

N° 8492

CHAMBRE DES DEPUTES

PROJET DE LOI

portant approbation de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la République hellénique sur l'échange et la protection mutuelle des informations classifiées, fait à Athènes, le 24 octobre 2024

* * *

Document de dépôt

Dépôt: le 5.2.2025

*

Le Premier ministre,

Vu les articles 76 et 95, alinéa 1^{er}, de la Constitution ;

Vu l'article 10 du Règlement interne du Gouvernement ;

Vu l'article 58, paragraphe 1^{er}, du Règlement de la Chambre des Députés ;

Vu l'article 1^{er}, paragraphe 1^{er}, de la loi modifiée du 16 juin 2017 sur l'organisation du Conseil d'État ;

Considérant la décision du Gouvernement en conseil du 17 janvier 2025 approuvant sur proposition du Ministre des Affaires étrangères et du Commerce extérieur le projet de loi ci-après ;

Arrête :

Art. 1^{er}. Le Ministre des Affaires étrangères et du Commerce extérieur est autorisé à déposer au nom du Gouvernement à la Chambre des Députés le projet de loi portant approbation de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la République hellénique sur l'échange et la protection mutuelle des informations classifiées, fait à Athènes, le 24 octobre 2024 et à demander l'avis y relatif au Conseil d'État.

Art. 2. La Ministre déléguée auprès du Premier ministre, chargée des Relations avec le Parlement est chargée, pour le compte du Premier ministre et du Ministre des Affaires étrangères et du Commerce extérieur, de l'exécution du présent arrêté.

Luxembourg, le 5 février 2025

Le Premier ministre,

Luc FRIEDEN

*Le Ministre des Affaires étrangères
et du Commerce extérieur,*

Xavier BETTEL

*

EXPOSE DES MOTIFS

Le projet de loi vise à approuver l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la République hellénique sur l'échange et la protection mutuelle des informations classifiées, fait à Athènes, le 24 octobre 2024 (ci-après « l'Accord »).

I. Genèse de l'Accord

Depuis 2005, le Gouvernement du Grand-Duché de Luxembourg s'efforce de conclure des accords relatifs à la protection réciproque et à l'échange d'informations classifiées avec tous les États membres de l'Union européenne et de l'Organisation du Traité de l'Atlantique Nord, ainsi qu'avec des pays avec lesquels le Luxembourg doit être en mesure d'échanger des informations classifiées. La conclusion de tels accords s'inscrit dans le cadre d'une politique de sécurité globale que le Gouvernement a délibérément cherché à renforcer au cours des dix dernières années, notamment compte tenu des menaces croissantes auxquelles le Grand-Duché de Luxembourg doit faire face telles que le terrorisme, la criminalité organisée, la prolifération des armes de destruction massive, les cyber-attaques, et, pour ce qui est des risques pesant sur le patrimoine économique et financier de l'État, l'espionnage industriel et technologique. Dans ce contexte, la prévention constitue un élément fondamental pour réduire les risques liés aux menaces, en particulier les menaces hybrides. Par conséquent, il est essentiel pour le Grand-Duché de Luxembourg de poursuivre ses efforts en vue de conclure des accords en matière de protection et d'échange d'informations classifiées avec un nombre accru de pays.

Le Luxembourg a conclu à ce jour 31 accords bilatéraux relatifs à la protection réciproque et à l'échange d'informations classifiées, auxquels s'ajoutent quatre accords conclus au niveau multilatéral (à savoir par l'Union européenne, l'Agence Spatiale Européenne, l'Organisation du Traité de l'Atlantique Nord et l'Organisation Conjointe de Coopération en matière d'Armement).

II. Nature de l'Accord

Il s'agit d'un accord bilatéral qui instaure le cadre juridique relatif à la protection réciproque et à l'échange d'informations dites classifiées entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la République hellénique.

III. Contenu de l'Accord

L'Accord vise à créer le cadre juridique dans lequel s'inscrit la protection réciproque d'informations classifiées échangées avec la Grèce et les instances grecques du secteur public et du secteur privé.

L'Accord énonce, d'une part, les principes de base qui régissent la protection et l'échange d'informations classifiées et, d'autre part, les règles d'ordre procédural. Il s'insère dans le cadre des législations nationales respectives des deux États parties (ci-après les « Parties » ou la « Partie ») applicables à la protection des informations classifiées, à savoir, pour ce qui est du Grand-Duché de Luxembourg, la loi modifiée du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité.

Pour ce qui est du régime de protection des informations classifiées, chaque Partie s'engage, en vertu de l'Accord, à accorder aux informations qui lui sont transmises par l'autre Partie, le même degré de protection que celui accordé à ses propres informations classifiées de niveau équivalent. Pour ce qui est de l'accès aux informations classifiées, les Parties réservent ce dernier, sur la base du principe du besoin d'en connaître, aux personnes qui ont été informées des règles de sécurité applicables au traitement et à la protection des informations classifiées et qui sont dûment autorisées à y accéder en vertu de leurs fonctions ou d'une habilitation de sécurité du niveau approprié, conformément aux lois et réglementations respectives des Parties. Les Parties reconnaissent mutuellement les habilitations de sécurité délivrées par elles. Il s'y ajoute que les Parties n'ont le droit d'utiliser les informations classifiées qu'aux fins pour lesquelles elles ont été communiquées et dans les limites fixées par la Partie d'origine. La Partie destinataire ne communique les informations classifiées à un tiers sans l'accord écrit préalable de la Partie d'origine. Sont également fixées les conditions qui régissent les visites des installations au sein desquelles sont stockées les informations classifiées. Enfin, l'Accord contient également des dispositions régissant les contrats classifiés.

Liste des lois d'approbation des accords relatifs à l'échange et à la protection réciproque d'informations classifiées :

- 1) Loi du 15 juin 2004 portant approbation de l'Accord sur la Sécurité des Informations entre les Parties au Traité de l'Atlantique Nord avec ses annexes 1, 2, et 3 signé par le Luxembourg le 14 juillet 1998.
- 2) Loi du 14 juin 2005 portant approbation
 - de la Convention portant création d'une Agence spatiale européenne, faite à Paris, le 30 mai 1975
 - de l'Accord entre les Etats parties à la Convention portant création d'une Agence spatiale européenne et l'Agence spatiale européenne concernant la protection et l'échange d'informations classifiées, fait à Paris, le 19 août 2002
 - de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et l'Agence spatiale européenne relatif à l'adhésion du Grand-Duché de Luxembourg à la Convention portant création de l'Agence spatiale européenne et des clauses et conditions s'y rapportant, fait à Paris, le 6 mai 2004.
- 3) Loi du 16 décembre 2008 portant approbation de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la République fédérale d'Allemagne concernant la protection réciproque des informations classifiées, signé à Berlin le 17 janvier 2006.
- 4) Loi du 16 décembre 2008 portant approbation de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la République française concernant l'échange et la protection réciproque des informations classifiées, signé à Luxembourg, le 24 février 2006.
- 5) Loi du 16 décembre 2008 portant approbation de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la République de Lettonie concernant l'échange et la protection réciproque des informations classifiées, signé à Luxembourg, le 13 septembre 2007.
- 6) Loi du 13 mars 2009 portant approbation de l'Accord entre le Grand-Duché de Luxembourg et la République portugaise concernant l'échange et la protection réciproque des informations classifiées, signé à Luxembourg, le 22 février 2008.
- 7) Loi du 24 juillet 2011 portant approbation de l'Accord entre le Grand-Duché de Luxembourg et le Royaume d'Espagne concernant l'échange et la protection réciproque des informations classifiées, signé à Luxembourg, le 12 novembre 2009.
- 8) Loi du 8 mai 2013 portant approbation des Accords entre le Gouvernement du Grand-Duché de Luxembourg et certains pays concernant l'échange et la protection réciproque des informations classifiées.
 - a. Accord de sécurité entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la République tchèque, signé à Prague, le 11 avril 2011.
 - b. Accord de sécurité entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement du Royaume de Suède, signé à Bruxelles, le 23 mai 2011.
 - c. Accord de sécurité entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la République slovaque, signé à Bratislava, le 26 juillet 2011.
 - d. Accord de sécurité entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la République de Finlande, signé à Bruxelles, le 1^{er} décembre 2011.
 - e. Accord de sécurité entre le Grand-Duché de Luxembourg et le Royaume de Belgique, signé à Luxembourg, le 9 février 2012.
 - f. Accord de sécurité entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la République de Slovénie, signé à Bruxelles, le 14 mai 2012.
 - g. Accord de sécurité entre le Grand-Duché de Luxembourg et la République d'Estonie, signé à Bruxelles, le 23 juillet 2012.
 - h. Accord de sécurité entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de Géorgie, signé à Luxembourg, le 15 octobre 2012.
- 9) Loi du 18 juillet 2014 portant approbation de l'Accord de sécurité entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement du Royaume de Norvège concernant l'échange et la protection réciproque d'informations classifiées, signé à Bruxelles, le 21 février 2013.

