

N° 8162

CHAMBRE DES DEPUTES

Session ordinaire 2022-2023

PROJET DE LOI

**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**

* * *

Document de dépôt

Dépôt: le 24.2.2023

*

ARRETE GRAND-DUCAL DE DEPOT

Nous HENRI, Grand-Duc de Luxembourg, Duc de Nassau,

Sur le rapport de Notre Ministre des Affaires étrangères et européennes et après délibération du Gouvernement en conseil ;

Arrêtons :

Article unique. Notre ministre des Affaires étrangères et européennes est autorisé à déposer en Notre nom 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 de Lituanie concernant l'échange et la protection réciproque d'informations classifiées, fait à Bruxelles, le 7 décembre 2020.

Palais de Luxembourg, le 3 février 2023

*Le Ministre des Affaires étrangères
et européennes,*

Jean ASSELBORN

HENRI

*

I. Texte du projet de loi	2
II. Exposé des motifs	2
III. Commentaire des articles	4
IV. Fiche d'évaluation d'impact	5
V. Fiche financière	7
VI. Texte de l'accord	8

*

TEXTE DU PROJET DE LOI

Art. unique

Est approuvé 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.

*

EXPOSE DES MOTIFS

Les menaces auxquelles l'Europe est confrontée de nos jours sont très variées et difficilement prévisibles. Parmi les menaces qui pèsent sur sécurité de notre pays, on peut citer, de manière non exhaustive, le terrorisme, les menaces cyber, la prolifération des armes de destruction massive, les conflits régionaux, la déliquescence des Etats et la criminalité organisée. Dans le registre des menaces qui pèsent plus particulièrement sur le patrimoine économique et financier des Etats, il convient aussi de mentionner l'espionnage industriel et technologique.

A cela s'ajoute que la conjugaison de certains de ces éléments pourrait exposer les Etats à une menace hybride. Contrairement à la menace massive et visible du temps de la guerre froide, aucune des nouvelles menaces n'est purement militaire et ne peut être contrée par des moyens purement militaires. A chacune de ces menaces, il faut opposer une combinaison de moyens d'action. Dans ce contexte, la prévention constitue un élément fondamental pour réduire les risques liés aux menaces, en particulier les menaces hybrides.

Au Luxembourg, la loi modifiée du 15 juin 2004 relative à la protection des pièces et aux habilitations de sécurité, s'inscrit précisément dans ce contexte préventif, alors qu'avant l'entrée en vigueur de cette loi, la protection des secrets était essentiellement organisée de manière répressive. Par le biais de cette loi, le législateur accorde aux autorités limitativement énumérées à l'article 5 le droit de procéder à la classification, à la dé-classification et au déclassement de pièces, afin de protéger les intérêts énumérés à l'article 3 de ladite loi.

En cas de transmission de ces pièces à des autorités étrangères, les autorités luxembourgeoises concernées doivent s'assurer de la protection de ces pièces. Il en va de même pour ces autorités étrangères, qui doivent être rassurées quant à la protection par les autorités luxembourgeoises de leurs pièces classifiées, faute de quoi ces échanges ne pourraient s'effectuer. Les accords bilatéraux que le gouvernement a conclus avec de nombreux pays règlent précisément cette question de l'échange et de protection d'informations classifiées.

En conclusion, l'échange et la protection réciproque d'informations classifiées entre le Gouvernement de la République de Lituanie et le Gouvernement du Grand-Duché de Luxembourg sera désormais régi par cet accord, ainsi que par les lois nationales en vigueur dans ces deux Etats, à l'exception des pièces classifiées tombant sous l'empire d'un régime de protection qui leur est propre, généralement dans un cadre multilatéral (p. ex. OTAN, UE).

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 et 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 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 ;
 - 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 ;
 - 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 ;
 - 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 ;
 - 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 ;
 - 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.

*

COMMENTAIRES DES ARTICLES

L'article unique de la loi vise à approuver 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 classifiés, fait à Bruxelles, le 7 décembre 2020 (ci-après « **l'accord** »).

Les premiers articles de l'accord (**articles 1 à 5**) visent à fixer le champ d'application, à établir les définitions des termes utilisés, à établir des équivalences entre les différents niveaux de classification nationaux, à arrêter les règles applicables à l'accès aux informations classifiés et à leur protection, ainsi qu'à déterminer les autorités nationales de sécurité compétentes.

