (Loi 11.12.1998) BE RESTRICTED
Noord-Atlantische Verdragsorganisatie	COSMIC TRÈS SECRET COSMIC TOP SECRET	OTAN SECRET NATO SECRET	OTAN CONFIDENTIEL NATO CONFIDENTIAL	OTAN RESTRICTED NATO RESTRICTED
Eurocontrol	/	Eurocontrol Geheim Eurocontrol Secret	Eurocontrol Vertraulich Eurocontrol Confidential Eurocontrol Confidential Eurocontrol Vertrouwelijk	/
Europees Ruimte- agentschap	ESA TOP SECRET	ESA SECRET	ESA CONFIDENTIAL	ESA RESTRICTED
Europese Unie Raad Commissie Euratom	TRÈS SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/ EU RESTRICTED
Cyprus Engelse equivalent:	Άκρως Απόρρητο TOP SECRET	Απόρρητο SECRET	Εμπιστευτικό CONFIDENTIAL	Περιορισμένης Χρήσης RESTRICTED

Duitsland	Streng Geheim	Geheim	VS- Vertraulich	/
Finland Engelse equivalent: In het Fins: In het Zweeds:	TOP SECRET ERITTÄIN SALAINEN YTTERST HEMLIG	SECRET SALAINEN HEMLIG	CONFIDENTIAL LUOTTAMUKSELLINEN KONFIDENTIELL	RESTRICTED KÄYTÖ RAOITETTU BEGRÄNSAD TILLGÅNG
Frankrijk vóór 1 juli 2021: na 1 juli 2021:	TRÈS SECRET DÉFENSE TRÈS SECRET	SECRET DÉFENSE SECRET	CONFIDENTIEL DÉFENSE Geen equivalentie – informatie wordt behandeld en beschermd overeenkomstig het classificatieniveau “GEHEIM”	/
Groothertogdom Luxemburg	TRÈS SECRET LUX	SECRET LUX	CONFIDENTIEL LUX	RESTREINT LUX
Hongarije	“Szigorúan titkos!”	“Titkos!”	“Bizalmas!”	“Korlátozott terjesztésű!”
Italië Engelse equivalent:	SEGRETISSIMO TOP SECRET	SEGRETO SECRET	RISERVATISSIMO CONFIDENTIAL	CONFIDENTIAL RESTRICTED
Nederland	Stg ZEER GEHEIM	Stg GEHEIM	Stg CONFIDENTIEEL	DEPARTEMENTAAL VERTROUWELIJK
Spanje	/	RESERVADO	CONFIDENTIAL	/

Verenigd Koninkrijk	UK TOP SECRET	UK SECRET	/	UK OFFICIAL-SENSITIVE	
Verenigde Staten	Top Secret	Secret	Confidential	/	
Zwitserland	Rigoureusement Secret Streng Geheim	Secret Geheim	Confidentiel Vertraulich	/	

Annexe 1

Équivalence des niveaux de classifications en application de conventions ou traités internationaux qui lient la Belgique, et le niveau de classification belge.

Belgique En langue néerlandaise: En langue française: En option pour l'utilisation int. compléter le marquage avec :	ZEER GEHEIM (Wet 1.12.1998) TRÈS SECRET (Loi 11.12.1998) BE TOP SECRET	GEHEIM (Wet 1.12.1998) SECRET (Loi 11.12.1998) BE SECRET	VERTROUWELIJK (Wet 1.12.1998) CONFIDENTIEL (Loi 11.12.1998) BE CONFIDENTIAL	BEPERKT (Wet 1.12.1998) RESTREINT (Loi 11.12.1998) BE RESTRICTED
Organisation du Traité de l'Atlantique Nord	COSMIC TRÈS SECRET COSMIC TOP SECRET	OTAN SECRET NATO SECRET	OTAN CONFIDENTIEL NATO CONFIDENTIAL	OTAN RESTRICTED NATO RESTRICTED
Eurocontrol	/	Eurocontrol Geheim Eurocontrol Secret	Eurocontrol Vertraulich Eurocontrol Confidentiel Eurocontrol Confidential Eurocontrol Vertrouwelijk	/
Agence spatiale européenne	ESA TOP SECRET	ESA SECRET	ESA CONFIDENTIAL	ESA RESTRICTED
Union européenne Conseil Commission Euratom	TRÈS SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Allemagne	Streng Geheim	Geheim	VS- Vertraulich	/
Chypre Equivalent anglais:	Άκρως Απόρρητο TOP SECRET	Απόρρητο SECRET	Εμπιστευτικό CONFIDENTIAL	Περιορισμένης Χρήσης RESTRICTED

