DÉCISION (UE) 2021/259 DE LA COMMISSION

du 10 février 2021

établissant des modalités d'application en matière de sécurité industrielle en ce qui concerne les subventions classifiées

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 249,

vu le traité instituant la Communauté européenne de l'énergie atomique, et notamment son article 106,

vu le règlement (UE, Euratom) 2018/1046 du Parlement européen et du Conseil du 18 juillet 2018 relatif aux règles financières applicables au budget général de l'Union, modifiant les règlements (UE) nº 1296/2013, (UE) nº 1301/2013, (UE) nº 1303/2013, (UE) nº 1304/2013, (UE) nº 1309/2013, (UE) nº 1316/2013, (UE) nº 223/2014, (UE) nº 283/2014 et la décision nº 541/2014/UE, et abrogeant le règlement (UE, Euratom) nº 966/2012 ([1]),

vu la décision (UE, Euratom) 2015/443 de la Commission du 13 mars 2015 relative à la sécurité au sein de la Commission ([2]),

vu la décision (UE, Euratom) 2015/444 de la Commission du 13 mars 2015 concernant les règles de sécurité aux fins de la protection des informations classifiées de l'Union européenne ([3]),

vu la décision (UE, Euratom) 2017/46 de la Commission du 10 janvier 2017 sur la sécurité des systèmes d'information et de communication au sein de la Commission européenne ([4]),

après consultation du groupe d'experts sécurité de la Commission, conformément à l'article 41, paragraphe 5, de la décision (UE, Euratom) 2015/444,

considérant ce qui suit:

(1) Les articles 41, 42, 47 et 48 de la décision (UE, Euratom) 2015/444 prévoient que des dispositions plus détaillées destinées à compléter et étayer le chapitre 6 de ladite décision doivent être définies dans des modalités d'application en matière de sécurité industrielle, régissant des aspects tels que l'octroi de conventions de subvention classifiées, les habilitations de sécurité d'établissement, les habilitations de sécurité du personnel, les visites et la transmission et le transport d'informations classifiées de l'Union européenne («ICUE»).

(2) Aux termes de la décision (UE, Euratom) 2015/444, les conventions de subvention classifiées doivent être exécutées en étroite coopération avec l'autorité nationale de sécurité, l'autorité de sécurité désignée ou toute autre autorité compétente des États membres concernés. Les États membres sont convenus de veiller à ce que toute entité relevant de leur juridiction qui peut recevoir ou produire des informations classifiées provenant de la Commission possède une habilitation de sécurité appropriée et soit en mesure d'assurer une protection adéquate équivalente à celle qui est accordée par les règles de sécurité du Conseil de l'Union européenne aux fins de la protection des informations classifiées de l'Union européenne portant un marquage de classification correspondant, conformément à l'accord entre les États membres de l'Union européenne, réunis au sein du Conseil, relatif à la protection des informations classifiées échangées dans l'intérêt de l'Union européenne (2011/C 202/05) ([5]).

([1]) JO L 193 du 30.7.2018, p. 1.
([2]) JO L 72 du 17.3.2015, p. 41.
([3]) JO L 72 du 17.3.2015, p. 53.
([4]) JO L 6 du 11.1.2017, p. 40.
([5]) JO C 202 du 8.7.2011, p. 13.

(3) Le Conseil, la Commission et le haut représentant de l'Union pour les affaires étrangères et la politique de sécurité sont convenus de garantir une cohérence maximale dans l'application des règles de sécurité en ce qui concerne la protection des ICUE tout en tenant compte des besoins institutionnels et organisationnels qui leur sont propres, conformément aux déclarations jointes au procès-verbal de la session du Conseil au cours de laquelle a été adoptée la décision 2013/488/UE du Conseil ([6]) concernant les règles de sécurité aux fins de la protection des informations classifiées de l'Union européenne.

(4) En conséquence, les modalités d'application de la Commission en matière de sécurité industrielle en ce qui concerne les subventions classifiées devraient également garantir une cohérence maximale et tenir compte des lignes directrices en matière de sécurité industrielle approuvées par le comité de sécurité du Conseil le 13 décembre 2016.

(5) Le 4 mai 2016, la Commission a adopté une décision ([7]) qui habilite le membre de la Commission chargé des questions de sécurité à adopter, au nom de la Commission et sous sa responsabilité, les modalités d'application prévues par l'article 60 de la décision (UE, Euratom) 2015/444,

A ADOPTÉ LA PRÉSENTE DÉCISION:

CHAPITRE 1

DISPOSITIONS GÉNÉRALES

Article premier

Objet et champ d'application

1. La présente décision établit des modalités d'application en matière de sécurité industrielle en ce qui concerne les subventions classifiées au sens de la décision (UE, Euratom) 2015/444, et notamment le chapitre 6 de ladite décision.

2. Elle définit des exigences spécifiques visant à garantir la protection des informations classifiées de l'Union européenne (ICUE) lors de la publication d'appels à propositions, lors de l'octroi de subventions et lors de l'exécution des conventions de subvention classifiées conclues par la Commission européenne.

3. La présente décision porte sur les subventions mettant en jeu des informations classifiées aux niveaux suivants:

a) RESTREINT UE/EU RESTRICTED;

b) CONFIDENTIEL UE/EU CONFIDENTIAL;

c) SECRET UE/EU SECRET.

4. La présente décision est applicable sans préjudice de règles spécifiques établies dans d'autres actes juridiques, tels que ceux relatifs au programme européen de développement industriel dans le domaine de la défense.

Article 2

Responsabilités au sein de la Commission

1. Dans le cadre des responsabilités qui lui incombent en vertu du règlement (UE, Euratom) 2018/1046 du Parlement européen et du Conseil, l'ordonnateur de l'autorité octroyant la subvention veille à ce que la subvention classifiée soit conforme à la décision (UE, Euratom) 2015/444 et à ses modalités d'application.

([6]) Décision 2013/488/UE du Conseil du 23 septembre 2013 concernant les règles de sécurité aux fins de la protection des informations classifiées de l'Union européenne (JO L 274 du 15.10.2013, p. 1).

([7]) Décision de la Commission du 4 mai 2016 relative à une habilitation en matière de sécurité [C(2016) 2797 final].

2. À cette fin, l'ordonnateur compétent demande, à chaque stade, l'avis de l'autorité de sécurité de la Commission sur les questions relatives aux éléments de sécurité d'une convention de subvention, d'un programme ou d'un projet classifiés et informe le responsable local de la sécurité des conventions de subvention classifiées conclues. La décision relative au niveau de classification d'un thème donné appartient à l'autorité octroyant la subvention, qui se prononce en tenant dûment compte du guide de la classification de sécurité.

3. Lorsque les instructions de sécurité relatives à un programme ou un projet visées à l'article 5, paragraphe 3, sont appliquées, l'autorité octroyant la subvention et l'autorité de sécurité de la Commission s'acquittent des responsabilités qui leur incombent en vertu desdites instructions.

4. En respectant les exigences des présentes modalités d'application, l'autorité de sécurité de la Commission coopère étroitement avec les autorités nationales de sécurité («ANS») et les autorités de sûreté désignées («ASD») des États membres concernés, notamment en ce qui concerne les habilitations de sécurité d'établissement («HSE») et les habilitations de sécurité du personnel («HSP»), les procédures de visite et les plans de transport.

5. Lorsque les subventions sont gérées par des agences exécutives ou d'autres organismes de financement de l'Union et que les règles spécifiques établies dans d'autres actes juridiques visés à l'article 1er, paragraphe 4, ne sont pas applicables:

a) le service délégant de la Commission exerce les droits relevant de l'autorité d'origine de toutes les ICUE produites dans le contexte des subventions si les modalités de délégation le prévoient;

b) le service délégant de la Commission est responsable de la détermination de la classification de sécurité;

c) les demandes d'informations pour habilitation de sécurité et les notifications aux ANS/ASD sont transmises par l'intermédiaire de l'autorité de sécurité de la Commission.

CHAPITRE 2

TRAITEMENT DES APPELS À PROPOSITIONS EN VUE DE L'OCTROI DE SUBVENTIONS CLASSIFIÉES

Article 3

Principes de base

1. Les parties classifiées des subventions sont appliquées uniquement par des bénéficiaires immatriculés dans un État membre, ou par des bénéficiaires immatriculés dans un pays tiers ou mis en place par une organisation internationale lorsque ce pays tiers ou cette organisation internationale a conclu un accord sur la sécurité des informations avec l'Union européenne ou un arrangement administratif avec la Commission ([8]).

2. Avant de lancer un appel à propositions en vue de l'octroi d'une subvention classifiée, l'autorité octroyant la subvention détermine la classification de sécurité de toute information susceptible d'être communiquée aux candidats. L'autorité octroyant la subvention détermine également la classification de sécurité maximale de toute information utilisée ou produite dans le cadre de l'exécution de la convention de subvention, du programme ou du projet, ou prévoit au moins le volume et le type d'informations à produire ou à traiter, ainsi que la nécessité d'un système d'information et de communication (SIC) classifié.

3. L'autorité octroyant la subvention veille à ce que les appels à propositions pour les subventions classifiées procurent des informations sur les obligations particulières en matière de sécurité liées aux informations classifiées. Les documents de l'appel à propositions précisent les délais dans lesquels les bénéficiaires doivent, si nécessaire, obtenir les habilitations de sécurité d'établissement (HSE). Les annexes I et II contiennent des modèles d'informations concernant les conditions relatives à l'appel à propositions.

([8]) La liste des accords conclus par l'Union européenne et des arrangements administratifs conclus par la Commission européenne, en vertu desquels des informations classifiées de l'Union européenne peuvent être échangées avec des pays tiers et des organisations internationales, est consultable sur le site internet de la Commission.

4. L'autorité octroyant la subvention veille à ce que les informations classifiées RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET ne soient divulguées aux candidats qu'une fois qu'ils ont signé un accord de confidentialité leur faisant obligation de traiter et de protéger les ICUE conformément à la décision (UE, Euratom) 2015/444, aux modalités d'application de cette dernière et aux règles nationales applicables.

5. Lorsque des informations RESTREINT UE/EU RESTRICTED sont communiquées aux candidats, les exigences minimales visées à l'article 5, paragraphe 7, de la présente décision sont mentionnées dans l'appel ou dans les accords de confidentialité conclus au stade de la proposition.

6. Tous les candidats et les bénéficiaires qui doivent traiter ou stocker des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET au sein de leurs établissements, au stade de la proposition ou durant l'exécution de la convention de subvention classifiée elle-même, détiennent une HSE au niveau requis, sauf dans les cas mentionnés au paragraphe 9. Ci-après sont indiqués les trois cas de figure qui peuvent se présenter au stade de l'appel à propositions pour une subvention classifiée mettant en jeu des ICUE au niveau CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET:

a) aucun accès aux ICUE au niveau CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET au stade de l'appel à propositions:

   lorsque l'appel à propositions concerne une subvention qui comportera des informations des ICUE au niveau CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET, mais ne requiert pas que le candidat traite ces informations au stade de l'appel à propositions, un candidat qui ne détient pas de HSE au niveau requis n'est pas exclu de la procédure de candidature au motif qu'il ne détient pas de HSE;

b) aucun accès aux ICUE au niveau CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET dans les locaux de l'autorité octroyant la subvention au stade de l'appel à propositions:

   l'accès aux informations est accordé au personnel du candidat qui détient une HSP au niveau requis et qui a un besoin d'en connaître;

c) traitement ou stockage d'ICUE au niveau CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET dans les locaux du candidat au stade de la proposition:

   lorsque l'appel à propositions exige des candidats qu'ils traitent ou stockent des ICUE dans leurs locaux, le candidat détient une HSE au niveau requis. En pareilles circonstances, l'autorité octroyant la subvention obtient, par l'intermédiaire de l'autorité de sécurité de la Commission, l'assurance de l'ANS ou de l'ASD concernée que le candidat a reçu une HSE appropriée avant que ne lui soient fournies des ICUE. L'accès aux informations est accordé au personnel du candidat qui détient une HSP au niveau requis et qui a un besoin d'en connaître.

7. En principe, une HSE ou une HSP n'est pas requise pour avoir accès aux informations classifiées RESTREINT UE/EU RESTRICTED, que ce soit au stade de la proposition ou pour l'exécution de la convention de subvention. Lorsque des États membres exigent une HSE ou une HSP pour des conventions de subvention ou des contrats de sous-traitance au niveau RESTREINT UE/EU RESTRICTED en vertu de leurs dispositions législatives et réglementaires nationales, comme indiqué à l'annexe IV, ces exigences nationales n'imposent aucune obligation supplémentaire aux autres États membres ou n'excluent pas les candidats, les bénéficiaires ou les sous-traitants des États membres qui n'imposent pas une telle HSE ou une telle HSP pour l'accès aux informations RESTREINT UE/EU RESTRICTED issues de conventions de subvention/contrats de sous-traitance connexes ou d'une mise en concurrence pour de tels conventions/contrats. Ces conventions de subvention sont exécutées dans les États membres conformément à leurs dispositions législatives et réglementaires.