- 10) Loi du 18 juillet 2014 portant approbation de l'Accord entre les Etats 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, signé à Bruxelles, le 25 mai 2011.
- 11) Loi du 27 novembre 2015 portant approbation
- de l'Accord de sécurité entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la République d'Autriche concernant l'échange et la protection réciproque des informations classifiées, signé à Vienne, le 13 novembre 2014
 - de l'Accord de sécurité entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la République de Croatie concernant l'échange et la protection réciproque des informations classifiées, signé à Luxembourg, le 13 mars 2014.
- 12) Loi du 3 décembre 2015 portant approbation de l'Accord de sécurité entre le Gouvernement du Grand-Duché de Luxembourg et l'Organisation Conjointe de Coopération en matière d'Armement (OCCAR) sur la protection des informations classifiées, fait à Luxembourg, le 6 janvier 2015.
- 13) Loi du 29 mars 2016 portant approbation de l'Accord de sécurité entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la République de Pologne concernant la protection réciproque d'informations classifiées, signé à Varsovie, le 12 mai 2015.
- 14) Loi du 31 août 2016 portant approbation de
- l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord concernant la protection réciproque d'informations classifiées, signé à Londres, le 8 septembre 2015
 - l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la République de Chypre concernant l'échange et la protection réciproque d'informations classifiées, signé à Luxembourg, le 3 septembre 2015.
- 15) Loi du 6 juin 2018 portant approbation de
- l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la République italienne concernant l'échange et la protection réciproque d'informations classifiées, fait à Rome le 20 avril 2017 ;
 - l'Accord de sécurité entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de Roumanie sur la protection réciproque des informations classifiées, signé à Bucarest, le 24 mai 2017.
- 16) Loi du 26 octobre 2019 portant approbation
1. de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la République de Bulgarie relatif à l'échange et à la protection réciproque d'informations classifiées, fait à Sofia, le 29 janvier 2018 ;
 2. de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Conseil des Ministres de la République d'Albanie relatif à la protection réciproque d'informations classifiées, fait à Luxembourg, le 25 juin 2018 ;
 3. de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de Hongrie relatif à l'échange et à la protection réciproque d'informations classifiées, fait à Budapest, le 5 septembre 2018 ;
 4. de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la République de Macédoine relatif à l'échange et à la protection réciproque d'informations classifiées, fait à Skopje, le 6 septembre 2018 ;
 5. de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la République fédérative du Brésil concernant l'échange et la protection réciproque d'informations classifiées, fait à New York, le 25 septembre 2018.
- 17) Loi du 30 novembre 2020 portant approbation de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la République de Malte relatif à la protection réciproque et à l'échange d'informations classifiées, fait à New York, le 26 septembre 2019.
- 18) Loi du 30 novembre 2020 portant approbation de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la République de Serbie concernant l'échange et la protection réciproque d'informations classifiées, fait à Luxembourg, le 4 février 2020.

- 19) Loi du 28 février 2024 portant approbation de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la République de Lituanie concernant l'échange et la protection réciproque d'informations classifiées, fait à Bruxelles, le 7 décembre 2020.
- 20) Loi du 28 février 2024 portant approbation de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la République française concernant l'échange et la protection des informations classifiées, fait à Paris, le 1^{er} juillet 2022¹.

*

TEXTE DU PROJET DE LOI

Article unique.

Est approuvé l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la République hellénique sur l'échange et la protection mutuelle des informations classifiées, fait à Athènes, le 24 octobre 2024.

*

ACCORD

entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la République Hellénique sur l'échange et la protection mutuelle des informations classifiées

Le Gouvernement du Grand-Duché de Luxembourg

et

le Gouvernement de la République Hellénique

Ci-après dénommés collectivement les « Parties » et individuellement la « Partie »,

Souhaitant assurer la protection des Informations classifiées produites ou échangées dans le cadre de la coopération entre les Parties ou entre des entités publiques et privées relevant de leur juridiction,

Dans le respect des intérêts nationaux et de la sécurité des Parties,

Reconnaissant les procédures standardisées relatives à la sécurité industrielle établies par le Multinational Industrial Security Working Group (MISWG),

ONT CONVENU de ce qui suit (ci-après l'« Accord ») :

Article 1

Objectif et champ d'application

1.1 Les Parties et les entités publiques et privées relevant de leur juridiction prennent, conformément à leurs lois et réglementations respectives, toutes les mesures appropriées pour assurer la protection des Informations classifiées produites ou échangées dans le cadre du présent Accord.

1.2 Le présent Accord s'applique à l'ensemble des activités, contrats ou accords impliquant des Informations classifiées, qui seront menés ou conclus entre les Parties après l'entrée en vigueur du présent Accord.

¹ Abrogeant l'accord cité sous 4).

1.3 Les dispositions du présent Accord s'appliquent également aux Informations classifiées déjà produites ou échangées dans le cadre de la coopération entre les Parties avant l'entrée en vigueur du présent Accord.