Espagne	/	RESERVADO	CONFIDENTIAL	/
Etats-Unis	Top Secret	Secret	Confidential	/
Finlande Equivalent anglais: En langue finlandaise: En langue suédoise:	TOP SECRET ERITTÄIN SALAINEN YTTERST HEMLIG	SECRET SALAINEN HEMLIG	CONFIDENTIAL LUOTTAMUKSELLINEN KONFIDENTIELL	RESTRICTED KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
France avant le 1 ^{er} juillet 2021: après le 1 ^{er} juillet 2021:	TRÈS SECRET DÉFENSE TRÈS SECRET	SECRET DÉFENSE SECRET	CONFIDENTIEL DÉFENSE Pas d'équivalence – informations traitées et protégées comme des informations "SECRET"	/
Grand-Duché de Luxembourg	TRÈS SECRET LUX	SECRET LUX	CONFIDENTIEL LUX	RESTREINT LUX
Hongarie	"Szigorúan titkos!"	"Titkos!"	"Bizalmas!"	"Korlátozott terjesztésű!"
Italie Equivalent anglais:	SEGRETISSIMO TOP SECRET	SEGRETO SECRET	RISERVATISSIMO CONFIDENTIAL	CONFIDENTIAL RESTRICTED
Pays-Bas	Stg ZEER GEHEIM	Stg GEHEIM	Stg CONFIDENTIEEL	DEPARTEMENTAAL VERTROUWELIJK

Royaume-Uni	UK TOP SECRET	UK SECRET	/	UK OFFICIAL-SENSITIVE
Suisse	Rigoureusement Secret Streng Geheim	Secret Geheim	Confidentiel Vertraulich	/

NOTE EXPLICATIVE

1. BASE LEGALE

La procédure relative aux habilitations de sécurité résulte des deux lois du 11 décembre 1998 relatives à la classification, aux habilitations de sécurité, aux avis de sécurité et au service public réglementé et à la création d'un organe de recours en matière d'habilitations et d'avis de sécurité et de leurs arrêtés d'exécution. Ces textes peuvent être obtenus auprès de l'officier de sécurité.

2. L'ENQUETE DE SECURITE

a. Objectif

L'enquête de sécurité a pour but de vérifier si la personne qui en fait l'objet présente des garanties suffisantes sur le plan de la discrétion, de la loyauté et de l'intégrité.

b. Sources de renseignements

Les enquêteurs ont accès à la documentation des deux services de renseignement et de sécurité, au casier judiciaire central, aux casiers judiciaires et aux registres de la population et des étrangers tenus par les communes, ainsi qu'au registre national des personnes physiques et au registre d'attente des étrangers. Ils ont également accès aux données des services de police qui sont accessibles à l'ensemble des fonctionnaires de police lors de l'exécution des contrôles d'identité. Les enquêteurs peuvent en outre demander toute autre information utile en possession des services de police, aussi bien de la police administrative que de la police judiciaire.

Les enquêteurs peuvent obtenir de certains autres services publics, dont la liste est fixée par arrêté royal, toutes informations utiles dans deux domaines précis : tout ce qui concerne l'identification de la personne et tout ce qui permet de vérifier sa solvabilité financière.

Les enquêteurs peuvent solliciter la collaboration de toute autre personne dans le cadre de l'enquête de sécurité.

Enfin, les enquêteurs peuvent procéder à une enquête de voisinage, interroger l'intéressé et recueillir des renseignements à l'étranger.

Les enquêteurs ne recourent pas systématiquement à toutes les sources d'informations mentionnées ci-dessus. Le nombre de sources consultées varie en fonction du niveau de l'habilitation ou des éléments défavorables éventuellement recueillis lors de l'enquête.

c. Délai dans lequel la procédure doit être terminée

Les délais maximums sont de CINQ, SIX et NEUF mois respectivement pour les niveaux CONFIDENTIEL, SECRET et TRÈS SECRET, à partir de la réception par l'officier de sécurité des documents requis, dûment complétés.