8. Lorsqu'une HSE est requise pour le traitement d'un appel à propositions et pour l'application d'une convention de subvention classifiée, l'autorité octroyant la subvention présente, par l'intermédiaire de l'autorité de sécurité de la Commission, une demande à l'ANS/ASD du bénéficiaire au moyen d'une fiche d'information pour habilitation de sécurité d'établissement («FIHSE») ou sous la forme d'un document électronique équivalent prévu à cet effet. L'annexe III, appendice D, contient un exemple de FIHSE ([9]). Il est répondu à la FIHSE, dans la mesure du possible, dans un délai de dix jours ouvrables à compter de la date de la demande.

9. Lorsque des établissements publics des États membres ou des établissements soumis au contrôle de leurs gouvernements participent à des subventions classifiées pour lesquels des HSE sont exigées, mais que des HSE ne sont pas délivrées pour des établissements de ce type en vertu des législations nationales, l'autorité octroyant la subvention vérifie auprès de l'ANS ou de l'ASD concernée, par l'intermédiaire de l'autorité de sécurité de la Commission, que ces établissements publics sont capables de traiter des ICUE au niveau requis.

([9]) D'autres formulaires utilisés peuvent différer, de par leur conception, de l'exemple fourni dans les présentes modalités d'application.

10. Lorsqu'une HSP est requise pour l'exécution d'une convention de subvention classifiée et lorsque, conformément aux règles nationales, une HSE est nécessaire avant qu'une HSP soit octroyée, l'autorité octroyant la subvention vérifie, auprès de l'ANS ou de l'ASD du bénéficiaire, par l'intermédiaire de l'autorité de sécurité de la Commission, au moyen d'une FIHSE, que le bénéficiaire détient une HSE ou que le processus d'obtention d'une HSE est en cours. Dans ce cas, la Commission n'envoie pas de demande de HSP au moyen d'une fiche d'information pour habilitation de sécurité du personnel («FIHSP»).

Article 4

Sous-traitance dans le cadre de subventions classifiées

1. Les conditions auxquelles les bénéficiaires peuvent sous-traiter des tâches mettant en jeu des ICUE sont définies dans l'appel à propositions ainsi que dans la convention de subvention. Ces conditions incluent l'exigence selon laquelle toutes les FIHSE doivent être transmises par l'intermédiaire de l'autorité de sécurité de la Commission. La sous-traitance fait l'objet d'un consentement écrit préalable de l'autorité octroyant la subvention. Le cas échéant, la sous-traitance est conforme aux exigences prévues dans l'acte de base établissant le programme.

2. Les parties classifiées des subventions sont sous-traitées uniquement à des entités immatriculées dans un État membre, ou à des entités immatriculées dans un pays tiers ou mises en place par une organisation internationale lorsque ce pays tiers ou cette organisation internationale a conclu un accord sur la sécurité des informations avec l'Union européenne ou un arrangement administratif avec la Commission ([10]).

CHAPITRE 3

TRAITEMENT DES SUBVENTIONS CLASSIFIÉES

Article 5

Principes de base

1. Lors de l'attribution d'une subvention classifiée, l'autorité octroyant la subvention, conjointement avec l'autorité de sécurité de la Commission, veille à ce que les obligations des bénéficiaires en matière de protection des ICUE utilisées ou produites dans le cadre de l'exécution de la subvention classifiée fassent partie intégrante de la convention de subvention. Les exigences de sécurité propres à une subvention prennent la forme d'une annexe de sécurité («AS»). Un modèle d'AS figure à l'annexe III.

2. Avant de signer une subvention classifiée, l'autorité octroyant la subvention approuve un guide de la classification de sécurité («GCS») pour les tâches à effectuer et les informations produites dans le cadre de l'exécution de la convention de subvention, ou au niveau du programme ou du projet, le cas échéant. Le GCS fait partie de l'AS.

3. Les exigences de sécurité propres à un programme ou un contrat prennent la forme d'instructions de sécurité relatives à un programme (ou un projet) («ISP»). Les ISP peuvent être rédigées à l'aide des dispositions du modèle d'AS figurant à l'annexe III. Les ISP sont élaborées par le service de la Commission qui gère le programme ou le projet, en étroite coopération avec l'autorité de sécurité de la Commission et sont soumises pour avis au groupe d'experts sécurité de la Commission. Lorsqu'une convention de subvention relève d'un programme ou d'un projet ayant ses propres ISP, l'AS de la convention de subvention doit revêtir une forme simplifiée et comporter une référence aux dispositions de sécurité exposées dans les ISP du programme ou du projet.

4. À l'exception des cas mentionnés à l'article 3, paragraphe 9, la convention de subvention classifiée n'est pas signée avant que l'ANS ou l'ASD du candidat n'ait confirmé l'obtention d'une HSE par le candidat ou, lorsque la convention de subvention classifiée est octroyée à un consortium, avant que l'ANS ou l'ASD d'au minimum un candidat appartenant au consortium, ou plus si nécessaire, ait confirmé l'obtention d'une HSE par le candidat.

5. En principe, et sauf règles pertinentes contraires, l'autorité octroyant la subvention est considérée comme l'autorité d'origine des ICUE produites au cours de l'exécution de la convention de subvention.

([10]) La liste des accords conclus par l'Union européenne et des arrangements administratifs conclus par la Commission européenne, en vertu desquels des informations classifiées de l'Union européenne peuvent être échangées avec des pays tiers et des organisations internationales, est consultable sur le site internet de la Commission.

6. L'autorité octroyant la subvention, par l'intermédiaire de l'autorité de sécurité de la Commission, informe les ANS ou les ASD de tous les bénéficiaires et sous-traitants de la signature de conventions de subvention ou de contrats de sous-traitance classifiés et de toute prolongation ou résiliation anticipée de ces conventions de subvention ou contrats de sous-traitance. La liste des exigences par pays figure à l'annexe IV.

7. Les conventions de subvention mettant en jeu des informations classifiées RESTREINT UE/EU RESTRICTED incluent une clause de sécurité rendant contraignantes pour les bénéficiaires les dispositions figurant à l'annexe III, appendice E. Ces conventions de subvention contiennent une AS exposant, au minimum, les exigences en matière de traitement des informations RESTREINT UE/EU RESTRICTED, y compris les aspects relatifs à l'assurance de l'information et les exigences spécifiques que doivent remplir les bénéficiaires en vue de l'agrément de leur SIC traitant des informations RESTREINT UE/EU RESTRICTED.

8. Lorsque les dispositions législatives et réglementaires nationales des États membres l'exigent, les ANS ou les ASD veillent à ce que les bénéficiaires ou sous-traitants relevant de leur juridiction respectent les dispositions applicables en matière de sécurité pour la protection des informations RESTREINT UE/EU RESTRICTED et effectuent des visites de vérification auprès des établissements des bénéficiaires ou des sous-traitants situés sur leur territoire. Lorsque l'ANS ou l'ASD n'est pas soumise à une telle obligation, l'autorité octroyant la subvention veille à ce que les bénéficiaires mettent en œuvre les dispositions de sécurité requises énoncées à l'annexe III, appendice E.

Article 6

Accès aux ICUE par le personnel des bénéficiaires et sous-traitants

1. L'autorité octroyant la subvention veille à ce que les conventions de subvention classifiées renferment des dispositions indiquant que le personnel des bénéficiaires ou sous-traitants qui, aux fins de l'exécution de la convention de subvention ou du contrat de sous-traitance classifiés, requiert l'accès à des ICUE, peut se voir accorder un tel accès uniquement si les conditions suivantes sont remplies:

a) avoir un besoin établi d'en connaître;

b) pour les informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET, avoir reçu une habilitation de sécurité du niveau correspondant par l'ANS ou l'ASD ou toute autre autorité de sécurité compétente;

c) avoir été informé des règles de sécurité applicables à la protection des ICUE et avoir reconnu les responsabilités qui lui incombent en matière de protection de ces informations.

2. Le cas échéant, l'accès aux ICUE est également conforme à l'acte de base établissant le programme et tient compte des marquages complémentaires définis dans le GCS.

3. Si un bénéficiaire ou un sous-traitant souhaite employer un ressortissant d'un pays non-membre de l'Union européenne à une fonction qui requiert l'accès à des ICUE classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET, il incombe au bénéficiaire ou au sous-traitant d'engager la procédure d'habilitation de sécurité concernant cette personne conformément aux dispositions législatives et réglementaires nationales applicables sur le lieu où l'accès aux ICUE doit être accordé.

Article 7

Accès aux ICUE par les experts prenant part à des contrôles, des examens ou des audits

1. Les externes (les «experts») qui prennent part à des contrôles, des examens ou des audits exécutés par l'autorité octroyant la subvention ou à des examens des performances des bénéficiaires nécessitant un accès à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET ne peuvent se voir offrir un contrat que lorsqu'ils ont reçu de l'ANS, de l'ASD ou de toute autre autorité de sécurité compétente une habilitation de sécurité du niveau correspondant. L'autorité octroyant la subvention, par l'intermédiaire de l'autorité de sécurité de la Commission, procède aux vérifications et, le cas échéant, demande à l'ANS ou à l'ASD de lancer la procédure de vérification en ce qui concerne les experts au minimum six mois avant le début de leurs contrats respectifs.

2. Avant la signature de leurs contrats, les experts sont informés des règles de sécurité applicables à la protection des ICUE et reconnaissent les responsabilités qui leur incombent en matière de protection de ces informations.

CHAPITRE 4

VISITES LIÉES À DES CONVENTIONS DE SUBVENTION CLASSIFIÉES

Article 8

Principes de base

1. Lorsque l'autorité octroyant la subvention, des experts, des bénéficiaires ou des sous-traitants doivent avoir accès à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET dans leurs locaux respectifs dans le contexte de l'application d'une convention de subvention classifiée, les visites sont organisées en liaison avec les ANS ou les ASD ou toute autre autorité de sécurité compétente concernée.

2. Les visites visées au paragraphe 1 sont soumises aux exigences suivantes:

a) la visite a un motif officiel lié à une subvention classifiée;

b) tout visiteur détient une HSP au niveau requis et jouit, sur la base du principe du besoin d'en connaître, d'un accès aux ICUE utilisées ou produites dans le cadre de l'application de la subvention classifiée.

Article 9

Demandes de visite

1. Les visites effectuées par les bénéficiaires ou les sous-traitants dans les établissements d'autres bénéficiaires ou sous-traitants, ou dans les locaux de l'autorité octroyant la subvention, qui impliquent l'accès à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET, sont organisées selon la procédure suivante:

a) le responsable de la sécurité de l'établissement qui envoie le visiteur remplit toutes les parties pertinentes du formulaire de demande de visite (DDV) et soumet la demande à l'ANS ou à l'ASD de l'établissement. Un modèle de formulaire de DDV figure à l'annexe III, appendice C;

b) l'ANS ou l'ASD de l'établissement d'envoi doit confirmer l'HSP du visiteur avant de soumettre la DDV à l'ANS ou à l'ASD de l'établissement d'accueil (ou à l'autorité de sécurité de la Commission si la visite a lieu dans les locaux de l'autorité octroyant la subvention);

c) le responsable de la sécurité de l'établissement d'envoi obtient ensuite de son ANS ou son ASD la réponse de l'ANS ou de l'ASD de l'établissement d'accueil (ou de l'autorité de sécurité de la Commission) signifiant l'approbation ou le rejet de la DDV;

d) une DDV est réputée approuvée si aucune objection n'est formulée dans les cinq jours ouvrables qui précèdent la date de la visite.

2. Les visites qui sont effectuées par des fonctionnaires ou des experts ou des auditeurs de l'autorité octroyant la subvention dans les établissements de bénéficiaires ou de sous-traitants et qui impliquent l'accès à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET sont organisées selon la procédure suivante:

a) le visiteur remplit toutes les parties pertinentes du formulaire de DDV et soumet celui-ci à l'autorité de sécurité de la Commission;

b) l'autorité de sécurité de la Commission confirme l'HSP du visiteur avant de soumettre la DDV à l'ANS ou à l'ASD de l'établissement d'accueil;

c) l'autorité de sécurité de la Commission obtient une réponse de l'ANS ou de l'ASD de l'établissement d'accueil signifiant l'approbation ou le rejet de la DDV;

d) une DDV est réputée approuvée si aucune objection n'est formulée dans les cinq jours ouvrables qui précèdent la date de la visite.