Article 2

Définitions

Aux fins du présent Accord, les définitions suivantes s'appliquent :

Informations classifiées : toutes les informations, quelle que soit leur forme, qui sont produites ou échangées entre les Parties ou entre des entités publiques et privées relevant de leur juridiction, en vertu des lois et réglementations nationales de l'une ou l'autre Partie, et qui, dans l'intérêt de la sécurité nationale, doivent être protégées contre toute divulgation, perte, destruction ou détournement non autorisés ou contre toute autre forme de compromission, et qui sont désignées comme telles et marquées de manière appropriée ;

Partie d'origine : la Partie, y compris toute entité publique ou privée relevant de sa juridiction, qui communique des Informations classifiées à la Partie destinataire ;

Partie destinataire : la Partie, y compris toute entité publique ou privée relevant de sa juridiction, qui reçoit des Informations classifiées de la Partie d'origine ;

Besoin d'en connaître : principe selon lequel l'accès à des Informations classifiées ne peut être accordé à une personne que dans le cadre de ses fonctions ou tâches officielles ;

Habilitation de sécurité du personnel : décision prise à l'issue d'une procédure d'habilitation de sécurité, conformément aux lois et réglementations respectives des Parties, sur la base de laquelle une personne est autorisée à accéder à des Informations classifiées et à les traiter jusqu'au niveau défini dans l'habilitation ;

Habilitation de sécurité d'établissement : décision prise à l'issue d'une procédure d'habilitation de sécurité, certifiant qu'un contractant, qui est une personne morale, remplit les conditions pour traiter des Informations classifiées d'un niveau de classification de sécurité donné, conformément aux lois et réglementations respectives des Parties ;

Contractant : personne physique ou morale possédant la capacité juridique de conclure des Contrats classifiés ;

Contrat classifié : un contrat ou un contrat de sous-traitance, y compris les négociations précontractuelles, qui contient des Informations classifiées ou implique l'accès à de telles informations ;

Infraction à la sécurité : un acte ou une omission, contraire aux lois et réglementations respectives des Parties, qui entraîne ou peut entraîner la divulgation, la perte, la destruction, le détournement ou tout autre type de compromission d'Informations classifiées ;

Tiers : tout État, y compris toute entité publique ou privée relevant de sa juridiction, ou toute organisation internationale qui n'est pas Partie au présent Accord.

Article 3

Autorités compétentes en matière de sécurité

3.1 Les Autorités nationales de sécurité désignées par les Parties, conformément à leurs lois et réglementations respectives, comme responsables de la mise en œuvre générale du présent Accord et de l'assurance de la protection des Informations classifiées produites ou échangées en vertu du présent Accord sont :

Pour le Grand-Duché de Luxembourg :

Ministère d'État, Service de renseignement de l'État, Autorité nationale de sécurité,

Pour la République Hellénique :

Autorité de sécurité nationale (NSA), État-major général de la défense nationale hellénique (HNDGS), Division conjointe du renseignement militaire (JMID).

3.2 Les Autorités nationales de sécurité se notifient par écrit toute autre autorité de sécurité compétente chargée de la mise en œuvre du présent Accord.

3.3 Les Parties se notifient mutuellement, par la voie diplomatique, toute modification ultérieure de leurs Autorités nationales de sécurité respectives ainsi que toute modification de leurs lois et réglementations respectives relatives aux Informations classifiées.

Article 4

Niveaux de classification de sécurité

4.1 Toute Information classifiée communiquée dans le cadre du présent Accord est marquée du niveau de classification de sécurité approprié conformément aux lois et réglementations respectives des Parties.

4.2 Les Parties s'engagent à protéger les Informations classifiées échangées entre elles et conviennent que les niveaux de classification de sécurité suivants s'équivalent :

<i>Pour le Grand-Duché de Luxembourg</i>	<i>Pour la République hellénique</i>	<i>En langue anglaise*</i>
TRES SECRET LUX	ΑΚΡΩΣ ΑΠΠΟΡΡΗΤΟ	TOP SECRET
SECRET LUX	ΑΠΟΡΡΗΤΟ	SECRET
CONFIDENTIEL LUX	ΕΜΠΙΣΤΕΥΤΙΚΟ	CONFIDENTIAL
RESTREINT LUX	ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	RESTRICTED

* Utilisés uniquement à des fins de compréhension et non pour un usage officiel.

Article 5

Accès aux informations classifiées

5.1 L'accès aux Informations classifiées est limité, sur la base du Besoin d'en connaître, aux personnes qui ont été formées au traitement et à la protection des Informations classifiées et qui y sont dûment autorisées, conformément aux lois et réglementations respectives des Parties.

5.2 Les Parties reconnaissent mutuellement les Habilitations de sécurité du personnel et les Habilitations de sécurité d'établissement accordées conformément à leurs lois et réglementations respectives. L'article 4, paragraphe 2 du présent Accord, s'applique en conséquence.

Article 6

Protection des informations classifiées

6.1 Conformément à leurs lois et réglementations nationales, les Parties prennent toutes les mesures appropriées pour protéger les Informations classifiées produites ou échangées dans le cadre du présent Accord. En vertu du présent Accord, les Parties accordent aux Informations classifiées le même degré de protection qu'à leurs propres Informations classifiées, avec le niveau de classification de sécurité correspondant.

6.2 La Partie d'origine :

- a) veille à ce que les Informations classifiées soient marquées d'un niveau de classification de sécurité approprié conformément à ses lois et réglementations nationales, et
- b) informe la Partie destinataire de toute condition de divulgation ou de toute limitation de l'utilisation des Informations classifiées, et l'informe par écrit de toute modification ultérieure du niveau de classification de sécurité.

6.3 La Partie destinataire s'engage à :

- a) veiller, conformément à ses lois et réglementations nationales, à ce que les Informations classifiées soient marquées d'un niveau de classification de sécurité équivalent, conformément à l'article 4, paragraphe 2 du présent Accord, et à

b) veiller à ce que le niveau de classification de sécurité ne soit pas modifié sans l'accord écrit préalable de la Partie d'origine.

6.4 Chaque Partie veille à ce que des mesures appropriées soient prises pour protéger les Informations classifiées qui sont traitées, stockées ou transmises dans des systèmes de communication et d'information. Ces mesures garantissent la confidentialité, l'intégrité, la disponibilité et, le cas échéant, la non-répudiation et l'authenticité des Informations classifiées, ainsi qu'un niveau approprié de responsabilité et de traçabilité des actions liées à ces informations.

Article 7

Restriction de l'usage d'informations classifiées

7.1 La Partie destinataire n'utilise les Informations classifiées qu'aux fins pour lesquelles elles ont été communiquées et dans les limites fixées par la Partie d'origine.

7.2 La Partie destinataire ne communique pas d'Informations classifiées à un Tiers sans l'accord écrit préalable de la Partie d'origine.

Article 8

Transfert d'informations classifiées

8.1 Les Informations classifiées sont transmises entre les Parties par la voie diplomatique ou par d'autres voies sécurisées convenues au préalable par les Autorités nationales de sécurité, conformément aux lois et réglementations respectives des Parties.

8.2 Les informations classifiées CONFIDENTIEL LUX/ΕΜΠΙΣΤΕΥΤΙΚΟ et d'un niveau supérieur sont enregistrées.

8.3 La transmission électronique d'Informations classifiées s'effectue par des moyens cryptographiques certifiés approuvés par les Autorités nationales de sécurité.

8.4 Les Informations classifiées portant la mention RESTREINT LUX/ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ peuvent également être envoyées par la poste ou par un autre service de livraison conformément aux lois et réglementations respectives des Parties.

Article 9

Reproduction, traduction et destruction des informations classifiées

9.1 Toutes les reproductions et traductions portent les niveaux de classification de sécurité appropriés et sont protégées de la même manière que les Informations classifiées originales. Les traductions et le nombre de reproductions sont limités au minimum requis à des fins officielles.

9.2 Toutes les traductions portent la mention du niveau de classification de sécurité des Informations classifiées d'origine et contiennent une annotation appropriée dans la langue de traduction indiquant qu'elles contiennent des Informations classifiées de la Partie d'origine.

9.3 Les Informations classifiées marquées TRES SECRET LUX/ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ, tant l'original que la traduction, ne peuvent être reproduites ou traduites qu'avec l'accord écrit préalable de la Partie d'origine.