Ces délais peuvent être prolongés de trois mois lorsque le service de renseignement et de sécurité doit recueillir des renseignements à l'étranger.

3. PERIODE DE VALIDITE D'UNE HABILITATION DE SECURITE

a. L'habilitation de sécurité est délivrée pour une période de CINQ ans maximum.

b. Le cas échéant, cette période peut être raccourcie en fonction des éléments recueillis lors de l'enquête ou pour adapter la durée de validité à la période pour laquelle l'habilitation de sécurité est demandée.

La période de validité prend cours à la date de la décision d'octroi de l'habilitation de sécurité.

4. CHANGEMENTS A COMMUNIQUER

Tout changement relatif aux données reprises dans le questionnaire de base doit être communiqué à l'officier de sécurité. S'il l'estime utile, celui-ci en informe l'autorité de sécurité.

5. ORGANE DE RECOURS EN MATIERE D'HABILITATIONS DE SECURITE

Lorsque l'octroi de l'habilitation de sécurité requise est refusé, lorsque la décision n'est pas intervenue ou n'a pas été notifiée dans le délai imparti ou lorsque l'habilitation de sécurité est retirée, la personne physique ou morale pour laquelle l'habilitation est demandée peut introduire un recours dans les trente jours qui suivent respectivement la notification de la décision ou l'expiration du délai, par courrier recommandé, auprès de l'organe de recours suivant :

Organe de recours en matière d'habilitations et d'avis de sécurité

Rue de Louvain 48/5
1000 Bruxelles
Tél : 02/286.29.11

	Naam: Graad: Handtekening:
--	----------------------------------

TOELICHTING

1. WETTELIJKE BASIS

De procedure met betrekking tot de veiligheidsmachtigingen vloeit voort uit de twee wetten van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, de veiligheidsadviezen en de publiek gereguleerde dienst en betreffende de oprichting van een beroepsorgaan inzake veiligheidsmachtigingen en veiligheidsadviezen en uit hun uitvoeringsbesluiten. Deze teksten kunnen bekomen worden bij de veiligheidsofficier.

2. HET VEILIGHEIDSONDERZOEK

a. Doelstelling

Het veiligheidsonderzoek heeft als doelstelling na te gaan of de persoon die er het voorwerp van uitmaakt, voldoende garanties biedt op het vlak van geheimhouding, loyaliteit en integriteit.

b. Informatiebronnen

De onderzoekers hebben toegang tot de documentatie van beide inlichtingen- en veiligheidsdiensten, het centraal strafregister, het gemeentelijk strafregister, de bevolkings- en vreemdelingenregisters bij de gemeentelijke administraties, alsook tot het Rijksregister van de natuurlijke personen en het wachtregister van de vreemdelingen. Zij hebben eveneens toegang tot de gegevens van de politiediensten, waartoe alle politiefunctionarissen toegang hebben voor de controle van de identiteit van een persoon. De onderzoekers mogen daarnaast alle andere nuttige gegevens, bijgehouden door de politiediensten, zowel van de bestuurlijke als van de gerechtelijke politie, vragen.

De onderzoekers kunnen van sommige andere overheidsdiensten, waarvan de lijst is vastgelegd bij koninklijk besluit, alle andere nuttige informatie verkrijgen in twee bepaalde domeinen : alles betreffende de identiteit van een persoon en alles wat zijn kredietwaardigheid kan vaststellen.

De onderzoekers kunnen aan elke andere persoon in het kader van het veiligheidsonderzoek om hun medewerking vragen.

Ten slotte kunnen de onderzoekers overgaan tot een omgevingsonderzoek, de betrokkene interviewen en inlichtingen in het buitenland inwinnen.

De onderzoekers consulteren niet systematisch alle hierboven vermelde bronnen. Het aantal geconsulteerde bronnen varieert in functie van het niveau van de veiligheidsmachtiging of negatieve elementen die in voorkomend geval tijdens het onderzoek worden bekomen.

c. Termijn waarbinnen de procedure moet afgerond worden

De maximale termijnen zijn VIJF, ZES en NEGEN maanden respectievelijk voor de niveaus VERTROUWELIJK, GEHEIM en ZEER GEHEIM, vanaf de ontvangst door de veiligheidsofficier van de correct en volledig ingevulde benodigde documenten.