3. Une DDV peut couvrir une seule visite ou des visites récurrentes. Dans le cas de visites récurrentes, la DDV peut être valable pendant une durée maximale d'un an à compter de la date de début demandée.

4. La durée de validité de la DDV n'excède pas la durée de validité de l'HSP du visiteur.

5. En règle générale, la DDV doit être soumise à l'autorité de sécurité compétente de l'établissement d'accueil au moins 15 jours ouvrables avant la date de la visite.

Article 10

Procédures de visite

1. Avant d'autoriser l'accès de visiteurs à des ICUE, le bureau de sécurité de l'établissement d'accueil se conforme à toutes les procédures et règles de sécurité relatives aux visites qui sont définies par son ANS ou son ASD.

2. Les visiteurs déclinent leur identité à leur arrivée dans l'établissement d'accueil en présentant une carte d'identité ou un passeport en cours de validité. Ces informations d'identification correspondent aux renseignements fournis dans la DDV.

3. L'établissement d'accueil veille à tenir un registre de tous les visiteurs, indiquant leur nom, l'organisation qu'ils représentent, la date d'expiration de l'HSP, la date de la visite et le nom des personnes auxquelles il est rendu visite. Ces registres sont conservés pendant une période d'au moins cinq ans, ou plus si les règles et réglementations nationales du pays dans lequel est situé l'établissement d'accueil l'exigent.

Article 11

Visites organisées directement

1. Dans le cadre de projets spécifiques, les ANS ou les ASD compétentes et l'autorité de sécurité de la Commission peuvent convenir d'une procédure permettant au responsable de la sécurité du visiteur et au responsable de la sécurité de l'établissement à visiter d'organiser directement des visites pour une subvention classifiée spécifique. Un modèle du formulaire à utiliser à cette fin figure à l'annexe III, appendice C. Cette procédure exceptionnelle est définie dans les ISP ou dans le cadre d'autres arrangements spécifiques. En pareil cas, les procédures prévues à l'article 9 et à l'article 10, paragraphe 1, ne s'appliquent pas.

2. Les visites impliquant l'accès à des informations classifiées RESTREINT UE/EU RESTRICTED sont organisées directement entre l'entité d'envoi et l'entité d'accueil sans qu'il soit nécessaire de suivre les procédures prévues à l'article 9 et à l'article 10, paragraphe 1.

CHAPITRE 5

TRANSMISSION ET TRANSPORT D'ICUE LORS DE L'EXÉCUTION DE CONVENTIONS DE SUBVENTION CLASSIFIÉES

Article 12

Principes de base

L'autorité octroyant la subvention veille à ce que toutes les décisions relatives au transfert et au transport d'ICUE soient conformes à la décision (UE, Euratom) 2015/444 et à ses modalités d'application, ainsi qu'aux dispositions de la convention de subvention classifiée, comprenant le consentement de l'autorité d'origine.

Article 13

Traitement électronique

1. Le traitement et la transmission électroniques d'ICUE sont effectués conformément aux chapitres 5 et 6 de la décision (UE, Euratom) 2015/444 de la Commission et à ses modalités d'application.

Les systèmes d'information et de communication détenus par un bénéficiaire et utilisés pour traiter des ICUE aux fins de l'exécution de la convention de subvention («SIC du bénéficiaire») sont soumis à l'agrément de l'autorité d'homologation de sécurité (AHS) compétente. Toute transmission d'ICUE par voie électronique est protégée par des produits cryptographiques approuvés conformément à l'article 36, paragraphe 4, de la décision (UE, Euratom) 2015/444. Des mesures de sécurité TEMPEST sont mises en œuvre conformément à l'article 36, paragraphe 6, de ladite décision.

2. L'habilitation de sécurité du SIC du bénéficiaire qui traite des ICUE au niveau RESTREINT UE/EU RESTRICTED et toute interconnexion y afférente peuvent être déléguées au responsable de la sécurité d'un bénéficiaire si les dispositions législatives et réglementaires nationales le permettent. Lorsque cette tâche est déléguée, le bénéficiaire est responsable de la mise en œuvre des exigences minimales en matière de sécurité décrites dans l'AS lors du traitement d'informations RESTREINT UE/EU RESTRICTED dans son SIC. Toutefois, les ANS ou les ASD et AHS compétentes demeurent responsables de la protection des informations RESTREINT UE/EU RESTRICTED traitées par le bénéficiaire et conservent le droit de contrôler les mesures de sécurité prises par les bénéficiaires. En outre, le bénéficiaire fournit à l'autorité octroyant la subvention et, lorsque les dispositions législatives et réglementaires nationales l'exigent, à l'AHS nationale compétente, une déclaration de conformité attestant que le SIC du bénéficiaire et les interconnexions s'y rapportant ont été agréés pour traiter des ICUE au niveau RESTREINT UE/EU RESTRICTED ([11]).

Article 14

Transport par des services de courrier commercial

Le transport d'ICUE par des services de courrier commercial est conforme aux dispositions pertinentes de la décision (UE, Euratom) 2019/1962 de la Commission ([12]) fixant les modalités d'application relatives au traitement des informations RESTREINT UE/EU RESTRICTED et de la décision (UE, Euratom) 2019/1961 de la Commission ([13]) fixant les modalités d'application relatives au traitement des informations CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET.

Article 15

Transport par porteur

1. Le transport par porteur d'informations classifiées est soumis à des exigences strictes en matière de sécurité.

2. Le transport par porteur d'informations classifiées RESTREINT UE/EU RESTRICTED peut être effectué par un membre du personnel du bénéficiaire à l'intérieur de l'Union européenne, pour autant que les conditions suivantes soient remplies:

a) l'enveloppe ou l'emballage utilisé(e) est opaque et ne comporte aucune indication de la classification de son contenu;

b) le porteur ne se sépare pas des informations classifiées;

c) l'enveloppe ou l'emballage n'est pas ouvert(e) pendant le transport.

3. Pour les informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET, le transport par porteur effectué par un membre du personnel du bénéficiaire dans un État membre est organisé à l'avance par l'entité expéditrice et l'entité destinataire. L'autorité expéditrice ou l'établissement expéditeur informe l'autorité ou l'établissement destinataire des éléments relatifs à l'envoi, en indiquant notamment la référence, la classification, l'heure d'arrivée prévue et le nom du service de courrier. Ce transport par porteur est autorisé pour autant que les conditions suivantes soient remplies:

a) les informations classifiées sont transportées sous double enveloppe/emballage;

b) l'enveloppe ou l'emballage extérieur(e) est sécurisé(e) et ne porte pas d'indication sur la classification de son contenu, tandis que l'enveloppe intérieure indique le niveau de classification;

c) le porteur ne se sépare pas des ICUE;

d) l'enveloppe ou l'emballage n'est pas ouvert(e) pendant le transport;

e) l'enveloppe ou l'emballage est transporté(e) dans un porte-documents fermant à clé ou emballage similaire agréé qui, de par ses dimensions et son poids, doit pouvoir rester en permanence en la possession personnelle du porteur et ne doit pas être déposé(e) dans une soute à bagage;

f) le porteur est muni d'un certificat de courrier délivré par son autorité de sécurité compétente qui l'autorise à transporter l'envoi classifié dûment identifié.

([11]) Les exigences minimales applicables aux systèmes d'information et de communication qui traitent des ICUE au niveau RESTREINT UE/EU RESTRICTED sont définies à l'annexe III, appendice E.

([12]) Décision (UE, Euratom) 2019/1962 de la Commission du 17 octobre 2019 fixant les modalités d'application relatives au traitement des informations RESTREINT UE/EU RESTRICTED (JO L 311 du 2.12.2019, p. 21).

([13]) Décision (UE, Euratom) 2019/1961 de la Commission du 17 octobre 2019 fixant les modalités d'application relatives au traitement des informations CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET (JO L 311 du 2.12.2019, p. 1).

4. Pour le transport par porteur d'informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET effectué par le personnel du bénéficiaire d'un État membre de l'Union européenne à un autre, les règles complémentaires suivantes s'appliquent:

a) le porteur est responsable de la sécurité du matériel classifié transporté jusqu'à la remise de celui-ci au destinataire;

b) en cas d'infraction à la sécurité, l'ANS ou l'ASD de l'expéditeur peut demander que les autorités du pays dans lequel l'infraction a eu lieu mènent une enquête, fassent état de leurs constatations et engagent une action en justice ou autre s'il y a lieu;

c) le porteur a été informé de toutes les obligations en matière de sûreté à respecter pendant le transport et a signé une déclaration qui l'atteste;

d) les instructions destinées au porteur sont jointes au certificat de courrier;

e) le porteur a reçu une description de l'envoi et un itinéraire;

f) les documents sont renvoyés à l'ANS ou l'ASD de délivrance après l'achèvement du (des) déplacement(s) ou sont tenus à disposition par le destinataire à des fins de contrôle;

g) si les autorités douanières, les services de l'immigration ou la police des frontières demandent à examiner et à contrôler l'envoi, il leur est permis de l'ouvrir et d'en observer des parties suffisantes afin d'établir qu'il ne contient rien d'autre que le matériel qui est déclaré;

h) les autorités douanières doivent être instamment priées de respecter l'autorité officielle des documents d'expédition et des documents d'autorisation transportés par le porteur.

Si un envoi est ouvert par les autorités douanières, l'ouverture doit être effectuée hors de la vue des personnes non autorisées et, dans la mesure du possible, en présence du porteur. Le porteur demande que l'envoi soit remballé et prie les autorités qui effectuent le contrôle de refermer l'envoi et de confirmer par écrit que celui-ci a été ouvert par elles.

5. Le transport par porteur d'informations classifiées RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET effectué par le personnel du bénéficiaire à destination d'un pays tiers ou d'une organisation internationale sont soumis aux dispositions de l'accord sur la sécurité des informations ou de l'arrangement administratif conclu entre, respectivement, l'Union européenne ou la Commission et ce pays tiers ou cette organisation internationale.

CHAPITRE 6

PLANIFICATION DE LA CONTINUITÉ DES ACTIVITÉS

Article 16

Plans d'urgence et mesures de retour aux conditions opérationnelles

L'autorité octroyant la subvention veille à ce que la convention de subvention classifiée fasse obligation aux bénéficiaires d'établir des plans d'urgence («PU») pour protéger les ICUE traitées dans le contexte de l'exécution de la convention de subvention classifiée dans des situations d'urgence et de mettre en place des mesures de prévention et de retour aux conditions opérationnelles dans le contexte d'une planification de la continuité des activités afin de limiter l'impact des incidents se rapportant au traitement et au stockage des ICUE. Les bénéficiaires confirment à l'autorité octroyant la subvention que leurs plans d'urgence sont en place.

Article 17

Entrée en vigueur

La présente décision entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Fait à Bruxelles, le 10 février 2021.

Par la Commission,
au nom de la présidente,
Johannes HAHN
Membre de la Commission

ANNEXE I

INFORMATIONS STANDARD DANS L'APPEL À PROPOSITIONS

(à adapter en fonction du type d'appel utilisé)

Sécurité

Les projets mettant en jeu des informations classifiées de l'Union européenne doivent faire l'objet de contrôles de sécurité avant que le financement soit autorisé et doivent respecter des règles de sécurité spécifiques [détaillées dans une annexe de sécurité (AS) accompagnant la convention de subvention].

Ces règles [régies par la décision (UE, Euratom) 2015/444 de la Commission ([1]) et/ou des règles nationales] comportent notamment les dispositions suivantes:

— les projets mettant en jeu des informations classifiées SECRET UE/EU SECRET (ou équivalent) **NE** peuvent **PAS** bénéficier d'un financement,

— les informations classifiées doivent être marquées conformément aux instructions de sécurité applicables de l'AS,

— en ce qui concerne les informations d'un niveau de classification CONFIDENTIEL UE/EU CONFIDENTIAL ou supérieur (ainsi que RESTREINT UE/EU RESTRICTED si les règles nationales l'exigent), les conditions suivantes doivent être respectées:

  — ces informations doivent être produites uniquement dans un établissement disposant d'une habilitation de sécurité octroyée par l'autorité nationale de sécurité compétente (ANS), conformément aux règles nationales, et l'accès à ces données ne peut avoir lieu que dans un tel établissement,

  — ces informations doivent être traitées uniquement dans une zone sécurisée agréée par l'ANS compétente,

  — l'accès à ces informations et le traitement de celles-ci sont réservés à des personnes disposant d'une habilitation de sécurité du personnel (HSP) et d'un besoin d'en connaître,

— à l'expiration de la convention de subvention, les informations classifiées doivent être restituées ou continuer à être protégées conformément aux règles applicables,

— les tâches mettant en jeu des informations classifiées de l'Union européenne (ICUE) ne peuvent être sous-traitées qu'avec l'approbation écrite préalable de l'autorité octroyant la subvention et uniquement avec des entités établies dans un État membre de l'Union européenne ou dans un pays tiers ayant conclu un accord sur la sécurité des informations avec l'Union européenne (ou un arrangement administratif avec la Commission),

— la divulgation d'ICUE à des tiers est soumise à l'approbation écrite préalable de l'autorité octroyant la subvention.