9.4 Les Informations classifiées marquées TRES SECRET LUX/ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ ne doivent pas être détruites. Lorsqu'elles ne sont plus nécessaires, elles sont renvoyées à la Partie d'origine.

9.5 Les Informations classifiées marquées SECRET LUX/ΑΠΟΡΡΗΤΟ ou marquées d'un niveau inférieur sont détruites lorsque la Partie destinataire ne les juge plus nécessaires, dans la mesure où cela empêche leur reconstitution totale ou partielle, conformément à ses lois et réglementations nationales.

9.6 Si une situation de crise rend impossible la protection ou la restitution des Informations classifiées produites ou échangées dans le cadre du présent Accord, les Informations classifiées sont immédiatement détruites. La Partie destinataire notifie dès que possible leur destruction à l'Autorité nationale de sécurité de la Partie d'origine.

Article 10

Contrats classifiés

10.1 Chaque Contrat classifié ou contrat de sous-traitance comprend une annexe relative à la sécurité, en vertu de laquelle l'autorité contractante relevant de la juridiction de la Partie d'origine précise les Informations classifiées qui seront communiquées au Contractant relevant de la juridiction de la Partie destinataire, le niveau de classification de sécurité attribué à ces informations et les obligations du Contractant en ce qui concerne la protection des Informations classifiées. Une copie de l'annexe de sécurité est envoyée à l'Autorité nationale de sécurité de la Partie destinataire.

10.2 L'Autorité nationale de sécurité de la Partie destinataire veille à ce que les Informations classifiées relatives à un Contrat classifié soient communiquées aux Contractants, aux sous-traitants ou aux contractants potentiels après :

- a) qu'il a été vérifié que le Contractant, le sous-traitant ou le contractant potentiel et ses établissements sont en mesure d'assurer une protection adéquate des Informations classifiées ;
- b) que les établissements disposent d'une Habilitation de sécurité d'établissement appropriée ;
et
- c) que les personnes qui exercent des fonctions nécessitant l'accès à des Informations classifiées disposent d'une Habilitation de sécurité du personnel appropriée.

10.3 La Partie destinataire veille à ce que toutes les personnes ayant accès aux Informations classifiées soient informées de leurs responsabilités et de leur obligation de protéger les Informations classifiées conformément à ses lois et réglementations nationales.

10.4 L'Autorité nationale de sécurité de la Partie d'origine peut demander qu'une inspection de sécurité concernant la protection des Informations classifiées soit effectuée dans un établissement afin d'assurer le respect permanent des normes de sécurité conformément à ses lois et réglementations nationales.

Article 11

Visites

11.1 Les visites nécessitant l'accès à des Informations classifiées sont soumises à l'autorisation préalable de l'Autorité nationale de sécurité de la Partie hôte.

11.2 Une demande de visite est soumise à l'Autorité nationale de sécurité compétente au moins trois (3) semaines avant le début de la visite. Pour chaque visiteur/participant, la demande de visite comprend les informations suivantes, qui ne seront utilisées qu'aux fins de la visite :

- a) nom et prénom(s) du visiteur, date et lieu de naissance, nationalité(s) et numéro de carte d'identité/passeport ;
- b) fonction du visiteur et nom de l'organisation représentée ;
- c) spécification du projet auquel le visiteur participe ;
- d) validité et niveau de classification de l'Habilitation de sécurité du personnel du visiteur, le cas échéant ;

- e) nom, adresse, numéro de téléphone, adresse électronique et point de contact de l'établissement à visiter ;
- f) objet de la visite, y compris le niveau de sécurité le plus élevé des Informations classifiées concernées ;
- g) date et durée de la visite, et dans le cas de visites récurrentes, la période totale couverte par les visites doit être indiquée ;
- h) la date et la signature de l'Autorité nationale de sécurité expéditrice ;
- i) d'autres données supplémentaires, approuvées par les Autorités nationales de sécurité.

11.3 En cas d'urgence, les Autorités nationales de sécurité peuvent convenir d'un délai plus court pour la présentation d'une demande de visite.

11.4 Les Autorités nationales de sécurité peuvent convenir d'une liste de visiteurs ayant droit à des visites récurrentes. La liste est valable pour une période initiale ne dépassant pas douze (12) mois et peut être prolongée pour une période supplémentaire ne dépassant pas douze (12) mois. La demande de visites récurrentes est présentée conformément à la procédure prévue au deuxième paragraphe du présent article. Une fois la liste approuvée, les visites peuvent être organisées directement entre les établissements concernés.

11.5 Chaque Partie garantit la protection des données à caractère personnel des visiteurs conformément à ses lois et réglementations nationales.

11.6 Toute Information classifiée à laquelle un visiteur a eu accès au cours de sa visite est considérée comme une Information classifiée au titre du présent Accord.

Article 12

Coopération en matière de protection des informations classifiées

12.1 Afin d'atteindre et de maintenir des niveaux de sécurité comparables, les Autorités nationales de sécurité se communiquent, sur demande, des informations concernant leurs normes, procédures et pratiques nationales en matière de sécurité pour la protection des Informations classifiées.

12.2 Sur demande, l'Autorité nationale de sécurité ou toute autre autorité de sécurité compétente de la Partie d'origine est autorisée à rendre visite à l'autre Partie afin de vérifier auprès de l'Autorité nationale de sécurité ou toute autorité de sécurité compétente de la Partie destinataire si les Informations classifiées échangées en vertu du présent Accord sont protégées conformément au présent Accord.

12.3 Les Autorités de sécurité compétentes s'informent mutuellement des risques de sécurité exceptionnels susceptibles de mettre en péril les Informations classifiées divulguées ou les systèmes de protection des Informations classifiées.

12.4 Sur demande, et conformément aux lois et réglementations respectives des Parties, les Autorités nationales de sécurité se prêtent mutuellement assistance pour mener à bien une procédure d'habilitation de sécurité. Elles échangent des informations sur les éventuels problèmes de sécurité qui revêtent de l'importance dans le cadre de la procédure d'habilitation de sécurité.

12.5 À la demande de l'Autorité nationale de sécurité de la Partie d'origine, l'Autorité nationale de sécurité de la Partie destinataire confirme par écrit la délivrance d'une Habilitation de sécurité du personnel à une personne physique ou d'une Habilitation de sécurité d'établissement à une personne morale.

12.6 Les Autorités nationales de sécurité s'informent mutuellement et sans délai de toute modification des Habilitations de sécurité du personnel et des Habilitations de sécurité d'établissement.

*Article 13****Infraction à la sécurité***

13.1 En cas d'Infraction à la sécurité entraînant la divulgation non autorisée, le détournement ou la perte d'Informations classifiées ou de soupçon d'une telle Infraction, l'Autorité nationale de sécurité de la Partie destinataire en informe immédiatement par écrit l'Autorité nationale de sécurité de la Partie d'origine et veille à l'ouverture d'une enquête appropriée.

13.2 Les autorités compétentes de la Partie destinataire prennent toutes les mesures appropriées en vertu de leurs lois et réglementations nationales pour limiter les conséquences de l'Infraction visée au premier paragraphe du présent article et dans le but de prévenir de nouvelles violations. Sur demande, la Partie d'origine fournit une assistance appropriée ; elle est informée des résultats de l'enquête et des mesures correctives prises à la suite de l'Infraction.