Deze termijnen kunnen met drie maanden verlengd worden wanneer de inlichtingen- en veiligheidsdienst inlichtingen moet inwinnen in het buitenland.

3. DE GELDIGHEIDSTERMIJN VAN EEN VEILIGHEIDSMACHTIGING

a. De veiligheidsmachtiging wordt toegestaan voor een periode van maximaal VIJF jaar.

b. In voorkomend geval kan deze periode ingekort worden naargelang de tijdens het onderzoek bekomen elementen of om de geldigheidsduur aan te passen aan de termijn waarvoor de veiligheidsmachtiging wordt gevraagd.

De veiligheidstermijn vangt aan op datum van de beslissing van toekenning van de veiligheidsmachtiging.

4. MEE TE DELEN WIJZIGINGEN

Elke wijziging met betrekking tot de gegevens vermeld in de basisvragenlijst moet aan de veiligheidsofficier worden meegedeeld. Indien deze het nuttig acht, licht hij de veiligheidsoverheid in.

5. HET BEROEPSORGAAN INZAKE VEILIGHEIDSMACHTIGINGEN

Wanneer de toekenning van de vereiste veiligheidsmachtiging wordt geweigerd, wanneer de beslissing niet genomen of ter kennis gebracht is binnen de voorziene termijn, of wanneer de veiligheidsmachtiging wordt ingetrokken, kan de natuurlijke of rechtspersoon voor wie de machtiging vereist is, binnen de dertig dagen, respectievelijk na de kennisgeving of na het verstrijken van de termijn, bij aangetekend schrijven beroep instellen bij het volgende beroepsorgaan :

Beroepsorgaan inzake veiligheidsmachtigingen en veiligheidsadviezen

Leuvenseweg 48/5
1000 Brussel
Tel: 02/286.29.11

Art. N3. Annexe 3**Modèle :****A. Consentement de la personne pour laquelle l'autorisation est demandée****B. Avertissement des autres personnes majeures faisant l'objet d'une enquête de sécurité****ACCORD DE LA PERSONNE POUR LAQUELLE L'HABILITATION EST DEMANDEE***(Uniquement d'application si l'accord est légalement requis)***Art. 16 et 17 de la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, aux avis de sécurité et au service public réglementé**

Je soussigné(e) (Nom, prénom) né(e) à
 le, donne mon accord pour l'exécution de l'enquête
 de sécurité dans le cadre de la procédure d'octroi d'une habilitation de sécurité.
 Cet accord vaut également pour toute enquête ultérieure destinée à contrôler s'il est toujours satisfait aux conditions
 requises pour le niveau initial de l'habilitation de sécurité.
 Cet accord peut être retiré à tout moment par la personne concernée qui ne souhaite plus être soumise à une enquête de
 sécurité ou qui ne souhaite plus être titulaire d'une habilitation de sécurité.

Fait à, le

(Lieu, date, signature du demandeur)

AVERTISSEMENT DES AUTRES PERSONNES MAJEURES FAISANT L'OBJET D'UNE ENQUETE DE SECURITE**Art. 16 et 17 la loi relative à la classification, aux habilitations de sécurité, aux avis de sécurité et au service public réglementé**

Je déclare avoir personnellement averti les personnes qui font partie de l'enquête et dont l'identité suit, comme certifié
 par leur signature, excepté

Dans tous les cas, il s'agit du partenaire éventuel de la personne concernée (personne avec laquelle la personne concernée
 entretient une relation durable, qu'elle réside ou non à la même adresse). Pour l'enquête de niveau SECRET ou TRES
 SECRET, il s'agit également de toutes les autres personnes âgées de plus de 18 ans et habitant à la même adresse que la
 personne pour laquelle l'habilitation de sécurité a été demandée.