Il est à noter que, selon le type d'activité, l'habilitation de sécurité de l'établissement peut être demandée avant la signature de la convention de subvention. L'autorité octroyant la subvention évaluera au cas par cas la nécessité de disposer d'habilitations et fixera la date à laquelle elles doivent être fournies durant la rédaction de la convention de subvention. Il est à noter que les conventions de subvention ne pourront **en aucun cas** être signées tant qu'au moins un des bénéficiaires du consortium ne dispose pas d'une habilitation de sécurité d'établissement.

Des recommandations supplémentaires en matière de sécurité peuvent être ajoutées à la convention de subvention sous la forme d'éléments livrables relatifs à la sécurité (*par exemple, la création d'un groupe consultatif sur la sécurité. la limitation du niveau de détail, l'utilisation d'un scénario fictif, l'exclusion de l'utilisation d'informations classifiées, etc.*).

Les bénéficiaires doivent veiller à ce que leurs projets ne soient pas soumis à des exigences de sécurité imposées au niveau national ou du pays tiers qui pourraient avoir des répercussions sur l'exécution de la convention de subvention ou remettre en question l'attribution de la subvention (*par exemple, des limitations technologiques, des classifications de sécurité nationales, etc.*). L'autorité octroyant la subvention doit être immédiatement informée de tout problème de sécurité potentiel.

[OPTION supplémentaire pour les accords-cadres de partenariat: En ce qui concerne les accords-cadres de partenariat, les candidatures relatives aux accords-cadres de partenariat et aux conventions de subvention doivent faire l'objet de contrôles de sécurité.]

([1]) Voir la décision (UE, Euratom) 2015/444 de la Commission du 13 mars 2015 concernant les règles de sécurité aux fins de la protection des informations classifiées de l'Union européenne (JO L 72 du 17.3.2015, p. 53).

ANNEXE II

CLAUSES STANDARD DE LA CONVENTION DE SUBVENTION

(à adapter en fonction du type de convention de subvention utilisé)

13.2 Sécurité — Informations classifiées

Les parties doivent traiter les informations classifiées (UE ou nationales) conformément au droit national ou européen relatif aux informations classifiées applicable [notamment la décision (UE, Euratom) 2015/444 de la Commission ([1]) et ses modalités d'application].

Les règles de sécurité spécifiques (le cas échéant) sont énoncées à l'annexe 5.

ANNEXE 5

Sécurité — Informations classifiées de l'Union européenne

[OPTION en cas d'actions liées à des informations classifiées de l'Union européenne (standard): Si l'action implique l'utilisation ou la production d'informations classifiées de l'Union européenne, ces informations doivent être traitées conformément à l'annexe de sécurité (-AS) et à son guide de la classification de sécurité (GCS), comme indiqué à l'annexe 1, et à la décision (UE, Euratom) 2015/444 et à ses modalités d'application, jusqu'à ce qu'elles soient déclassifiées.

Les éléments livrables qui contiennent des informations classifiées de l'Union européenne doivent être présentés conformément à des procédures spéciales convenues avec l'autorité octroyant la subvention.

Les tâches mettant en jeu des informations classifiées de l'Union européenne ne peuvent être sous-traitées qu'avec l'approbation écrite préalable de l'autorité octroyant la subvention et seules les entités établies dans un État membre de l'Union européenne ou dans un pays tiers ayant conclu un accord sur la sécurité des informations avec l'Union européenne (ou un arrangement administratif avec la Commission).

Les informations classifiées de l'Union européenne ne peuvent être divulguées à des tiers (y compris à des participants à l'exécution de l'action) sans l'approbation préalable expresse et écrite de l'autorité octroyant la subvention.]

([1]) Décision (UE, Euratom) 2015/444 de la Commission du 13 mars 2015 concernant les règles de sécurité aux fins de la protection des informations classifiées de l'Union européenne (JO L 72 du 17.3.2015, p. 53).

ANNEXE III

[Annexe IV (du/de la ……)]

ANNEXE DE SÉCURITÉ (AS) [1]

[Modèle]

[1] Le présent modèle d'AS est applicable lorsque la Commission est considérée comme l'autorité d'origine des informations classifiées créées et traitées pour l'exécution de la convention de subvention. Lorsque l'autorité d'origine des informations classifiées créées et traitées pour l'exécution de la convention de subvention n'est pas la Commission, et lorsqu'un cadre de sécurité spécifique est mis en place par l'État membre prenant part à la subvention, d'autres modèles d'AS peuvent être applicables.

Appendice A

EXIGENCES EN MATIÈRE DE SÉCURITÉ

L'autorité octroyant la subvention doit intégrer les exigences de sécurité suivantes dans l'annexe de sécurité (AS). Il se peut que certaines clauses ne soient pas applicables à la convention de subvention. Celles-ci sont indiquées entre crochets.

La liste des clauses n'est pas exhaustive. D'autres clauses peuvent être ajoutées en fonction de la nature de la subvention classifiée.

CONDITIONS GÉNÉRALES [*NB: applicables à toutes les conventions de subvention classifiées*]

1. La présente annexe de sécurité (AS) fait partie intégrante de la convention de subvention classifiée [ou du contrat de sous-traitance] et décrit les exigences de sécurité propres à la convention de subvention. Le non-respect de ces exigences peut constituer un motif suffisant pour résilier la convention de subvention.

2. Les bénéficiaires de la subvention sont soumis à toutes les obligations figurant dans la décision (UE, Euratom) 2015/444 de la Commission ([2]) (ci-après la «décision 2015/444 de la Commission») et dans ses modalités d'application ([3]). Si le bénéficiaire de la subvention rencontre des problèmes dans l'application du cadre juridique concerné dans un État membre, il doit en référer à l'autorité de sécurité de la Commission et à l'autorité nationale de sécurité (ANS) ou à l'autorité de sécurité désignée (ASD).

3. Les informations classifiées produites lors de l'exécution de la convention de subvention doivent être marquées comme étant des informations classifiées de l'Union européenne (ICUE) au niveau de classification de sécurité, tel qu'indiqué dans le guide de la classification de sécurité (GCS) figurant à l'appendice B de la présente annexe. Il n'est permis de s'écarter du niveau de classification de sécurité prévu par le GCS que sur autorisation écrite de l'autorité octroyant la subvention.

4. Les droits relevant de l'autorité d'origine de toute ICUE créée et traitée pour l'exécution de la convention de subvention classifiée sont exercés par la Commission, en tant qu'autorité octroyant la subvention.

5. Sans le consentement écrit de l'autorité octroyant la subvention, le bénéficiaire ou le sous-traitant ne doit pas utiliser d'informations ou de matériel fournis par l'autorité octroyant la subvention ou produits pour le compte de cette dernière à des fins autres que celle prévues par la convention de subvention.

6. Lorsqu'une habilitation de sécurité d'établissement (HSE) est exigée en vue de l'exécution d'une convention de subvention, le bénéficiaire doit demander à l'autorité octroyant la subvention de procéder à la demande d'habilitation de sécurité d'établissement.

7. Le bénéficiaire doit enquêter sur toute infraction à la sécurité relative aux ICUE et en référer à l'autorité octroyant la subvention dès que possible. Le bénéficiaire ou le sous-traitant doit immédiatement rendre compte à son ANS ou à son ASD et, lorsque les dispositions législatives et réglementaires nationales l'autorisent, à l'autorité de sécurité de la Commission, de tous les cas dans lesquels il est avéré ou il existe des motifs de soupçonner que des ICUE fournies ou produites en vertu de la convention de subvention ont été perdues ou divulguées à des personnes non autorisées.

([2]) Décision (UE, Euratom) 2015/444 de la Commission du 13 mars 2015 concernant les règles de sécurité aux fins de la protection des informations classifiées de l'Union européenne (JO L 72 du 17.3.2015, p. 53).

([3]) L'autorité octroyant la subvention insérera les références une fois que ces modalités d'application auront été adoptées.

8. Après la fin de la convention de subvention, le bénéficiaire ou le sous-traitant doit restituer à l'autorité octroyant la subvention, dans les meilleurs délais, toute ICUE qu'il détient. Dans la mesure du possible, le bénéficiaire ou le sous-traitant doit détruire les ICUE au lieu de les restituer. Il convient à cet égard de procéder conformément aux dispositions législatives et réglementaires nationales du pays dans lequel le bénéficiaire est établi, avec l'accord préalable de l'autorité de sécurité de la Commission et conformément aux instructions de celle-ci. Les ICUE doivent être détruites de manière à ne pas pouvoir être reconstituées, que ce soit entièrement ou partiellement.

9. Lorsque le bénéficiaire ou le sous-traitant est autorisé à conserver des ICUE après la résiliation ou le terme de la convention de subvention, les ICUE doivent continuer à être protégées conformément à la décision 2015/444 de la Commission, ainsi qu'à ses modalités d'application ([4]).

10. Toute gestion, tout traitement et toute transmission électroniques d'ICUE doivent être conformes aux dispositions des chapitres 5 et 6 de la décision 2015/444 de la Commission. Parmi celles-ci figure notamment l'exigence que les systèmes d'information et de communication détenus par le bénéficiaire et utilisés pour traiter des ICUE aux fins de la convention de subvention (ci-après dénommés «SIC du bénéficiaire») sont soumis à agrément ([5]), que toute transmission d'ICUE par voie électronique doit être protégée par des produits cryptographiques approuvés conformément à l'article 36, paragraphe 4, de la décision 2015/444 de la Commission et que des mesures de sécurité TEMPEST doivent être mises en œuvre conformément à l'article 36, paragraphe 6, de ladite décision.

11. Le bénéficiaire ou le sous-traitant doit disposer de plans d'urgence (PU) pour protéger toute ICUE traitée dans le cadre de l'exécution de la convention de subvention classifiée dans les situations d'urgence et mettre en place des mesures de prévention et de retour aux conditions opérationnelles afin de limiter l'impact des incidents se rapportant au traitement et au stockage des ICUE. Le bénéficiaire ou le sous-traitant doivent communiquer son plan d'urgence à l'autorité octroyant la subvention.

CONVENTION DE SUBVENTION NÉCESSITANT L'ACCÈS À DES INFORMATIONS CLASSIFIÉES RESTREINT UE/EU RESTRICTED

12. En principe, la convention de subvention ([6]) n'impose pas d'habilitation de sécurité du personnel (HSP). Toutefois, les informations ou le matériel classifiés RESTREINT UE/EU RESTRICTED ne doivent être accessibles qu'au personnel du bénéficiaire qui en a besoin pour exécuter la convention de subvention (principe du «besoin d'en connaître»), qui a été informé par le responsable de la sécurité du bénéficiaire de ses responsabilités et des conséquences de toute infraction à la sécurité ou compromission de ces informations et qui a reconnu par écrit les conséquences d'un défaut de protection des ICUE.

13. Sauf dans le cas où l'autorité octroyant la subvention a donné son consentement par écrit, le bénéficiaire ou le sous-traitant ne doivent pas donner accès aux informations ou au matériel classifiés RESTREINT UE/EU RESTRICTED à des entités ou personnes autres que leur personnel ayant besoin d'en connaître.

14. Le bénéficiaire ou le sous-traitant doit conserver les marquages de classification de sécurité des informations classifiées produites par la convention de subvention ou fournies lors de son exécution et ne doit pas déclassifier d'informations sans l'autorisation écrite de l'autorité octroyant la subvention.

15. Les informations ou le matériel classifiés RESTREINT UE/EU RESTRICTED doivent être stockés dans un meuble de bureau fermé à clé lorsqu'ils ne sont pas utilisés. S'ils sont déplacés, les documents doivent être transportés dans une enveloppe opaque. Le porteur ne doit pas s'en séparer, et ils ne doivent pas être déballés pendant le transport.

([4]) L'autorité octroyant la subvention insérera les références une fois que ces modalités d'application auront été adoptées.

([5]) La partie qui sollicite l'agrément devra fournir à l'autorité octroyant la subvention une déclaration de conformité, par l'intermédiaire de l'autorité de sécurité de la Commission et en coordination avec l'autorité nationale d'homologation de sécurité (AHS) compétente.

([6]) Lorsque les bénéficiaires sont issus d'États membres exigeant une HSP ou une HSE aux fins de subventions classifiées RESTREINT UE/EU RESTRICTED, l'autorité octroyant la subvention énumère dans l'AS les exigences en matière d'HSP et d'HSE concernées pour les bénéficiaires en question.