13.3 Lorsqu'une Infraction à la sécurité se produit chez un Tiers, l'Autorité nationale de sécurité du Tiers est invitée par l'Autorité nationale de sécurité de la Partie destinataire à prendre sans délai les mesures visées au deuxième alinéa du présent article.

*Article 14****Dépenses***

Chaque Partie contractante prend en charge ses propres frais encourus dans le cadre de la mise en œuvre du présent Accord.

*Article 15****Règlement des litiges***

Tout litige concernant l'interprétation ou la mise en œuvre du présent Accord est réglé par consultation et/ou négociation entre les Parties et n'est pas soumis à un tribunal national ou international ni à un quelconque arbitrage pour règlement.

*Article 16****Dispositions finales***

16.1 Le présent Accord entre en vigueur le premier jour du deuxième mois suivant la réception de la dernière notification par laquelle les Parties s'informent mutuellement, par la voie diplomatique, que les conditions juridiques internes requises pour son entrée en vigueur ont été remplies.

16.2 Le présent Accord peut être modifié par consentement mutuel écrit des Parties. Ces modifications entrent en vigueur conformément à la procédure prévue au premier paragraphe du présent article.

16.3 Le présent Accord est conclu pour une durée indéterminée. Chaque Partie peut résilier le présent Accord en adressant à l'autre Partie une notification écrite de résiliation par la voie diplomatique. Dans ce cas, le présent Accord sera résilié six (6) mois après la date de réception de la notification de résiliation par l'autre Partie.

16.4 En cas de résiliation du présent Accord, toute Information classifiée échangée ou produite dans le cadre du présent Accord continue d'être protégée conformément aux dispositions du présent Accord et, sur demande, est renvoyée à la Partie d'origine.

16.5 Si nécessaire, les Autorités nationales de sécurité ou toute autre autorité de sécurité compétente des Parties peuvent se consulter sur les aspects techniques détaillés liés à l'application du présent Accord et peuvent conclure, au cas par cas, des instruments juridiques appropriés ou des protocoles de sécurité spécifiques afin de compléter le présent Accord.

EN FOI DE QUOI, les soussignés, dûment autorisés à cet effet, ont signé le présent Accord.

FAIT à Athènes, le 24 octobre 2024, en deux exemplaires originaux, chacun en langues française, grecque et anglaise et chaque texte faisant également foi. En cas de divergence d'interprétation, le texte anglais prévaut.

*Pour le Gouvernement
du Grand-Duché de Luxembourg*

Elisabeth CARDOSO

*Ambassadrice du Grand-Duché
de Luxembourg en Grèce*

*Pour le Gouvernement
de la République Hellénique*

Major Général
Grigorios P. BOUNTLIAKIS

*Directeur du Service E' de l'État-major général
de la défense nationale*

*

AGREEMENT

between the Government of the Grand Duchy of Luxembourg and the Government of the Hellenic Republic on exchange and mutual protection of classified information

The Government of the Grand Duchy of Luxembourg

and

the Government of the Hellenic Republic

Hereinafter collectively referred to as the "Parties" and individually as the "Party",

Wishing to ensure the protection of Classified Information generated or exchanged in the course of cooperation between the Parties or between public and private entities under their jurisdiction,

In respect of the national interests and security of the Parties,

Acknowledging the standardized Industrial Security procedures established by the Multinational Industrial Security Working Group (MISWG),

HAVE AGREED as follows (hereafter the "Agreement"):

Article 1

Objective and scope

1.1 The Parties and public and private entities under their jurisdiction shall, in accordance with the Parties' respective laws and regulations, take all appropriate measures to ensure the protection of Classified Information which is generated or exchanged under this Agreement.

1.2 This Agreement shall apply to any activities, contracts or agreements involving Classified Information that will be conducted or concluded between the Parties following the entering into force of this Agreement.

1.3 The provisions of this Agreement shall also apply to Classified Information already generated or exchanged in the process of cooperation between the Parties before the entering into force of this Agreement.

*Article 2****Definitions***

For the purposes of this Agreement, the following definitions shall apply:

Classified Information: any information, regardless of its form, which is generated or exchanged between the Parties or between public and private entities under their jurisdiction, under the national laws and regulations of either Party, and which, in the interests of national security, requires protection against unauthorised disclosure, loss, destruction, or misappropriation or any other kind of compromise and is designated as such and marked appropriately;

Originating Party: the Party, including any public or private entities under its jurisdiction, which releases Classified Information to the Recipient Party;

Recipient Party: the Party, including any public or private entities under its jurisdiction, which receives Classified Information from the Originating Party;

Need-to-Know: a principle by which access to Classified Information may be granted to an individual only in connection with his/her official duties or tasks;

Personnel Security Clearance: a determination, following a security vetting process, in accordance with the Parties' respective laws and regulations, on the basis of which an individual is authorised to access to and handle Classified Information up to the level defined in the clearance;

Facility Security Clearance: a determination, following a security vetting process, certifying that a contractor which is a legal entity fulfills the conditions to handle Classified Information of a specified security classification level in accordance with the Parties' respective laws and regulations;

Contractor: an individual or legal entity possessing the legal capacity to conclude Classified Contracts;

Classified Contract: a contract or a subcontract, including pre-contractual negotiations, which contains Classified Information or involves access to such information;

Breach of Security: an act or an omission, contrary to the Parties' respective laws and regulations, which results, or may result in disclosure, loss, destruction, misappropriation or any other type of compromise of Classified Information;

Third Party: any State, including any public or private entity under its jurisdiction, or any international organisation that is not a Party to this Agreement.

*Article 3****Competent security authorities***

3.1 The National Security Authorities designated in accordance with the Parties' respective laws and regulations by them as responsible for the general implementation of this Agreement and for the assurance of protection of Classified Information generated or exchanged according to this Agreement are:

For the Grand Duchy of Luxembourg:

Ministère d'Etat, Service de renseignement de l'Etat, Autorité nationale de sécurité,

For the Hellenic Republic:

National Security Authority (NSA), Hellenic National Defence General Staff (HNDGS), Joint Military Intelligence Division (JMID).

3.2 The National Security Authorities shall notify each other in writing of any other competent security authorities responsible for the implementation of this Agreement.

3.3 The Parties shall notify each other, through diplomatic channels, of any subsequent changes to their respective National Security Authorities as well as of any change in their respective laws and regulations related to Classified Information.

*Article 4****Security classification levels***

4.1 Any Classified Information released under this Agreement shall be marked with the appropriate security classification level in accordance with the Parties' respective laws and regulations.

4.2 The Parties undertake to protect Classified Information exchanged between them and agree that the following security classification levels shall be equivalent:

<i>For the Grand Duchy of Luxembourg</i>	<i>For the Hellenic Republic</i>	<i>In the english language*</i>
TRES SECRET LUX	ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	TOP SECRET
SECRET LUX	ΑΠΟΡΡΗΤΟ	SECRET
CONFIDENTIEL LUX	ΕΜΠΙΣΤΕΥΤΙΚΟ	CONFIDENTIAL
RESTREINT LUX	ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	RESTRICTED

* Used only for understanding purposes, not for official use.

*Article 5****Access to classified information***

5.1 Access to Classified Information shall be limited to individuals on a Need-to-Know basis, who have been briefed on handling and protecting Classified Information, and who are duly authorised thereto in accordance with the Parties' respective laws and regulations.