N°	Nom	Prénom(s)	Lieu et date de naissance	Signature
1				
2				
3				
4				
5				
6				
7				
8				

9				
10				

Fait à, le

(Lieu, date, signature du demandeur)

Si l'habilitation de sécurité est requise pour l'accès à un emploi, une fonction ou un grade, le refus explicite du candidat ou, le cas échéant, l'absence d'accord dans un délai de quinze jours suivant le jour de la réception du document l'avertissant de l'enquête, met automatiquement fin à la procédure de recrutement, d'engagement, de nomination ou de promotion (Art. 16. § 1er, alinéa 4, de la loi relative à la classification, aux habilitations de sécurité, aux avis de sécurité et au service public réglementé).

Art. N3. Bijlage 3**Model:**

- A. Instemming van de persoon voor wie de machtiging wordt gevraagd**
B. Kennisgeving aan de andere meerderjarige personen die het voorwerp uitmaken van een veiligheidsonderzoek

INSTEMMING VAN DE PERSOON VOOR WIE DE MACHTIGING WORDT GEVRAAGD*(Enkel van toepassing indien de instemming wettelijk vereist is)*

Art. 16 en 17 van de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, de veiligheidsadviezen en de publiek gereguleerde dienst

Ik ondergetekende (Naam, voornaam) geboren te
 op, geef mijn instemming tot het uitvoeren van een
 veiligheidsonderzoek in het kader van de procedure voor de toekenning van een veiligheidsmachtiging.

Deze instemming geldt eveneens voor enig later onderzoek dat erop gericht is na te gaan of nog steeds wordt
 voldaan aan de voorwaarden die vereist waren voor het aanvangsniveau van de veiligheidsmachtiging.

Deze instemming kan op ieder ogenblik ingetrokken worden door de betrokken persoon die niet langer wenst een
 veiligheidsonderzoek te ondergaan of houder te zijn van een veiligheidsmachtiging.

Opgemaakt te....., op

(Plaats, datum, handtekening aanvrager)

**KENNISGEVING AAN DE ANDERE MEERDERJARIGE PERSONEN DIE HET VOORWERP UITMAKEN VAN EEN
VEILIGHEIDSONDERZOEK**

Artikel 16 en 17 van de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, de veiligheidsadviezen en de publiek gereguleerde dienst

Ik verklaar de personen die het voorwerp uitmaken van dit onderzoek en waarvan de identiteit hieronder vermeld is,
 persoonlijk te hebben verwittigd, zoals bevestigd door hun handtekening, uitgezonderd

In elk geval gaat het om de eventuele partner van de betrokkene (persoon met wie de betrokkene een duurzame relatie heeft, al dan niet woonachtig op hetzelfde adres). Voor het onderzoek van het niveau GEHEIM of ZEER GEHEIM gaat het om alle andere personen ouder dan 18 jaar die met de persoon voor wie de veiligheidsmachtiging is aangevraagd op hetzelfde adres wonen.

Nr.	Naam	Voornaam	Geboorteplaats en -datum	Handtekening
1				
2				
3				
4				
5				
6				
7				

8				
9				
10				

Opgemaakt te, op

(Plaats, datum, handtekening aanvrager)

Indien de machtiging vereist is voor de toegang tot een betrekking, een functie of een graad, maakt de uitdrukkelijke weigering van de kandidaat of, in voorkomend geval, het uitblijven van de instemming binnen een termijn van vijftien kalenderdagen na de ontvangst van het document dat hem van het onderzoek op de hoogte brengt, automatisch een einde aan de procedure tot werving, indienstneming, benoeming of bevordering (Art. 16, § 1, vierde lid, van de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, de veiligheidsadviezen en de publiek gereguleerde dienst).

N.4. Annexe 4 :**Modèle :****Retrait de l'accord de la personne pour laquelle l'habilitation est demandée****AVIS DE RETRAIT DE L'ACCORD**

Art. 16 et 17 de la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, aux avis de sécurité et au service public réglementé

Je soussigné(Nom, prénoms) né(e)
à le, déclare par la présente
(Biffer la mention inutile) :

1. retirer à partir d'aujourd'hui l'accord que j'ai donné pour l'exécution d'une enquête de sécurité dans le cadre de la procédure d'octroi d'une habilitation de sécurité.

ou

2. ne plus consentir à être titulaire d'une habilitation de sécurité.

Je suis conscient que cette décision a comme conséquence que je ne peux plus avoir accès à des informations classifiées.