16. Le bénéficiaire ou le sous-traitant peut transmettre des documents classifiés RESTREINT UE/EU RESTRICTED à l'autorité octroyant la subvention en recourant à des sociétés de courrier commercial, aux services postaux, au transport par porteur ou à des moyens électroniques. À cette fin, le bénéficiaire ou le sous-traitant doit se conformer aux instructions de sécurité du programme (ou du projet) (ISP) émises par la Commission et/ou aux modalités d'application de la Commission en matière de sécurité industrielle en ce qui concerne les subventions classifiées ([7]).

17. Lorsqu'ils ne sont plus nécessaires, les documents classifiés RESTREINT UE/EU RESTRICTED doivent être détruits de manière à ne pas pouvoir être reconstitués, que ce soit entièrement ou partiellement.

18. L'habilitation de sécurité du SIC du bénéficiaire qui traite des ICUE au niveau RESTREINT UE/EU RESTRICTED et toute interconnexion y afférente peuvent être déléguées au responsable de la sécurité du bénéficiaire si les dispositions législatives et réglementaires nationales l'autorisent. Lorsque l'habilitation est ainsi déléguée, les ANS, ASD ou les autorités d'homologation de sécurité (AHS) demeurent responsables de la protection de toute information RESTREINT UE/EU RESTRICTED traitée par le bénéficiaire et conservent le droit de contrôler les mesures de sécurité prises par le bénéficiaire. En outre, le bénéficiaire fournit à l'autorité octroyant la subvention et, lorsque les dispositions législatives et réglementaires nationales l'exigent, à l'AHS nationale compétente, une déclaration de conformité attestant que le SIC du bénéficiaire et les interconnexions s'y rapportant ont été agréés pour traiter des ICUE au niveau RESTREINT UE/EU RESTRICTED.

TRAITEMENT DES INFORMATIONS CLASSIFIÉES RESTREINT UE/EU RESTRICTED DANS LES SYSTÈMES D'INFORMATION ET DE COMMUNICATION (SIC)

19. Les exigences minimales applicables aux SIC qui traitent des informations classifiées au niveau RESTREINT UE/EU RESTRICTED sont définies à l'appendice E de la présente annexe de sécurité.

CONDITIONS DANS LESQUELLES LE BÉNÉFICIAIRE PEUT RECOURIR À LA SOUS-TRAITANCE

20. Le bénéficiaire doit obtenir l'autorisation de l'autorité octroyant la subvention avant de pouvoir sous-traiter une partie d'une convention de subvention classifiée.

21. Aucun contrat de sous-traitance ne peut être attribué à une entité immatriculée dans un pays tiers ou à une entité appartenant à une organisation internationale, si ce pays tiers ou cette organisation internationale n'a pas conclu un accord sur la sécurité des informations avec l'Union ou un arrangement administratif avec la Commission.

22. Si le bénéficiaire recourt à la sous-traitance, les dispositions de la convention de subvention en matière de sécurité s'appliquent mutatis mutandis au(x) sous-traitant(s) et à son (leur) personnel. En pareil cas, il incombe au bénéficiaire de veiller à ce que tous les sous-traitants appliquent ces principes à leurs propres arrangements de sous-traitance. Pour veiller à une supervision appropriée en matière de sécurité, les ANS et/ou les ASD du bénéficiaire et du sous-traitant sont informées par l'autorité de sécurité de la Commission de l'attribution de tous les contrats de sous-traitance classifiés correspondants aux niveaux CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET. Le cas échéant, les ANS et/ou les ASD du bénéficiaire et du sous-traitant reçoivent un exemplaire des dispositions de sécurité propres au contrat de sous-traitance. La liste des ANS et/ou des ASD qui exigent une notification concernant les dispositions de sécurité des conventions de subvention classifiées RESTREINT UE/EU RESTRICTED figure à l'annexe des modalités d'application de la Commission en matière de sécurité industrielle en ce qui concerne les conventions de subvention classifiées ([8]).

23. Le bénéficiaire ne peut divulguer aucune ICUE à un sous-traitant sans l'approbation écrite préalable de l'autorité octroyant la subvention. Si des ICUE doivent être transmises aux sous-traitants de manière fréquente ou systématique, l'autorité octroyant la subvention peut donner son approbation pour une durée déterminée (par exemple 12 mois) ou pour la durée du contrat de sous-traitance.

([7]) L'autorité octroyant la subvention insérera les références une fois que ces modalités d'application auront été adoptées.
([8]) L'autorité octroyant la subvention insérera les références une fois que ces modalités d'application auront été adoptées.

VISITES

Si la procédure de demande de visite (DDV) standard doit être appliquée aux visites mettant en jeu des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET, l'autorité octroyant la subvention doit intégrer les points 24, 25 et 26 et supprimer le point 27. Si des visites impliquant un accès à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET sont organisées directement par l'établissement d'envoi et l'établissement d'accueil, l'autorité octroyant la subvention doit supprimer les points 25 et 26 et insérer uniquement le point 27.

24. Les visites impliquant un accès ou un accès potentiel à des informations classifiées RESTREINT UE/EU RESTRICTED sont organisées directement par l'établissement d'envoi et l'établissement d'accueil sans qu'il soit nécessaire de suivre la procédure prévue aux points 25 à 27 ci-dessous.

[25. Les visites impliquant un accès ou un accès potentiel à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET sont soumises à la procédure suivante:

a) le responsable de la sécurité de l'établissement qui envoie le visiteur remplit toutes les parties pertinentes du formulaire de DDV (appendice C) et soumet la demande à l'ANS ou à l'ASD de l'établissement;

b) l'ANS ou l'ASD de l'établissement d'envoi doit confirmer l'HSP du visiteur avant de soumettre la DDV à l'ANS ou à l'ASD de l'établissement d'accueil (ou à l'autorité de sécurité de la Commission si la visite a lieu dans les locaux de l'autorité octroyant la subvention);

c) le responsable de la sécurité de l'établissement d'envoi obtient ensuite de son ANS ou de son ASD la réponse de l'ANS ou de l'ASD de l'établissement d'accueil (ou de l'autorité de sécurité de la Commission) signifiant l'approbation ou le rejet de la DDV;

d) une DDV est réputée approuvée si aucune objection n'est formulée dans les cinq jours ouvrables qui précèdent la date de la visite.]

[26. Avant que soit donné au(x) visiteur(s) l'accès à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET, l'établissement d'accueil doit avoir reçu l'autorisation de son ANS ou de son ASD.]

[27. Les visites impliquant un accès ou un accès potentiel à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET sont organisées directement par l'établissement d'envoi et l'établissement d'accueil (un exemple de formulaire pouvant être utilisé à cette fin figure à l'appendice C).]

28. Les visiteurs doivent décliner leur identité à leur arrivée dans l'établissement d'accueil en présentant une carte d'identité ou un passeport en cours de validité.

29. L'établissement qui accueille la visite doit veiller à tenir un registre de tous les visiteurs, comportant leur nom, l'organisation qu'ils représentent, la date d'expiration de l'HSP (le cas échéant), la date de la visite et le nom de la ou des personnes auxquelles il est rendu visite. Sans préjudice des règles européennes en matière de protection des données, ce registre doit être conservé pendant une période d'au moins cinq ans ou pendant la durée prévue par les règles et réglementations nationales, selon le cas.

VISITES D'ÉVALUATION

30. L'autorité de sécurité de la Commission peut, en coopération avec les ANS ou les ASD compétentes, effectuer des visites dans les établissements des bénéficiaires ou sous-traitants afin de vérifier que les exigences de sécurité applicables au traitement des ICUE sont respectées.

GUIDE DE LA CLASSIFICATION DE SÉCURITÉ

31. Le guide de la classification de sécurité (GCS) de la convention de subvention contient la liste de tous les éléments de la convention de subvention qui sont classifiés ou à classifier au cours de l'exécution de ladite convention, les règles prévues à cet effet et les niveaux de classification de sécurité applicables. Le GCS fait partie intégrante de la convention de subvention et figure à l'appendice B de la présente annexe.

Appendice B

GUIDE DE LA CLASSIFICATION DE SÉCURITÉ

[texte spécifique à adapter en fonction de l'objet de la convention de subvention]

Appendice C

DEMANDE DE VISITE (MODÈLE)

INSTRUCTIONS DÉTAILLÉES POUR REMPLIR LA DEMANDE DE VISITE

(La demande doit être présentée en anglais uniquement)

HEADING	Cochez les cases correspondant au type de visite et au type d'informations et indiquez le nombre de sites à visiter et le nombre de visiteurs.
4. **ADMINISTRATIVE DATA**	À remplir par l'ANS/ASD à l'origine de la demande.
5. **REQUESTING ORGANISATION OR INDUSTRIAL FACILITY**	Indiquez la dénomination complète et l'adresse postale. Indiquez la ville, l'État et le code postal comme il convient.
6. **ORGANISATION OR INDUSTRIAL FACILITY TO BE VISITED**	Indiquez la dénomination complète et l'adresse postale. Indiquez la ville, l'État, le code postal, les numéros de télex ou de télécopieur (le cas échéant), le numéro de téléphone et l'adresse électronique. Indiquez le nom, les numéros de téléphone/télécopieur et l'adresse électronique de votre interlocuteur principal ou de la personne avec laquelle vous avez pris rendez-vous pour la visite. Remarques: 1) Il est important d'indiquer le code postal correct car une entreprise peut disposer de différents établissements. 2) En cas de demande manuelle, l'annexe 1 peut être utilisée lorsque deux installations ou plus doivent faire l'objet d'une visite se rapportant au même objet. En cas d'utilisation d'une annexe, le point 3 doit indiquer: «SEE ANNEX 1, NUMBER OF FAC.:..» (mentionnez le nombre d'établissements).
7. **DATES OF VISIT**	Indiquez la date effective ou la période (de date à date) de la visite dans le format «jour - mois - année». Indiquez, entre parenthèses, une autre date ou période possible, le cas échéant.
8. **TYPE OF INITIATIVE**	Précisez si la visite est une initiative de l'organisation ou de l'établissement à l'origine de la demande ou s'il s'agit d'une invitation émanant de l'établissement à visiter.
9. **THE VISIT RELATES TO:**	Indiquez l'intitulé complet du projet, du contrat ou de l'appel d'offres en utilisant uniquement des abréviations courantes.
10. **SUBJECT TO BE DISCUSSED/ JUSTIFICATION**	Exposez succinctement le(s)motif(s) de la visite. N'utilisez pas d'abréviations sans explication. Remarques: Dans le cas de visites récurrentes, ce point doit porter la mention «Recurring visits» en tant que premiers termes dans l'élément de données (par exemple, «Recurring visits to discuss_____»).
11. **ANTICIPATED LEVEL OF CLASSIFIED INFORMATION TO BE INVOLVED**	Indiquez SECRET UE/EU SECRET (S-UE/EU-S) ou CONFIDENTIEL UE/EU CONFIDENTIAL (C-UE/EU-C), selon le cas.

12. **PARTICULARS OF VISITOR(S)**	Remarque: lorsque plus de deux visiteurs prennent part à la visite, il convient d'utiliser l'annexe 2.
13. **THE SECURITY OFFICER OF THE REQUESTING ENTITY**	Ce point doit mentionner le nom, les numéros de téléphone et de télécopieur et l'adresse électronique du responsable de la sécurité de l'établissement à l'origine de la demande.
14. **CERTIFICATION OF SECURITY CLEARANCE**	Ce champ doit être rempli par l'autorité de certification. Notes à l'attention de l'autorité de certification: a) Indiquez le nom, l'adresse, les numéros de téléphone et de télécopieur et l'adresse électronique (peut être préimprimé). b) Ce point doit porter une signature et un cachet (s'il y a lieu).
15. **REQUESTING SECURITY AUTHORITY**	Ce champ doit être rempli par l'ANS/ASD. Note à l'attention de l'ANS/ASD: a) Indiquez le nom, l'adresse, les numéros de téléphone et de télécopieur et l'adresse électronique (peut être préimprimé). b) Ce point doit porter une signature et un cachet (s'il y a lieu).

Tous les champs doivent être remplis et le formulaire doit être transmis via les canaux intergouvernementaux ([9]).

DEMANDE DE VISITE

(MODÈLE)

TO: _____

1. **TYPE OF VISIT REQUEST**	2. **TYPE OF INFORMATION**	3. **SUMMARY**
☐ Single ☐ Recurring ☐ Emergency ☐ Amendment ☐ Dates ☐ Visitors ☐ Facility For an amendment, insert the NSA/DSA original RFV Reference No_____	☐ C-UE/EU-C ☐ S-UE/EU-S	No of sites: _____ No of visitors: _____

4. **ADMINISTRATIVE DATA:**	
Requester: To:	NSA/DSA RFV Reference No_____ Date *(dd/mm/yyyy)*: _____/_____/_____

([9]) S'il a été convenu que des visites impliquant un accès ou un accès potentiel à des ICUE au niveau CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET pouvaient être organisées directement, le formulaire rempli peut être soumis directement au responsable de la sécurité de l'établissement à visiter.