5.2 The Parties shall mutually recognise their Personnel Security Clearances and Facility Security Clearances granted in accordance with their respective laws and regulations. Article 4, paragraph 2 of this Agreement, shall apply accordingly.

*Article 6****Protection of classified information***

6.1 In accordance with their national laws and regulations, the Parties shall take all appropriate measures for the protection of Classified Information, which is generated or exchanged under this Agreement. The Parties shall afford to Classified Information under this Agreement the same protection as to their own Classified Information with the corresponding security classification level.

6.2 The Originating Party shall:

- a) ensure that Classified Information is marked with an appropriate security classification level in accordance with its national laws and regulations, and
- b) inform the Recipient Party of any conditions of release or limitations on the use of Classified Information, and inform in writing of any subsequent changes in security classification level.

6.3 The Recipient Party shall:

- a) in accordance with its national laws and regulations, ensure that Classified Information is marked with an equivalent level of security classification in accordance with Article 4, paragraph 2 of this Agreement, and
- b) ensure that the security classification level is not changed without the prior written consent of the Originating Party.

6.4 Each Party shall ensure that appropriate measures are taken to protect Classified Information which is processed, stored or transmitted in communication and information systems. Such measures

shall ensure the confidentiality, integrity, availability and, where applicable, non-repudiation and authenticity of Classified Information, as well as an appropriate level of accountability and traceability of actions in relation to that information.

Article 7

Restriction on the use of classified information

7.1 The Recipient Party shall use Classified Information solely for the purpose for which it has been released and within the limitations stated by the Originating Party.

7.2 The Recipient Party shall not release Classified Information to a Third Party without the prior written consent of the Originating Party.

Article 8

Transfer of classified information

8.1 Classified Information shall be transferred between the Parties through diplomatic channels or through other secure channels mutually agreed upon in advance by their National Security Authorities in accordance with the Parties' respective laws and regulations.

8.2 Information classified CONFIDENTIEL LUX/ΕΜΠΙΣΤΕΥΤΙΚΟ and above shall be registered.

8.3 Electronic transmission of Classified Information shall be carried out through certified cryptographic means agreed upon by the National Security Authorities.

8.4 Classified Information marked as RESTREINT LUX/ΠΕΠΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ may also be transferred by post or another delivery service in accordance with the Parties' respective laws and regulations.

Article 9

Reproduction, translation and destruction of classified information

9.1 All reproductions and translations shall bear appropriate security classification levels and shall be protected in the same way as the original Classified Information. Translations and the number of reproductions shall be limited to the minimum amount required for official purposes.

9.2 All translations shall be marked with the security classification level of the original Classified Information, and shall contain suitable annotation in the language of translation indicating that they contain Classified Information of the Originating Party.

9.3 Classified Information marked as TRES SECRET LUX/ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ, both the original and translation, shall be reproduced or translated only upon prior written consent of the Originating Party.

9.4 Classified Information marked as TRES SECRET LUX/ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ shall not be destroyed. When no longer required, it shall be returned to the Originating Party.

9.5 Classified Information marked as SECRET LUX/ΑΠΟΡΡΗΤΟ or below shall be destroyed when it is no longer considered necessary by the Recipient Party, insofar as to prevent its reconstruction in whole or in part, in accordance with its national laws and regulations.

9.6 If a crisis situation makes it impossible to protect or return Classified Information generated or exchanged under this Agreement, the Classified Information shall be destroyed immediately. The

Recipient Party shall notify the National Security Authority of the Originating Party of its destruction as soon as possible.

Article 10

Classified contracts

10.1 A security annex shall be an integral part of each Classified Contract, or subcontract, by which the contracting authority under the jurisdiction of the Originating Party shall specify which Classified Information is to be released to the Contractor under the jurisdiction of the Recipient Party, which security classification level has been assigned to that information and the Contractor's obligations to protect the Classified Information. A copy of the security annex shall be sent to the National Security Authority of the Recipient Party.

10.2 The National Security Authority of the Recipient Party shall ensure that Classified Information related to a Classified Contract is released to Contractors, subcontractors or prospective contractors after:

- a) it has been ensured that the Contractor, subcontractor or prospective contractor and its facilities are able to provide suitable protection for the Classified Information;
- b) the facilities have an appropriate Facility Security Clearance; and
- c) persons who perform functions which require access to Classified Information have appropriate Personnel Security Clearance.

10.3 The Recipient Party shall ensure that all persons having access to Classified Information are informed of their responsibilities and obligation to protect the Classified Information in accordance with its national laws and regulations.

10.4 The National Security Authority of the Originating Party may request that a security inspection regarding the protection of Classified Information is undertaken at a facility to ensure the continuing compliance with security standards in accordance with its laws and regulations.

Article 11

Visits

11.1 Visits requiring access to Classified Information shall be subject to the prior authorisation of the National Security Authority of the host Party.

11.2 A request for visit shall be submitted to the competent National Security Authority at least three (3) weeks prior to the commencement of the visit. The request for visit shall include for each visitor/participant, the following information, which shall be used only for the purpose of the visit:

- a) first and last name(s) of the visitor, date and place of birth, nationality(ies) and identity card/passport number;
- b) position of the visitor and name of the organization represented;
- c) a specification of the project in which the visitor is a participant;
- d) the validity and classification level of the visitor's Personnel Security Clearance, if required;
- e) name, address, phone number, e-mail address and point of contact of the facility to be visited;
- f) the purpose of the visit, including the highest security classification level of Classified Information to be involved;
- g) the date and duration of the visit, and in the case of recurring visits, the total period covered by the visits shall be stated;
- h) date and signature of the sending National Security Authority;
- i) other additional data, agreed upon by the National Security Authorities.

11.3 In urgent cases, the National Security Authorities may agree on a shorter period for the submission of a request for visit.

11.4 The National Security Authorities may agree on a list of visitors entitled to recurring visits. The list shall be valid for an initial period not exceeding twelve (12) months and may be extended for a further period not exceeding twelve (12) months. The request for recurring visits shall be submitted in accordance with the procedure set forth in the second paragraph of this article. Once a list has been approved, visits may be arranged directly between the facilities involved.

11.5 Each Party shall guarantee the protection of personal data of visitors in accordance with its national laws and regulations.

11.6 Any Classified Information to which a visitor had access to, during his visit, shall be considered as Classified Information under this Agreement.

Article 12

Cooperation on the protection of classified information

12.1 In order to achieve and maintain comparable standards of security, the National Security Authorities shall, on request, provide each other with information about their national security standards, procedures and practices for the protection of Classified Information.

12.2 Upon request, the National Security Authority or any other competent security authority of the Originating Party shall be authorized to visit the other Party in order to ascertain with the National Security Authority or any competent security authority of the Recipient Party, whether the Classified Information exchanged pursuant to this Agreement is protected in accordance with this Agreement.

12.3 The competent security authorities shall inform each other of exceptional security risks that may endanger released Classified Information or Classified Information protection systems.

12.4 Upon request, and in accordance with the Parties' respective laws and regulations, the National Security Authorities shall assist each other in carrying out a security vetting process. They shall exchange information on possible security concerns that are of importance in the security vetting process.

12.5 Upon request of the National Security Authority of the Originating Party, the National Security Authority of the Recipient Party shall issue a written confirmation that an individual has been issued a Personnel Security Clearance or a legal entity has been issued a Facility Security Clearance.

12.6 The National Security Authorities shall promptly inform each other about any changes in Personnel Security Clearances and Facility Security Clearances.