Sont arrêtés ensuite les règles applicables au transfert, à la traduction, à la reproduction, ainsi qu'à la destruction des informations classifiées (**articles 6 à 7**). L'**article 8** porte sur les modalités de conclusion et d'exécution de contrats classifiés (le terme « contrat classifié » étant défini à l'article 2). L'**article 9** prévoit les modalités et conditions relatives aux visites que les représentants d'une des parties peuvent effectuer au sein des installations de l'autre partie.

L'article 10 prévoit la procédure à suivre en cas d'infraction à la sécurité. Enfin, les derniers articles (**articles 11 à 13**) contiennent des dispositions relatives aux coûts, au règlement des litiges, ainsi que les dispositions finales (durée, entrée en vigueur et modification) de l'accord.

*

FICHE D'EVALUATION D'IMPACT

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 de Lituanie concernant l'échange et la protection réciproque d'informations classifiées, fait à Bruxelles, le 7 décembre 2020
Ministère initiateur:	Ministère des Affaires étrangères et européennes
Auteur:	Aurélien Adler ; Daniela Holderer
Tél. :	247-82337; 247-72489
Courriel:	aurelien.adler@mae.etat.lu ; daniela.holderer@mae.etat.lu
Objectif(s) du projet:	Créer le cadre juridique pour l'échange et la protection réciproque d'informations classifiées entre le Luxembourg et la République de Lituanie.
Autre(s) Ministère(s)/Organisme(s)/Commune(s)impliqué(e)(s):	Ministère d'Etat, Service de renseignement de l'Etat, Autorité nationale de sécurité (ANS)
Date:	23 décembre 2022

Mieux légiférer

- Partie(s) prenante(s) (organismes divers, citoyens,...) consultée(s): Oui: Non: ¹
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? Oui: Non: N.a.:²
(c.-à-d. des exemptions ou dérogations sont-elles prévues suivant la taille de l'entreprise et/ou son secteur d'activité?)
Remarques/Observations:

1 Double-click sur la case pour ouvrir la fenêtre permettant de l'activer

2 N.a.: non applicable.

4. 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:
5. 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:
6. Le projet contient-il une charge administrative³ 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 approximatif total? (nombre de destinataires x coût administratif⁴ par destinataire)
7. a) Le projet prend-il recours à un échange de données interadministratif (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? Oui: Non: N.a.:
 Si oui, de quelle(s) donnée(s) et/ou administration(s) s'agit-il?
8. 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.:
9. 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:
10. En cas de transposition de directives européennes, le principe « la directive, rien que la directive » est-il respecté? Oui: Non: N.a.:
 Sinon, pourquoi?
11. 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:

3 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 oeuvre 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.

4 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...).

12. Des heures d'ouverture de guichet, favorables et adaptées aux besoins du/des destinataire(s), seront-elles introduites? Oui: Non: N.a.:
Remarques/Observations:
13. 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?
14. Y a-t-il un besoin en formation du personnel de l'administration concernée? Oui: Non: N.a.:
Si oui, lequel?
Remarques/Observations:

Egalité des chances

15. 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: Les questions d'égalité des femmes et des hommes ne sont pas touchées par l'échange et la protection réciproque d'informations classifiées.
 - négatif en matière d'égalité des femmes et des hommes? Oui: Non:
Si oui, expliquez de quelle manière:
16. Y a-t-il un impact financier différent sur les femmes et les hommes ? Oui: Non: N.a.:
Si oui, expliquez de quelle manière:

Directive « services »

17. Le projet introduit-il une exigence relative à la liberté d'établissement soumise à évaluation⁵ ? Oui: Non: N.a.:
Si oui, veuillez annexer le formulaire A, disponible au site Internet du Ministère de l'Economie:
www.eco.public.lu/attributions/dg2/d_consommation/d_march_int_rieur/Services/index.html
18. Le projet introduit-il une exigence relative à la libre prestation de services transfrontaliers⁶ ? Oui: Non: N.a.:
Si oui, veuillez annexer le formulaire B, disponible au site Internet du Ministère de l'Economie:
www.eco.public.lu/attributions/dg2/d_consommation/d_march_int_rieur/Services/index.html

*

FICHE FINANCIERE

Le présent projet de loi devrait avoir un impact neutre, étant donné qu'il ne prévoit pas de mesures à charge du budget de l'Etat.