En outre, si l'habilitation est requise pour l'accès à un emploi, une fonction ou un grade, le refus explicite du candidat ou, le cas échéant, l'absence d'accord dans un délai de quinze jours suivant le jour de la réception du document l'avertissant de l'enquête, met automatiquement fin à la procédure de recrutement, d'engagement, de nomination ou de promotion (Art. 16, § 1er, alinéa 4, de la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, aux avis de sécurité et au service public réglementé).

Fait à, le

(Lieu, date, signature)

N.4. Bijlage 4:**Model:****Intrekking van de instemming van de persoon voor wie de machtiging wordt gevraagd****BERICHT VAN INTREKKING INSTEMMING**

**Art. 16 en 17 van de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen,
de veiligheidsadviezen en de publiek gereguleerde dienst**

Ik ondergetekende.....(Naam, voornaam) geboren te
op verklaar hierbij (*De onnodige vermelding schrappen*):

1. vanaf heden, mijn instemming in te trekken die ik gaf tot het uitvoeren van een veiligheidsonderzoek in het kader van de procedure voor toekenning van een veiligheidsmachtiging.

of

2. niet meer in te stemmen houder te zijn van een veiligheidsmachtiging.

Ik ben er mij van bewust dat deze beslissing tot gevolg zal hebben dat ik geen toegang meer kan hebben tot geclassificeerde informatie.

Bovendien, indien de machtiging vereist is voor de toegang tot een betrekking, een functie of een graad, maakt de uitdrukkelijke weigering van de kandidaat of, in voorkomend geval, het uitblijven van de instemming binnen een termijn van vijftien kalenderdagen na de ontvangst van het document dat hem van het onderzoek op de hoogte brengt, automatisch een einde aan de procedure tot werving, indienstneming, benoeming of bevordering (Art. 16, § 1, vierde lid, van de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, de veiligheidsadviezen en de publiek gereguleerde dienst).

Opgemaakt te....., op

(Plaats, datum, handtekening)

Art. N3. Annexe 3**Modèle :****Accusé de réception du questionnaire de base.****A****ACCUSE DE RECEPTION**

Je soussigné(e).....(*Nom, prénom*) officier de sécurité,

Déclare avoir reçu le questionnaire de base de(*Nom, prénom*)

Le questionnaire de base est dûment complété et signé.

L'intéressé(e) a donné son accord pour l'exécution d'une enquête de sécurité (*).

A.....le.....

(*Lieu, date, signature*)

(A couper – destiné à l'intéressé(e))

(*) Barrer si légalement non requis

B**ACCUSE DE RECEPTION**

Je soussigné(e).....(*Nom, prénom*) déclare avoir reçu ce jour un avertissement et un questionnaire de base. Je m'engage à rendre le questionnaire de base dûment complété et signé endéans les quinze jours à l'officier de sécurité de l'unité, de la firme ou de l'organisme, auquel (à laquelle) j'appartiens, ou auprès duquel (de laquelle) je postule à un emploi.

A.....le.....

(*Lieu, date, signature*)

(A couper – destiné à l'officier de sécurité))

Art. N.5. Bijlage 5:**Model:****Bericht van ontvangst van de basisvragenlijst.****A****BERICHT VAN ONTVANGST**

Ik ondergetekende.....(Naam, voornaam)
veiligheidsofficier,
Verklaar de basisvragenlijst van(Naam,
voornaam) te hebben ontvangen.
De basisvragenlijst is correct en volledig ingevuld en werd ondertekend.
Betrokkene heeft zijn instemming tot het voeren van een veiligheidsonderzoek
gegeven (*).

Te.....de.....

(Plaats, datum, handtekening)
(Afsnijden – bestemd voor de betrokkene)

(*) Schrappen indien wettelijk niet vereist

B**BERICHT VAN ONTVANGST**

Ik ondergetekende.....(Naam, voornaam) verklaar
heden een kennisgeving en een basisvragenlijst ontvangen te hebben. Ik
verbind er mij toe de basisvragenlijst binnen de vijftien dage correct en
volledig ingevuld en ondertekend terug over te maken aan de
veiligheidsofficier van de eenheid, firma of het organisme, waartoe ik behoor
of waarbij ik gepostuleerd heb voor een betrekking.

Te.....de.....

(Plaats, datum, handtekening)
(Afsnijden – bestemd voor de veiligheidsofficier))