Article 13

Breach of security

13.1 In the event of a Breach of Security resulting in the unauthorised disclosure, misappropriation or loss of Classified Information or suspicion of such a Breach, the National Security Authority of the Recipient Party shall immediately notify the National Security Authority of the Originating Party thereof in writing and ensure the initiation of an appropriate investigation.

13.2 The competent authorities of the Recipient Party shall take all appropriate measures under its national laws and regulations to limit the consequences of the breach referred to in the first paragraph of this article and to prevent any further breaches. Upon request, the Originating Party shall provide appropriate assistance; it shall be informed of the outcome of the investigation and the corrective measures taken due to the breach.

13.3 When a Breach of Security has occurred in a Third Party, the National Security Authority of the Third Party shall be requested by the National Security Authority of the Recipient Party to take without delay the measures referred to in the second paragraph of this article.

Article 14

Expenses

Each Contracting Party shall bear its own costs incurred in the course of implementing this Agreement.

Article 15

Resolution of disputes

Any dispute regarding the interpretation or implementation of this Agreement shall be settled by consultation and/or negotiation between the Parties and shall not be referred to any national or international tribunal or to any third party for settlement.

Article 16

Final provisions

16.1 This Agreement shall enter into force on the first day of the second month following the receipt of the last notification by which the Parties inform each other, through diplomatic channels, that the internal legal requirements for its entry into force have been fulfilled.

16.2 This Agreement may be amended by the mutual, written consent of the Parties. Such amendments shall enter into force in accordance with the procedure set forth in the first paragraph of this article.

16.3 This Agreement shall be concluded for an indefinite period. Either Party may terminate this Agreement by giving a written notice of termination to the other Party through diplomatic channels. In such case, this Agreement will be terminated six (6) months after the date of the receipt of the termination notice by the other Party.

16.4 In the event of termination of this Agreement, any Classified Information exchanged or generated under this Agreement shall continue to be protected in accordance with the provisions set forth herein and, upon request, returned to the Originating Party.

16.5 Where necessary, the National Security Authorities or any other competent security authorities of the Parties may consult each other on detailed technical aspects relating to the application of this Agreement and may conclude, on a case-by-case basis, appropriate legal instruments or specific security protocols in order to complement this Agreement.

IN WITNESS WHEREOF, the undersigned, duly authorised to this effect, have signed this Agreement.

DONE at Athens, on this 24th day of October 2024, in two originals, each in the French, Greek, and English languages and each text being equally authentic. In case of divergence of interpretation, the English text shall prevail.

*For the Government of the
Grand Duchy of Luxembourg*

Elisabeth CARDOSO

*Ambassador of the Grand Duchy
of Luxembourg in Greece*

*For the Government of the
Hellenic Republic*

Major Général
Grigorios P. BOUNTLIAKIS

*Director of the E' Branch of the Hellenic
National Defence General Staff*

COMMENTAIRE DE L'ARTICLE UNIQUE

L'article unique du projet de loi vise à approuver l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la République hellénique sur l'échange et la protection mutuelle des informations classifiées, fait à Athènes, le 24 octobre 2024.

L'Accord entrera en vigueur lorsque les deux Parties auront rempli les conditions juridiques internes pour son entrée en vigueur, dans les conditions de l'article 16, paragraphe 1^{er}, de l'Accord.

*

FICHE FINANCIERE

conformément à l'article 79 de la loi modifiée du 8 juin 1999
sur le budget, la comptabilité et la trésorerie de l'État.

Le projet de loi sous examen ne comporte pas de dispositions dont l'application est susceptible de grever le budget de l'Etat.

*

CHECK DE DURABILITÉ - NOHALTEGKEETSCHCK



La présente page interactive nécessite au minimum la version 8.1.3 d'Adobe Acrobat® Reader®. La dernière version d'Adobe Acrobat Reader pour tous systèmes (Windows®, Mac, etc.) est téléchargeable gratuitement sur le site de Adobe Systems Incorporated.

Ministre responsable :	Le Ministre des Affaires étrangères et du Commerce extérieur
Projet de loi ou amendement :	Projet de loi portant approbation de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la République hellénique, fait à Athènes, le 24 octobre 2024.

Le check de durabilité est un outil d'évaluation des actes législatifs par rapport à leur impact sur le développement durable. Son objectif est de donner l'occasion d'introduire des aspects relatifs au développement durable à un stade préparatoire des projets de loi. Tout en faisant avancer ce thème transversal qu'est le développement durable, il permet aussi d'assurer une plus grande cohérence politique et une meilleure qualité des textes législatifs.

1. Est-ce que le projet de loi sous rubrique a un impact sur le champ d'action (1-10) du 3^{ième} Plan national pour un développement durable (PNDD) ?
2. En cas de réponse négative, expliquez-en succinctement les raisons.
3. En cas de réponse positive sous 1., quels seront les effets positifs et/ou négatifs éventuels de cet impact ?
4. Quelles catégories de personnes seront touchées par cet impact ?
5. Quelles mesures sont envisagées afin de pouvoir atténuer les effets négatifs et comment pourront être renforcés les aspects positifs de cet impact ?

Afin de faciliter cet exercice, l'instrument du contrôle de la durabilité est accompagné par des points d'orientation – **auxquels il n'est pas besoin de réagir ou répondre mais qui servent uniquement d'orientation**, ainsi que par une documentation sur les dix champs d'actions précités.

1. Assurer une inclusion sociale et une éducation pour tous.

Points d'orientation
Documentation Oui Non

N/A

2. Assurer les conditions d'une population en bonne santé.

Points d'orientation
Documentation Oui Non

N/A

3. Promouvoir une consommation et une production durables.

Points d'orientation
Documentation Oui Non

N/A

4. Diversifier et assurer une économie inclusive et porteuse d'avenir.Points d'orientation
Documentation Oui Non

N/A

5. Planifier et coordonner l'utilisation du territoire.Points d'orientation
Documentation Oui Non

N/A

6. Assurer une mobilité durable.Points d'orientation
Documentation Oui Non

N/A

7. Arrêter la dégradation de notre environnement et respecter les capacités des ressources naturelles.Points d'orientation
Documentation Oui Non

N/A

8. Protéger le climat, s'adapter au changement climatique et assurer une énergie durable.Points d'orientation
Documentation Oui Non

N/A

9. Contribuer, sur le plan global, à l'éradication de la pauvreté et à la cohérence des politiques pour le développement durable.Points d'orientation
Documentation Oui Non

N/A

10. Garantir des finances durables.Points d'orientation
Documentation Oui Non

N/A

Cette partie du formulaire est facultative - Veuillez cocher la case correspondante

En outre, et dans une optique d'enrichir davantage l'analyse apportée par le contrôle de la durabilité, il est proposé de recourir, de manière facultative, à une évaluation de l'impact des mesures sur base d'indicateurs retenus dans le PNDD. Ces indicateurs sont suivis par le STATEC.

Continuer avec l'évaluation ? Oui Non

(1) Dans le tableau, choisissez l'évaluation : **non applicable**, ou de 1 = **pas du tout probable** à 5 = **très possible**

FICHE D'ÉVALUATION D'IMPACT MESURES LÉGISLATIVES, RÉGLEMENTAIRES ET AUTRES



La présente page interactive nécessite au minimum la version 8.1.3 d'Adobe Acrobat® Reader®. La dernière version d'Adobe Acrobat Reader pour tous systèmes (Windows®, Mac, etc.) est téléchargeable gratuitement sur le site de Adobe Systems Incorporated.