*

⁵ Article 15, paragraphe 2 de la directive « services » (cf. Note explicative, p. 10-11)

⁶ Article 16, paragraphe 1, troisième alinéa et paragraphe 3, première phrase de la directive « services » (cf. Note explicative, p.10-11)

TEXTE DE L'ACCORD

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

Le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la République de Lituanie et (ci-après dénommés les « Parties » ou individuellement la « Partie »),

souhaitant développer et renforcer leur coopération politique, économique, technologique et militaire,

désirant promouvoir la confiance mutuelle,

reconnaissant qu'une coopération efficace peut exiger l'échange d'informations classifiées entre les Parties,

désirant établir un ensemble de règles régissant la protection réciproque d'informations classifiées, produites ou échangées dans le cadre d'une coopération entre les Parties,

CONVIENNENT ce qui suit :

Article 1

Objet et champ d'application

(1) Le présent Accord a pour but de garantir la protection des informations classifiées (telles que définies ci-après) échangées ou produites dans le cadre de la coopération entre les Parties et d'établir un ensemble de règles et de procédures régissant leur protection réciproque.

(2) Le présent Accord est applicable à l'ensemble des activités, contrats ou accords impliquant des informations classifiées qui seront menés ou conclus entre les Parties à l'avenir ou ont été menés ou conclus avant la date d'entrée en vigueur des présentes.

Article 2

Définitions

Aux fins du présent Accord :

- (1) Une « **infraction à la sécurité** » désigne tout acte ou omission contraire aux lois et réglementations nationales en vigueur ou au présent Accord, susceptible d'entraîner la divulgation, la perte, la destruction, le détournement ou tout autre type de compromission d'informations classifiées.
- (2) Un « **contrat classifié** » désigne un contrat, un contrat de sous-traitance ou un projet dont la mise en œuvre nécessite l'accès aux informations classifiées ou la production de telles informations.
- (3) Les « **informations classifiées** » désignent toute information, quelle qu'en soit la forme, la nature ou le mode de transfert, produite ou en cours de production et qui, à des fins de sécurité nationale et conformément aux lois et réglementations nationales, doit être protégée contre toute infraction à la sécurité et a été ainsi désignée par l'attribution d'un niveau de classification de sécurité.
- (4) Une « **autorité compétente** » désigne toute autorité gouvernementale, autre que l'autorité nationale de sécurité, qui, conformément aux lois et réglementations nationales en vigueur, est chargée de l'exécution des tâches déléguées en vertu du présent Accord.

- (5) Un « **contractant** » désigne toute personne physique ou morale dotée de la capacité juridique de conclure des contrats classifiés conformément aux modalités du présent Accord.
- (6) Une « **habilitation de sécurité d'établissement** » renvoie à une décision positive rendue par l'autorité nationale de sécurité, établie sous la forme d'un document confirmant qu'un sous-traitant est autorisé à exécuter des actions liées à l'utilisation d'informations classifiées jusqu'à un certain niveau de classification de sécurité, conformément aux lois et réglementations nationales.
- (7) « **L'Autorité nationale de sécurité** » désigne l'autorité nationale qui, conformément aux lois et réglementations nationales, est chargée de superviser la mise en œuvre du présent Accord. Ces autorités sont énumérées à l'article 5 du présent Accord.
- (8) Le « **principe du besoin d'en connaître** » renvoie à la nécessité d'accéder à des informations classifiées dans le cadre de devoirs officiels et/ou d'une mission officielle concrète.
- (9) La « **Partie d'origine** » désigne la Partie, en ce compris toute instance de sa juridiction, qui fournit des informations classifiées conformément aux lois et réglementations nationales.
- (10) Une « **habilitation de sécurité individuelle** » renvoie à une décision positive de l'autorité nationale de sécurité ou de l'autorité compétente, établie sous la forme d'un document attestant de la loyauté et la fiabilité d'une personne ainsi que d'autres aspects relatifs à la sécurité, conformément aux lois et réglementations nationales, et octroyant l'accès aux informations classifiées jusqu'à un certain niveau de classification de sécurité.
- (11) La « **Partie destinataire** » désigne la Partie, en ce compris toute instance relevant de sa juridiction, à laquelle sont transmises des informations classifiées de la Partie d'origine, conformément aux lois et réglementations nationales.
- (12) Une « **tierce partie** » désigne tout État, y compris toute instance publique ou privée, organisation internationale, personne physique ou morale, qui n'est pas l'une des Parties au présent Accord.