5. **REQUESTING ORGANISATION OR INDUSTRIAL FACILITY:**

NAME:

POSTAL ADDRESS:

E-MAIL ADDRESS:

FAX NO: TELEPHONE NO:

6. **ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED *(Annex 1 to be completed)***

7. **DATE OF VISIT *(dd/mm/yyyy)*: FROM _____/_____/_____ TO _____/_____/_____**

8. **TYPE OF INITIATIVE:**

☐ Initiated by requesting organisation or facility

☐ By invitation of the facility to be visited

9. **THE VISIT RELATES TO CONTRACT:**

10. **SUBJECT TO BE DISCUSSED/REASONS/PURPOSE (Include details of host entity and any other relevant information. Abbreviations should be avoided):**

11. **ANTICIPATED HIGHEST CLASSIFICATION LEVEL OF INFORMATION/MATERIAL OR SITE ACCESS TO BE INVOLVED:**

12. **PARTICULARS OF VISITOR(S) *(Annex 2 to be completed)***

13. **THE SECURITY OFFICER OF THE REQUESTING ORGANISATION OR INDUSTRIAL FACILITY:**

NAME:

TELEPHONE NO:

E-MAIL ADDRESS:

SIGNATURE:

14. CERTIFICATION OF SECURITY CLEARANCE LEVEL:

NAME:

ADDRESS:

TELEPHONE NO:

E-MAIL ADDRESS:

SIGNATURE:

STAMP

DATE *(dd/mm/yyyy)*:
_____/_____/_____

15. **REQUESTING NATIONAL SECURITY AUTHORITY/DESIGNATED SECURITY AUTHORITY:**

NAME:

ADDRESS:

TELEPHONE NO:

E-MAIL ADDRESS:

STAMP

SIGNATURE:

DATE *(dd/mm/yyyy)*:
_____/_____/_____

16. **REMARKS *(Mandatory justification required in the case of an emergency visit)*:**

<Espace réservé pour la référence à la législation applicable en matière de données à caractère personnel et le lien vers les informations obligatoires pour la personne concernée, par exemple la manière dont est mis en œuvre l'article 13 du règlement général sur la protection des données ([10]).>

([10]) Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).

ANNEXE 1 du FORMULAIRE DE DDV

ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED
1. NAME: ADDRESS: TELEPHONE NO: FAX NO: NAME OF POINT OF CONTACT: E-MAIL: TELEPHONE NO: NAME OF SECURITY OFFICER OR SECONDARY POINT OF CONTACT: E-MAIL: TELEPHONE NO:
2. NAME: ADDRESS: TELEPHONE NO: FAX NO: NAME OF POINT OF CONTACT: E-MAIL: TELEPHONE NO: NAME OF SECURITY OFFICER OR SECONDARY POINT OF CONTACT: E-MAIL: TELEPHONE NO: ***(Continue as required)***

<Espace réservé pour la référence à la législation applicable en matière de données à caractère personnel et le lien vers les informations obligatoires pour la personne concernée, par exemple la manière dont est mis en œuvre l'article 13 du règlement général sur la protection des données ([11]).>

([11]) Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).

ANNEXE 2 du FORMULAIRE DE DDV

PARTICULARS OF VISITOR(S)
1. SURNAME: FIRST NAMES (as per passport): DATE OF BIRTH *(dd/mm/yyyy)*: ____/____/____ PLACE OF BIRTH: NATIONALITY: SECURITY CLEARANCE LEVEL: PP/ID NUMBER: POSITION: COMPANY/ORGANISATION:
2. SURNAME: FIRST NAMES (as per passport): DATE OF BIRTH *(dd/mm/yyyy)*: ____/____/____ PLACE OF BIRTH: NATIONALITY: SECURITY CLEARANCE LEVEL: PP/ID NUMBER: POSITION: COMPANY/ORGANISATION: ***(Continue as required)***

<Espace réservé pour la référence à la législation applicable en matière de données à caractère personnel et le lien vers les informations obligatoires pour la personne concernée, par exemple la manière dont est mis en œuvre l'article 13 du règlement général sur la protection des données ([12]).>

([12]) Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).

Appendice D

FICHE D'INFORMATION HABILITATION DE SÉCURITÉ D'ÉTABLISSEMENT (FIHSE) (MODÈLE)

1. **INTRODUCTION**

1.1. Ci-joint figure un spécimen de fiche d'information habilitation de sécurité d'établissement (FIHSE) pour l'échange rapide d'informations entre l'autorité nationale de sécurité (ANS) ou l'autorité de sécurité désignée (ASD), les autres autorités nationales compétentes en matière de sécurité et l'autorité de sécurité de la Commission (agissant au nom des autorités octroyant la subvention) en ce qui concerne l'habilitation de sécurité d'établissement (HSE) d'un établissement intervenant dans les candidatures relatives à des conventions de subventions classifiées ou à des contrats de sous-traitance classifiés et à leur exécution.

1.2. La FIHSE n'est valable que si elle porte le cachet de l'ANS, de l'ASD concernée ou de toute autre autorité compétente.

1.3. La FIHSE comprend une section «demande» et une section «réponse»; elle peut être utilisée aux fins indiquées ci-dessus ou à toute autre fin pour laquelle le statut de HSE d'un établissement donné est exigé. Le motif de la requête doit être indiqué par l'ANS ou l'ASD à l'origine de la demande dans le champ 7 de la section «demande».

1.4. Les données contenues dans la FIHSE ne sont normalement pas classifiées; en conséquence, lorsque la FIHSE passe d'un intervenant à l'autre (ANS/ASD/Commission), il est préférable que la transmission se fasse par voie électronique.

1.5. Les ANS/ASD doivent tout mettre en œuvre pour répondre à une demande FIHSE dans un délai de dix jours ouvrables.

1.6. En cas de transfert d'informations classifiées ou d'attribution d'une convention de subvention ou d'un contrat de sous-traitance classifiés en rapport avec cette assurance, l'ANS ou l'ASD émettrice doit en être informée.

Procédures et instructions pour utiliser la fiche d'information habilitation de sécurité d'établissement (FIHSE)

Ces instructions détaillées sont destinées à l'ANS, à l'ASD ou à l'autorité octroyant la subvention ainsi qu'à l'autorité de sécurité de la Commission qui complètent la FIHSE concernée. La demande doit, de préférence, être dactylographiée en lettres capitales.

EN-TÊTE	Le demandeur insère la dénomination complète de l'ANS/ASD et le nom du pays.
1. **TYPE DE DEMANDE**	L'autorité octroyant la subvention à l'origine de la demande coche la case correspondant au type de demande FIHSE concerné. Indiquez le niveau d'habilitation de sécurité demandé. Il convient de recourir aux abréviations suivantes: SECRET UE/EU SECRET = S-UE/EU-S CONFIDENTIEL UE/EU CONFIDENTIAL = C-UE/EU-C SIC = systèmes d'information et de communication pour le traitement des informations classifiées
2. **RENSEIGNEMENTS SUR LE DEMANDEUR**	Les champs 1 à 6 ne nécessitent pas d'explications. Dans le champ 4, il convient d'utiliser le code pays standard à deux lettres. Le champ 5 est facultatif.
3. **MOTIF DE LA DEMANDE**	Mentionnez le motif précis de la demande, fournissez des indicateurs de projet, et indiquez le numéro de l'appel à propositions ou de la subvention. Veuillez préciser les besoins en matière de capacité de stockage, le niveau de classification des SIC, etc. Mentionnez toute date limite/d'expiration/d'attribution susceptible d'avoir une incidence sur l'achèvement d'une HSE.

4. **ANS/ASD À L'ORIGINE DE LA DEMANDE**	Indiquez le nom du demandeur effectif (pour le compte de l'ANS/ASD) et la date de la demande en format numérique (jj/mm/aaaa).
5. **SECTION «RÉPONSE»**	Champs 1-5: sélectionnez les champs qui conviennent. Champ 2: si une HSE est en cours, il est recommandé de fournir au demandeur une indication du délai de traitement requis (s'il est connu). Champ 6: a) Bien que la validation varie d'un pays ou même d'un établissement à l'autre, il est recommandé d'indiquer la date d'expiration de l'HSE. b) Lorsque la date d'expiration de l'assurance HSE est indéterminée, ce champ peut être biffé. c) Conformément aux règles et réglementations nationales respectives, le demandeur ou le bénéficiaire ou le sous-traitant est responsable de la demande de renouvellement de l'HSE.
6. **REMARQUES**	Peut être utilisé pour fournir des informations complémentaires concernant l'HSE, l'établissement ou les éléments qui précèdent.
7. **ANS/ASD ÉMETTRICE**	Indiquez le nom de l'autorité qui délivre (pour le compte de l'ANS/ASD) et la date de la réponse en format numérique (jj/mm/aaaa).

FICHE D'INFORMATION HABILITATION DE SÉCURITÉ D'ÉTABLISSEMENT (FIHSE) (MODÈLE)

Tous les champs doivent être remplis et le formulaire doit être transmis via les canaux intergouvernementaux ou les canaux entre administrations publiques et organisations internationales.

DEMANDE D'ASSURANCE D'HABILITATION DE SÉCURITÉ D'ÉTABLISSEMENT

À: _____

(nom du pays de l'ANS/ASD)

Veuillez remplir les cases de réponse comme il convient:

[ ] Fournir une assurance HSE au niveau: [ ] S-UE/EU-S [ ] C-UE/EU-C

pour l'établissement ci-dessous

[ ] Y compris sauvegarde de matériel/d'informations classifié(es)

[ ] Y compris systèmes d'information et de communication (SIC) pour le traitement d'informations classifiées

[ ] Engager, directement ou sur demande correspondante d'un bénéficiaire ou d'un sous-traitant, la procédure d'obtention d'une HSE jusque et y compris au niveau ....., assortie du niveau ..... . pour la sauvegarde et du niveau ..... pour le SIC, si l'établissement ne dispose pas actuellement de ces niveaux de capacités.

Confirmez l'exactitude des données de l'établissement énumérées ci-dessous et procédez aux corrections/ajouts nécessaires.

1. Dénomination complète de l'établissement:	Corrections/ajouts:
.....	.....
2. Adresse complète de l'établissement:	
.....	.....
3. Adresse postale (si différente de celle indiquée au point 2)	
.....	.....
4. Code postal/ville/pays	
.....	.....
5. Nom du responsable de la sécurité	
.....	
.....	
6. Téléphone/télécopieur/courriel du responsable de la sécurité	
.....	.....

7. La présente demande est motivée comme suit: [fournissez des précisions sur la phase précontractuelle (sélection des propositions), la subvention ou le contrat de sous-traitance, le programme/projet, etc.]

.....

ANS/ASD/Autorité octroyant la subvention à l'origine de la demande: Nom: .....

Date: (jj/mm/aaaa).....

RÉPONSE (dans les dix jours ouvrables)

Il est certifié par la présente que:

1. [ ] l'établissement susmentionné détient une HSE jusque et y compris au niveau [ ] S-UE/EU-S.

   [ ] C-UE/EU-C.

2. l'établissement susmentionné a la capacité de protéger des informations/du matériel classifié(es):

   [ ] oui, niveau: ..... . [ ] non.

3 . l'établissement susmentionné dispose d'un SIC agréé/autorisé:

   [ ] oui, niveau: ..... . [ ] non.

4. [ ] en ce qui concerne la demande susmentionnée, la procédure d'HSE a été engagée. Vous serez informé(e) de la mise en place ou du refus de l'homologation.

5. [ ] l'établissement susmentionné ne détient pas d'HSE.

6. La présente assurance HSE arrive à expiration le: ..... . *(jj/mm/aaaa*), ou à une date indiquée par l'ANS/ASD. En cas d'invalidation anticipée ou de modification des informations qui précèdent, vous serez informé(e).

7. Remarques:
   .....

*ANS/ASD émettrice*Dénomination: ..... *Date: (jj/mm/aaaa)* .....

<Espace réservé pour la référence à la législation applicable en matière de données à caractère personnel et le lien vers les informations obligatoires pour la personne concernée, par exemple la manière dont est mis en œuvre l'article 13 du règlement général sur la protection des données ([13]).>

([13]) Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).