1. Coordonnées du projet

Les champs marqués d'un * sont obligatoires

Intitulé du projet :	Projet de loi portant approbation de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la République hellénique sur l'échange et la protection mutuelle des informations classifiées, fait à Athènes, le 24 octobre 2024.		
Ministre:	Le Ministre des Affaires étrangères et du Commerce extérieur		
Auteur(s) :	Daniela Holderer		
Téléphone :	247 72489	Courriel :	daniela.holderer@mae.etat.lu
Objectif(s) du projet :	Approbation législative d'un accord bilatéral		
Autre(s) Ministère(s) / Organisme(s) / Commune(s) impliqué(e)(s)	Ministère d'Etat (Autorité nationale de sécurité)		
Date :	11/12/2024		

2. Objectifs à valeur constitutionnelle

Les champs marqués d'un * sont obligatoires

Le projet contribue-t-il à la réalisation des objectifs à valeur constitutionnelle ? Oui Non

Dans l'affirmative, veuillez sélectionner les objectifs concernés et veuillez fournir une brève explication dans la case «Remarques» indiquant en quoi cet ou ces objectifs sont réalisés :

Garantir le droit au travail et veiller à assurer l'exercice de ce droit

Promouvoir le dialogue social

Veiller à ce que toute personne puisse vivre dignement et dispose d'un logement approprié

Garantir la protection de l'environnement humain et naturel en œuvrant à l'établissement d'un équilibre durable entre la conservation de la nature, en particulier sa capacité de renouvellement, ainsi que la sauvegarde de la biodiversité, et satisfaction des besoins des générations présentes et futures

S'engager à lutter contre le dérèglement climatique et œuvrer en faveur de la neutralité climatique

Protéger le bien-être des animaux

Garantir l'accès à la culture et le droit à l'épanouissement culturel

Promouvoir la protection du patrimoine culturel

Promouvoir la liberté de la recherche scientifique dans le respect des valeurs d'une société démocratique fondée sur les droits fondamentaux et les libertés publiques

Remarques :

3. Mieux légiférer

Les champs marqués d'un * sont obligatoires

Partie(s) prenante(s) (organismes divers, citoyens,...) consultée(s) : Oui Non

Si oui, laquelle / lesquelles :

Remarques / Observations :

Destinataires du projet :

- Entreprises / Professions libérales :

Oui Non

- Citoyens :

Oui Non

- Administrations :

Oui Non

Le principe « Think small first » est-il respecté ?

(c.-à-d. des exemptions ou dérogations sont-elles prévues suivant la taille de l'entreprise et/ou son secteur d'activité ?)

Oui Non N.a. ¹

Remarques / Observations :

¹ N.a. : non applicable.

Le projet est-il lisible et compréhensible pour le destinataire ? Oui Non

Existe-t-il un texte coordonné ou un guide pratique, mis à jour et publié d'une façon régulière ?

Oui Non

Remarques / Observations :

Le projet a-t-il saisi l'opportunité pour supprimer ou simplifier des régimes d'autorisation et de déclaration existants, ou pour améliorer la qualité des procédures ? Oui Non

Remarques / Observations :

Le projet contient-il une charge administrative ² pour le(s) destinataire(s) ? (un coût imposé pour satisfaire à une obligation d'information émanant du projet ?) Oui Non

Si oui, quel est le coût administratif ³ approximatif total ? (nombre de destinataires x coût administratif par destinataire)

² Il s'agit d'obligations et de formalités administratives imposées aux entreprises et aux citoyens, liées à l'exécution, l'application ou la mise en œuvre d'une loi, d'un règlement grand-ducal, d'une application administrative, d'un règlement ministériel, d'une circulaire, d'une directive, d'un règlement UE ou d'un accord international prévoyant un droit, une interdiction ou une obligation.

³ Coût auquel un destinataire est confronté lorsqu'il répond à une obligation d'information inscrite dans une loi ou un texte d'application de celle-ci (exemple : taxe, coût de salaire, perte de temps ou de congé, coût de déplacement physique, achat de matériel, etc.).

a) Le projet prend-il recours à un échange de données inter-administratif (national ou international) plutôt que de demander l'information au destinataire ? Oui Non N.a.

Si oui, de quelle(s) donnée(s) et/ou administration(s) s'agit-il ?

b) Le projet en question contient-il des dispositions spécifiques concernant la protection des personnes à l'égard du traitement des données à caractère personnel ⁴ ? Oui Non N.a.

Si oui, de quelle(s) donnée(s) et/ou administration(s) s'agit-il ?

⁴ 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. (www.cnpd.public.lu)

Le projet prévoit-il :

- une autorisation tacite en cas de non réponse de l'administration ? Oui Non N.a.
- des délais de réponse à respecter par l'administration ? Oui Non N.a.
- le principe que l'administration ne pourra demander des informations supplémentaires qu'une seule fois ? Oui Non N.a.

Y a-t-il une possibilité de regroupement de formalités et/ou de procédures (p.ex. prévues le cas échéant par un autre texte) ? Oui Non N.a.

Si oui, laquelle :

En cas de transposition de directives communautaires, le principe « la directive, rien que la directive » est-il respecté ? Oui Non N.a.

Sinon, pourquoi ?

Le projet contribue-t-il en général à une :

- a) simplification administrative, et/ou à une** Oui Non
- b) amélioration de la qualité réglementaire ?** Oui Non

Remarques / Observations :

Des heures d'ouverture de guichet, favorables et adaptées aux besoins du/des destinataire(s), seront-elles introduites ? Oui Non N.a.

Y a-t-il une nécessité d'adapter un système informatique auprès de l'Etat (e-Government ou application back-office) Oui Non

Si oui, quel est le délai pour disposer du nouveau système ?

Y a-t-il un besoin en formation du personnel de l'administration concernée ? Oui Non N.a.

Si oui, lequel ?

Remarques / Observations :

4. Egalité des chances

Les champs marqués d'un * sont obligatoires

Le projet est-il :

- principalement centré sur l'égalité des femmes et des hommes ? Oui Non
- positif en matière d'égalité des femmes et des hommes ? Oui Non

Si oui, expliquez de quelle manière :

- neutre en matière d'égalité des femmes et des hommes ? Oui Non

Si oui, expliquez pourquoi :

- négatif en matière d'égalité des femmes et des hommes ? Oui Non

Si oui, expliquez de quelle manière :

Y a-t-il un impact financier différent sur les femmes et les hommes ? Oui Non N.a.

Si oui, expliquez de quelle manière :

5. Projets nécessitant une notification auprès de la Commission européenne

Directive « services » : Le projet introduit-il une exigence en matière d'établissement ou de prestation de services transfrontalière ? Oui Non N.a.

Si oui, veuillez contacter le Ministère de l'Economie en suivant les démarches suivantes :
<https://meco.gouvernement.lu/fr/le-ministere/domaines-activite/services-marche-interieur/notifications-directive-services.html>

Directive « règles techniques » : Le projet introduit-il une exigence ou réglementation technique par rapport à un produit ou à un service de la société de l'information (domaine de la technologie et de l'information)? Oui Non N.a.

Si oui, veuillez contacter l'ILNAS en suivant les démarches suivantes :
<https://portail-qualite.public.lu/content/dam/qualite/publications/normalisation/2017/ilnas-notification-infolyer-web.pdf>