Article 3

Niveaux de sécurité

- (1) Les Parties reconnaissent que les niveaux de sécurité suivants sont équivalents et se correspondent comme suit :

<i>Pour le Grand-Duché de Luxembourg</i>	<i>Equivalent en anglais</i>	<i>Pour la République de Lituanie</i>
TRÈS SECRET LUX	TOP SECRET	VISISKAI SLAPTAI
SECRET LUX	SECRET	SLAPTAI
CONFIDENTIEL LUX	CONFIDENTIAL	KONFIDENCIALIAI
RESTREINT LUX	RESTRICTED	RIBOTO NAUDOJIMO

- (2) La Partie destinataire attribuera à l'information classifiée reçue le niveau de sécurité équivalent qui lui est propre. La Partie destinataire ne pourra déclassifier les informations classifiées reçues ou altérer leur niveau de sécurité sans l'accord écrit préalable de la Partie d'origine.
- (3) La Partie d'origine informera la Partie destinataire, par écrit et sans délai, de toute modification apportée au niveau de classification des informations échangées.

Article 4

Protection des informations classifiées

- (1) Conformément à leurs lois et réglementations nationales en vigueur, les Parties s'engagent à mettre en œuvre toutes les mesures appropriées afin de protéger les informations classifiées généralement produites ou échangées en vertu du présent Accord. Elles attribueront auxdites informations

classifiées un niveau de protection au minimum équivalent à celui qui est accordé à leurs informations classifiées nationales de même niveau de classification de sécurité, conformément aux dispositions de l'article 3.

(2) L'accès aux informations classifiées sera exclusivement réservé aux personnes qui ont besoin de connaître de telles informations et qui disposent de l'autorisation appropriée, en vertu des lois et réglementations nationales en vigueur, pour accéder à des informations classifiées d'un niveau de classification de sécurité équivalent.

(3) La Partie destinataire s'engage :

- a) à ne délivrer aucune information classifiée à une tierce partie sans l'accord écrit de l'autorité nationale de sécurité de la Partie d'origine ;
- b) à ne pas utiliser d'informations classifiées à d'autres fins que celles auxquelles elles lui ont été transmises ;
- c) à préserver les droits privés, tels que les droits de brevets, les droits d'auteur ou les secrets commerciaux associés à des informations classifiées.

(4) Les Parties reconnaissent mutuellement leurs habilitations de sécurité individuelle et d'établissement délivrées conformément aux lois et réglementations nationales en vigueur.

(5) Dans le cadre du présent Accord, les autorités nationales de sécurité se tiennent mutuellement informées sans délai de toute révocation d'habilitation de sécurité individuelle et d'établissement ou de toute modification apportée au niveau de classification de sécurité.

(6) Si tout autre Accord conclu entre les Parties comporte des règles plus strictes eu égard à l'échange ou à la protection des informations classifiées, de telles règles s'appliquent.

Article 5

Autorités nationales de sécurité

(1) Les autorités nationales de sécurité des Parties sont :

<i>Pour le Grand-Duché de Luxembourg</i>	<i>Pour la République de Lituanie</i>
Service de renseignement de l'État Autorité nationale de sécurité	Commission for secrets protection co-ordination

(2) Les Parties se tiennent mutuellement informées, par la voie diplomatique, de toute modification apportée à leurs autorités nationales de sécurité.

(3) Sur demande, les autorités nationales de sécurité se tiennent mutuellement informées de leurs lois et réglementations nationales en vigueur en matière de protection des informations classifiées et/ou de toute modification significative qui leur est apportée.

(4) Sur demande, les autorités nationales de sécurité se communiquent mutuellement les informations se rapportant aux autorités compétentes chargées de l'exécution des tâches déléguées en vertu des présentes.

(5) Afin de garantir une coopération efficace dans l'exécution des présentes, les autorités nationales de sécurité pourront organiser des consultations si l'une d'entre elles en formule la demande.

(6) En vue d'appliquer et de maintenir des normes de sécurité similaires, les autorités nationales de sécurité se tiennent mutuellement informées, sur demande, des normes, procédures et pratiques de sécurité appliquées par chaque Partie en matière de protection des informations classifiées.