Appendice E

Exigences minimales en matière de protection des ICUE en format électronique au niveau RESTREINT UE/EU RESTRICTED traitées dans le SIC du bénéficiaire

Généralités

1. Il incombe au bénéficiaire de veiller à ce que la protection des informations RESTREINT UE/EU RESTRICTED réponde aux exigences minimales en matière de sécurité définies dans la présente clause de sécurité et à toute autre exigence supplémentaire indiquée par l'autorité octroyant la subvention ou, le cas échéant, par l'autorité nationale de sécurité (ANS) ou l'autorité de sécurité désignée (ASD).

2. Le bénéficiaire est responsable de la mise en œuvre des exigences de sécurité définies dans le présent document.

3. Aux fins du présent document, un système d'information et de communication (SIC) comprend tout matériel servant à traiter, stocker et transmettre des ICUE, y compris les postes de travail, imprimantes, photocopieuses, télécopieurs, serveurs, systèmes de gestion de réseau, contrôleurs de réseau et contrôleurs de communication, ordinateurs portables ou ultraportables, tablettes informatiques, téléphones intelligents et dispositifs de stockage amovibles tels que clés USB, CD, cartes SD, etc.

4. Les équipements spéciaux, comme les produits cryptographiques, doivent être protégés conformément aux procédures d'exploitation de sécurité (SecOp) qui leur sont propres.

5. Le bénéficiaire doit mettre en place une structure chargée de gérer la sécurité des SIC traitant des informations classifiées RESTREINT UE/EU RESTRICTED et désigner un responsable de la sécurité pour l'établissement concerné.

6. Le recours à des solutions informatiques (matériel, logiciels ou services) appartenant, à titre privé, au personnel du bénéficiaire pour le stockage ou le traitement d'informations RESTREINT UE/EU RESTRICTED n'est pas autorisé.

7. L'agrément du SIC du bénéficiaire destiné à traiter des informations classifiées RESTREINT UE/EU RESTRICTED doit être approuvé par l'autorité d'homologation de sécurité (AHS) de l'État membre concerné ou délégué au responsable de la sécurité du bénéficiaire conformément aux dispositions législatives et réglementaires nationales.

8. Seules les informations classifiées RESTREINT UE/EU RESTRICTED qui sont chiffrées au moyen de produits cryptographiques approuvés peuvent être traitées, stockées ou transmises (par liaison filaire ou sans fil) comme toute autre information non classifiée dans le cadre de la convention de subvention. Ces produits cryptographiques doivent être approuvés par l'Union européenne ou par un État membre.

9. Les établissements extérieurs intervenant dans des travaux d'entretien/de réparation doivent être contractuellement tenus de respecter les dispositions applicables en matière de traitement d'informations classifiées RESTREINT UE/EU RESTRICTED, telles qu'elles sont énoncées dans le présent document.

10. À la demande de l'autorité octroyant la subvention ou de l'ANS, de l'ASD ou de l'AHS compétente, le bénéficiaire doit apporter la preuve de la conformité avec la clause de sécurité de la convention de subvention. Si un audit et un contrôle des processus et installations du bénéficiaire sont en outre demandés, aux fins de la conformité avec ces exigences, le bénéficiaire doit autoriser les représentants de l'autorité octroyant la subvention, de l'ANS, de l'ASD et/ou de l'AHS ou de l'autorité de sécurité de l'Union européenne compétente à procéder de tels audits et contrôles.

Sécurité physique

11. Les espaces dans lesquels sont utilisés les SIC pour l'affichage, le stockage, le traitement ou la transmission d'informations classifiées RESTREINT UE/EU RESTRICTED ou les espaces où se trouvent les serveurs, les systèmes de gestion de réseau, les contrôleurs de réseau et les contrôleurs de communication pour ces SIC doivent être configurés en tant que zones séparées et contrôlées, équipées d'un système de contrôle d'accès approprié. L'accès à ces zones séparées et contrôlées doit être limité aux personnes ayant une autorisation spéciale. Sans préjudice du point 8, le matériel décrit au point 3 doit être entreposé dans ces zones séparées et contrôlées.

12. Des mécanismes et/ou des procédures de sécurité doivent être mis en œuvre pour réglementer l'introduction dans des composants du SIC, ou la connexion à ceux-ci, de supports de stockage amovibles (tels que des dispositifs USB, unités de mémoire de masse ou disques compacts réinscriptibles).

Accès au SIC

13. L'accès au SIC d'un bénéficiaire qui traite des ICUE est autorisé selon le principe du strict besoin d'en connaître et sur la base d'une autorisation accordée au personnel.

14. Tous les SIC doivent disposer de listes à jour des utilisateurs autorisés. Tous les utilisateurs doivent être authentifiés au début de chaque session de traitement.

15. Les mots de passe, qui font partie de la plupart des mesures de sécurité pour l'identification et l'authentification, doivent comporter au moins neuf caractères, à savoir des caractères numériques et «spéciaux» (si le système le permet) ainsi que des caractères alphabétiques. Ces mots de passe doivent être changés au moins tous les 180 jours, et doivent l'être dans les plus brefs délais s'ils ont été compromis ou divulgués à une personne non autorisée, ou en cas de présomption d'une telle compromission ou divulgation.

16. Tous les SIC doivent être dotés de contrôles d'accès internes destinés à empêcher tout utilisateur non autorisé d'accéder à des informations classifiées RESTREINT UE/EU RESTRICTED ou de modifier de telles informations, ainsi que de modifier les contrôles du système et les contrôles de sécurité. Les utilisateurs doivent être automatiquement déconnectés du SIC si leur terminal reste inactif pendant un certain temps, ou bien le SIC doit activer un écran de veille protégé par mot de passe après 15 minutes d'inactivité.

17. Chaque utilisateur du SIC se voit attribuer un compte d'utilisateur et un identifiant uniques. Les comptes d'utilisateurs doivent être verrouillés automatiquement après au moins cinq tentatives successives de connexion infructueuses.

18. Tous les utilisateurs du SIC doivent être informés de leurs responsabilités et des procédures à suivre pour protéger les informations classifiées RESTREINT UE/EU RESTRICTED dans le SIC. Les responsabilités et les procédures à suivre doivent faire l'objet d'une documentation et donner lieu à une reconnaissance écrite de la part des utilisateurs.

19. Les procédures d'exploitation de sécurité (SecOp) doivent être à la disposition des utilisateurs et des administrateurs et doivent comporter une description des fonctions de sécurité ainsi que la liste correspondante des tâches, instructions et plans.

Tenue de registres, contrôle et réaction face aux incidents

20. Tout accès au SIC doit être consigné.

21. Les événements suivants doivent être enregistrés:

    a) toute tentative de connexion, qu'elle ait abouti ou échoué;

    b) la déconnexion (y compris après expiration du délai, le cas échéant);

    c) la création, la suppression ou la modification de droits d'accès et de privilèges;

    d) la création, la suppression ou la modification de mots de passe.

22. Pour tous les événements énumérés ci-dessus, les informations minimales suivantes doivent être communiquées:

    a) type d'événement;

    b) identifiant utilisateur;

    c) date et heure;

    d) identifiant du dispositif.

23. Les registres doivent aider le responsable de la sécurité à examiner d'éventuels incidents de sécurité. Ils peuvent également servir à l'appui de toute enquête judiciaire en cas d'incident de sécurité. Tous les enregistrements de sécurité doivent être régulièrement vérifiés aux fins de la détection d'éventuels incidents de sécurité. Les registres doivent être protégés contre toute suppression ou modification non autorisée.

24. Le bénéficiaire doit disposer d'une stratégie de riposte bien en place pour faire face aux incidents de sécurité. Les utilisateurs et les administrateurs doivent recevoir des instructions sur la manière de réagir aux incidents et de signaler ces derniers, et sur la marche à suivre en cas d'urgence.

25. Toute compromission ou compromission présumée d'informations classifiées RESTREINT UE/EU RESTRICTED doit donner lieu à un rapport à l'autorité octroyant la subvention. Ce rapport doit contenir une description des informations en cause et des circonstances de la compromission ou de la compromission présumée. Tous les utilisateurs du SIC doivent être informés de la manière de rapporter au responsable de la sécurité tout incident de sécurité réel ou présumé.

Mise en réseau et interconnexion

26. Lorsque le SIC d'un bénéficiaire qui traite des informations classifiées RESTREINT UE/EU RESTRICTED est interconnecté à un SIC qui n'est pas agréé, cette situation aggrave considérablement la menace tant pour la sécurité du SIC que pour les informations RESTREINT UE/EU RESTRICTED traitées par celui-ci. Sont notamment concernés l'internet et d'autres SIC, publics ou privés, tels que d'autres SIC appartenant au bénéficiaire ou au sous-traitant. En pareil cas, le bénéficiaire doit procéder à une évaluation des risques afin de déterminer les exigences de sécurité supplémentaires à mettre en œuvre dans le cadre du processus d'homologation de sécurité. Le bénéficiaire fournit à l'autorité octroyant la subvention et, lorsque les dispositions législatives et réglementaires nationales l'exigent, à l'AHS compétente, une déclaration de conformité attestant que le SIC du bénéficiaire et les interconnexions s'y rapportant ont été agréés pour traiter des ICUE au niveau RESTREINT UE/EU RESTRICTED.

27. L'accès à distance à des services LAN à partir d'autres systèmes (par exemple, accès à distance à la messagerie électronique ou au support système à distance) est interdit, à moins que des mesures de sécurité spéciales ne soient mises en œuvre et qu'elles soient agréées par l'autorité octroyant la subvention, et lorsque les dispositions législatives et réglementaires nationales l'exigent, qu'elles soient approuvées par l'AHS compétente.

Gestion de la configuration

28. Une configuration matérielle et logicielle précise, telle qu'elle ressort des documents d'homologation/agrément (y compris les diagrammes système et réseau), doit être disponible et faire l'objet d'un entretien régulier.

29. Le responsable de la sécurité du bénéficiaire doit procéder à des contrôles de configuration sur le matériel et les logiciels afin de s'assurer qu'aucun matériel ou logiciel non autorisé n'a été installé.

30. Les modifications apportées à la configuration du SIC du bénéficiaire doivent être évaluées sous l'angle de leurs implications en matière de sécurité et doivent être approuvées par le responsable de la sécurité et, si les dispositions législatives et réglementaires nationales l'exigent, par l'AHS.

31. Le système doit être analysé au moins une fois par trimestre sous l'angle des vulnérabilités en matière de sécurité Un logiciel de détection de programmes malveillants doit être installé et être tenu à jour. Si possible, ce logiciel doit faire l'objet d'une approbation à l'échelle nationale ou d'une approbation reconnue au niveau international; à défaut, il devrait correspondre à une norme industrielle largement acceptée.

32. Le bénéficiaire doit élaborer un plan de continuité des activités. Des procédures de sauvegarde doivent être mises en place aux fins suivantes:

    a) fréquence des sauvegardes;

    b) exigences en matière de stockage sur site (conteneurs ignifugés) ou hors site;

    c) contrôle de l'accès autorisé aux copies de sauvegarde.

Expurgation et destruction

33. Dans le cas d'un SIC ou d'un support de stockage de données qui contenait, à un moment donné, des informations RESTREINT UE/EU RESTRICTED, l'expurgation suivante doit être opérée sur l'ensemble du système ou du support de stockage avant mise au rebut:

    a) les mémoires flash [par exemple clés USB, cartes SD, disques transistorisés (SSD) ou disques durs hybrides] doivent faire l'objet d'au moins trois passes de réécriture, puis être vérifiées pour veiller à ce que le contenu d'origine ne puisse pas être récupéré, ou être effacées à l'aide d'un logiciel de suppression approuvé;

    b) les supports magnétiques (disques durs, par exemple) doivent faire l'objet d'un processus de réécriture ou de démagnétisation;

    c) les supports optiques (CD ou DVD, par exemple) doivent être déchiquetés ou désintégrés;

    d) pour tout autre support de stockage, l'autorité octroyant la subvention ou, le cas échéant, l'ANS, l'ASD ou l'AHS, doit être consulté sur les exigences à respecter en matière de sécurité.

34. Tout support de stockage de données doit être expurgé de ses informations classifiées RESTREINT UE/EU RESTRICTED avant qu'il ne soit remis à une entité qui n'est pas autorisée à avoir accès à des informations classifiées RESTREINT UE/EU RESTRICTED (pour des travaux d'entretien, par exemple).

ANNEXE IV

Habilitation de sécurité du personnel et habilitation de sécurité d'établissement pour les bénéficiaires ou les sous-traitants qui traitent des informations RESTREINT UE/EU RESTRICTED et les ANS/ASD qui exigent la notification des conventions de subvention classifiées au niveau RESTREINT UE/EU RESTRICTED ([1])

État membre	HSE		Notification à l'ANS et/ou l'ASD de la convention de subvention ou du contrat de sous-traitance mettant en jeu des informations R-UE/EU-R		HSP	
	OUI	NON	OUI	NON	OUI	NON
Belgique		**X**		**X**		**X**
Bulgarie		**X**		**X**		**X**
Tchéquie		**X**		**X**		**X**
Danemark	**X**		**X**		**X**	
Allemagne		**X**		**X**		**X**
Estonie	**X**		**X**			**X**
Irlande		**X**		**X**		**X**
Grèce	**X**			**X**	**X**	
Espagne		**X**	**X**			**X**
France		**X**		**X**		**X**
Croatie		**X**	**X**			**X**
Italie		**X**	**X**			**X**
Chypre		**X**	**X**			**X**
Lettonie		**X**		**X**		**X**
Lituanie	**X**		**X**			**X**
Luxembourg	**X**		**X**		**X**	
Hongrie		**X**		**X**		**X**
Malte		**X**		**X**		**X**
Pays-Bas	**X** (uniquement pour les conventions de subvention et les contrats de sous-traitance liés à la défense)		**X** (uniquement pour les conventions de subvention et les contrats de sous-traitance liés à la défense)			**X**
Autriche		**X**		**X**		**X**
Pologne		**X**		**X**		**X**

([1]) Ces exigences nationales concernant les HSE/HSP et les notifications pour les conventions de subvention classifiée mettant en jeu des informations classifiées RESTREINT UE/EU RESTRICTED ne doivent pas imposer d'obligations supplémentaires aux autres États membres ou aux bénéficiaires et sous-traitants relevant de leur juridiction.
NB: Il est obligatoire de notifier les conventions de subvention mettant en jeu des informations CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET.

Portugal		**X**		**X**		**X**
Roumanie		**X**		**X**		**X**
Slovénie	**X**		**X**			**X**
Slovaquie	**X**		**X**			**X**
Finlande		**X**		**X**		**X**
Suède		**X**		**X**		**X**

ANNEXE V

LISTE DES SERVICES DES AUTORITÉS NATIONALES DE SÉCURITÉ/AUTORITÉS DE SÉCURITÉ DÉSIGNÉES CHARGÉS DU TRAITEMENT DES PROCÉDURES LIÉES À LA SÉCURITÉ INDUSTRIELLE

BELGIQUE

Autorité nationale de sécurité
FPS Foreign Affairs
Rue des Petits Carmes 15
1000 Bruxelles

Tél. +32 25014542 (Secrétariat)

Fax +32 25014596

Courriel: nvo-ans@diplobel.fed.be

BULGARIE

1. State Commission on Information Security — National Security Authority
   Kozloduy Street 4
   1202 Sofia
   Tél. +359 29835775
   Fax +359 29873750
   Courriel: dksi@government.bg

2. Defence Information Service at the Ministry of Defence (security service)
   Dyakon Ignatiy Street 3
   1092 Sofia
   Tél. +359 29227002
   Fax +359 29885211
   Courriel: office@iksbg.org

3. State Intelligence Agency (security service)
   Hajdushka Polyana Street 12
   1612 Sofia
   Tél. +359 29813221
   Fax +359 29862706
   Courriel: office@dar.bg

4. State Agency for Technical Operations (security service)
   Shesti Septemvri Street 29
   1000 Sofia
   Tél. +359 29824971
   Fax +359 29461339
   Courriel: dato@dato.bg

(Les autorités compétentes susmentionnées mènent les procédures de vérification en vue de la délivrance d'HSE aux entités juridiques qui demandent à conclure un contrat classifié et d'HSP aux personnes qui exécutent un contrat classifié pour les besoins de ces autorités.)

5. State Agency National Security (security service)

   Cherni Vrah Blvd. 45
   1407 Sofia

   Tél. +359 28147109

   Fax +359 29632188, +359 28147441

   Courriel: dans@dans.bg

(Le service de sécurité susmentionné mène les procédures de vérification en vue de la délivrance d'HSE et d'HSP à l'ensemble des autres entités juridiques et personnes qui demandent à conclure un contrat classifié ou une convention de subvention classifiée ou exécutent un contrat classifié ou une convention de subvention classifiée.)

TCHÉQUIE

Autorité nationale de sécurité
Industrial Security Department
PO Box 49
150 06 Praha 56

Tél. +420 257283129

Courriel: sbr@nbu.cz

DANEMARK

1. Politiets Efterretningstjeneste
   (Danish Security Intelligence Service)

   Klausdalsbrovej 1

   2860 Søborg

   Tél. +45 33148888

   Fax +45 33430190

2. Forsvarets Efterretningstjeneste
   (Danish Defence Intelligence Service)
   Kastellet 30
   2100 København Ø

   Tél. +45 33325566

   Fax +45 33931320

ALLEMAGNE

1. Pour les questions relatives à la politique de sécurité industrielle, les HSE, les plans de transport (hors matériel cryptographique/informations commerciales confidentielles):
   Ministre fédéral de l'économie et de l'énergie

   Industrial Security Division — RS3

   Villemombler Str. 76

   53123 Bonn

   Tél. +49 228996154028

   Fax +49 228996152676

   Courriel: dsagermany-rs3@bmwi.bund.de (adresse électronique professionnelle)

2. Pour les demandes de visite standard adressées par des entreprises allemandes ou à des entreprises allemandes:
Ministre fédéral de l'économie et de l'énergie

Industrial Security Division — RS2
Villemombler Str. 76
53123 Bonn

Tél. +49 228996152401

Fax +49 228996152603

Courriel: rs2-international@bmwi.bund.de ((adresse électronique professionnelle)

3. Plans de transport pour matériel cryptographique:

Federal Office for Information Security (BSI)
National Distribution Agency/NDA-EU DEU
Mainzer Str. 84
53179 Bonn

Tél. +49 2289995826052

Fax +49 228991095826052

Courriel: NDAEU@bsi.bund.de

ESTONIE

National Security Authority Department
Estonian Foreign Intelligence Service
Rahumäe tee 4B
11316 Tallinn

Tél. +372 6939211

Fax +372 6935001

Courriel: nsa@fis.gov.ee

IRLANDE

National Security Authority Ireland
Department of Foreign Affairs and Trade
76-78 Harcourt Street
Dublin 2
D02 DX45

Tél. +353 14082724

Courriel: nsa@dfa.ie

GRÈCE

Hellenic National Defence General Staff
E' Division (Security INTEL, CI BRANCH)
E3 Directorate
Industrial Security Office
Mesogeion Avenue 227-231
155 61 Holargos, Athens

Tél. +30 2106572022, +30 2106572178

Fax +30 2106527612

Courriel: daa.industrial@hndgs.mil.gr

ESPAGNE

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Calle Argentona, 30
28023 Madrid

Tél. +34 912832583, +34 912832752, +34 913725928

Fax +34 913725808

Courriel: nsa-sp@areatec.com

Pour les informations relatives à des programmes classifiés: programas.ons@areatec.com

Pour les questions d'habilitation de sécurité du personnel: hps.ons@areatec.com

Pour les plans de transport et les visites internationales: sp-ivtco@areatec.com

FRANCE

National Security Authority (NSA) (pour l'action et la mise en œuvre dans des domaines autres que l'industrie de la défense)
Secrétariat général de la défense et de la sécurité nationale
Sous-direction Protection du secret (SGDSN/PSD)
51 boulevard de la Tour-Maubourg
75700 Paris 07 SP

Tél. +33 171758193

Fax +33 171758200

Courriel: ANSFrance@sgdsn.gouv.fr

Designated Security Authority (pour la mise en œuvre dans le domaine de l'industrie de la défense)
Direction Générale de l'Armement
Service de la Sécurité de Défense et des systèmes d'Information (DGA/SSDI)
60 boulevard du général-Martial-Valin
CS 21623
75509 Paris Cedex 15

Tél. +33 988670421

Courriel: pour les formulaires et les DDV à la sortie: dga-ssdi.ai.fct@intradef.gouv.fr

pour les DDV à l'entrée: dga-ssdi.visit.fct@intradef.gouv.fr

CROATIE

Office of the National Security Council
Croatian NSA
Jurjevska 34
HR-10000 Zagreb

Tél. +385 14681222

Fax +385 14686049

Courriel: NSACroatia@uvns.hr

ITALIE

Presidenza del Consiglio dei Ministri
D.I.S. - U.C.Se.
Via di Santa Susanna 15
00187 Roma RM

Tél. +39 0661174266

Fax +39 064885273

CHYPRE

ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Λεωφόρος Στροβόλου, 172-174
Στρόβολος, 2048, Λευκωσία

Τηλέφωνα: +357 22807569, +357 22807764

Τηλεομοιότυπο: +357 22302351

Courriel: cynsa@mod.gov.cy

Ministry of Defence
National Security Authority (NSA)
Strovolos Avenue 172-174
2048 Strovolos, Nicosia

Tél. +357 22807569, +357 22807764

Fax +357 22302351

Courriel: cynsa@mod.gov.cy

LETTONIE

Autorité nationale de sécurité
Constitution Protection Bureau of the Republic of Latvia
PO Box 286
Riga, LV-1001

Tél. +371 67025418, +371 67025463

Fax +371 67025454

Courriel: ndi@sab.gov.lv, ndi@zd.gov.lv

LITUANIE

Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija
(The Commission for Secrets Protection Coordination of the Republic of Lituania)
Autorité nationale de sécurité
Pilaitės pr. 19
LT-06264 Vilnius

Tél. +370 70666128

Courriel: nsa@vsd.lt

LUXEMBOURG

Autorité Nationale de Sécurité
207, route d'Esch
L-1471 Luxembourg

Tél. +352 24782210

Courriel: ans@me.etat.lu

HONGRIE

National Security Authority of Hungary
Budapest, P.O. Box 710/50, 1399
Budapest, Szilágyi Erzsébet fasor 11/B, 1024

Tél. +36 13911862

Fax +36 13911889

Courriel: nbf@nbf.hu

MALTE

Director of Standardisation
Designated Security Authority for Industrial Security
Standards & Metrology Institute
Malta Competition and Consumer Affairs Authority
Mizzi House
National Road
Blata I-Bajda, HMR 9010

Tél.+356 23952000

Fax +356 21242406

Courriel: certification@mccaa.org.mt

PAYS-BAS

1. Ministry of the Interior and Kingdom Relations
PO Box 20010
2500 EA The Hague

Tél. +31 703204400

Fax +31 703200733

Courriel: nsa-nl-industry@minbzk.nl

2. Ministry of Defence
Industrial Security Department
PO Box 20701
2500 ES The Hague

Tél. +31 704419407

Fax +31 703459189

Courriel: indussec@mindef.nl

AUTRICHE

1. Federal Chancellery of Austria
Department I/10, Office for Information Security

Ballhausplatz 2
10104 Vienna

Tél. +43 153115202594

Courriel: isk@bka.gv.at

2. DSA in the military sphere:
BMLVS/Abwehramt

Postfach 2000
1030 Vienna

Courriel: abwa@bmlvs.gv.at

POLOGNE

Internal Security Agency
Department for the Protection of Classified Information
Rakowiecka 2 A
00-993 Warsaw

Tél. +48 225857944

Fax +48 225857443

Courriel: nsa@abw.gov.pl

PORTUGAL

Gabinete Nacional de Segurança
Serviço de Segurança Industrial
Rua da Junqueira nº 69
1300-342 Lisbon

Tél. +351 213031710

Fax +351 213031711

Courriel: sind@gns.gov.pt, franco@gns.gov.pt

ROUMANIE

Oficiul Registrului Național al Informațiilor Secrete de Stat — ORNISS
Romanian NSA — ORNISS — National Registry Office for Classified Information
Mures Street 4th
012275 Bucharest

Tél. +40 212075115

Fax +40 212245830

Courriel: relatii.publice@orniss.ro, nsa.romania@nsa.ro

SLOVÉNIE

Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
SI-1000 Ljubljana

Tél. +386 14781390

Fax +386 14781399

Courriel: gp.uvtp@gov.si

SLOVAQUIE

Národný bezpečnostný úrad
(Autorité nationale de sécurité)
Security Clearance Department
Budatínska 30
851 06 Bratislava

Tél. +421 268691111

Fax +421 268691700

Courriel: podatelna@nbu.gov.sk

FINLANDE

Autorité nationale de sécurité
Ministry for Foreign Affairs
PO Box 453
FI-00023 Government

Courriel: NSA@formin.fi

SUÈDE

1. Autorité nationale de sécurité

   Utrikesdepartementet (Ministry for Foreign Affairs)
   UD SÄK/NSA
   SE-103 39 Stockholm
   Tél. +46 84051000
   Fax +46 87231176
   Courriel: ud-nsa@gov.se

2. ASD

   Försvarets Materielverk (Swedish Defence Materiel Administration)
   FMV Säkerhetsskydd
   SE-115 88 Stockholm
   Tél. +46 87824000
   Fax +46 87826900
   Courriel: security@fmv.se