(7) Les autorités nationales de sécurité respectives pourront conclure des modalités de mise en œuvre sur la base du présent Accord.

(8) Sur demande, et conformément aux lois et réglementations nationales en vigueur, les autorités compétentes s'assisteront mutuellement dans le cadre de la réalisation des procédures de vérification.

(9) Dans le cadre du présent Accord, les autorités nationales de sécurité se tiennent mutuellement informées sans délai de toute modification apportée aux habilitations de sécurité individuelle ou d'établissement, notamment en cas de révocation ou de modification du niveau de classification.

Article 6

Transfert d'informations classifiées

(1) En règle générale, les informations classifiées seront transférées par des coursiers diplomatiques ou militaires ou par tout autre moyen approuvé préalablement par les autorités compétentes des Parties. La Partie destinataire confirmera par écrit la réception d'informations identifiées comme étant de niveau SLAPTAI/SECRET LUX/SECRET ou d'un niveau supérieur.

(2) Les informations classifiées pourront être transmises par le biais de systèmes, de réseaux ou d'autres moyens électromagnétiques de communication protégés, approuvés conformément aux lois et réglementations nationales en vigueur et assortis d'un certificat dûment établi.

(3) D'autres moyens ne pourront être utilisés pour le transfert d'informations classifiées que s'ils ont été approuvés par les autorités nationales de sécurité des Parties.

Article 7

Traduction, reproduction, destruction d'informations classifiées

(1) La traduction ou la reproduction d'informations classifiées SLAPTAI/SECRET LUX/SECRET sont autorisées uniquement avec l'accord écrit de la Partie d'origine.

(2) Toutes les traductions d'informations classifiées seront effectuées par des personnes disposant d'une habilitation de sécurité individuelle appropriée. Ces traductions porteront l'ensemble des marquages de classification de sécurité originaux.

(3) Lors de la reproduction d'informations classifiées, tous les marquages de classification des informations originales, ainsi que les instructions supplémentaires relatives à leur traitement, seront également reproduits ou indiqués sur chaque exemplaire. Les informations ainsi reproduites sont placées sous le même niveau de contrôle que les informations originales. Le nombre de copies est limité à celui requis pour un usage officiel.

(4) Les informations classifiées identifiées comme étant de niveau SLAPTAI/SECRET LUX/SECRET ou d'un niveau inférieur pourront être détruites dès lors qu'elles ne sont plus nécessaires, conformément aux lois et réglementations nationales en vigueur. Les informations classifiées seront détruites de la façon requise pour empêcher leur reconstruction en tout ou partie. Un exemplaire du rapport relatif à la destruction desdites informations classifiées sera remis à la Partie d'origine.

(5) Les informations classifiées VISISKAI SLAPTAI/ TRES SECRET LUX/TOP SECRET ne seront pas détruites. En règle générale, celles-ci doivent être renvoyées à la Partie d'origine.

(6) Dans le cas d'une situation d'urgence rendant impossible la protection et le renvoi des informations classifiées produites ou échangées en vertu du présent Accord, les informations classifiées seront détruites immédiatement. La Partie destinataire informera dès que possible la Partie d'origine de la destruction des informations classifiées.

*Article 8****Contrats classifiés***

(1) Les contrats classifiés sont conclus et exécutés conformément aux lois et réglementations nationales de chaque Partie. Sur demande, l'autorité nationale de sécurité de chaque Partie fournira les informations attestant de la délivrance à un sous-traitant proposé et à ses employés respectifs d'une habilitation de sécurité appropriée correspondant au niveau de classification de sécurité des informations classifiées concernées. Si le sous-traitant proposé ou l'un de ses employés respectifs ne détiennent pas d'habilitation de sécurité appropriée, l'autorité nationale de sécurité peut demander que ce sous-traitant, ou ses employés respectifs, obtiennent une telle habilitation. Une habilitation de sécurité appropriée sera délivrée au sous-traitant ou à ses employés respectifs avant la conclusion du contrat classifié.

(2) Il incombe à l'autorité nationale de sécurité de la Partie dont le territoire est visé par l'exécution du contrat classifié de prescrire et d'administrer les mesures de sécurité applicables audit contrat selon les mêmes normes et les mêmes exigences que celles qui régissent la protection de ses propres contrats classifiés.

(3) Des instructions relatives à la sécurité feront partie intégrante de chaque contrat classifié. Ces instructions couvriront notamment les aspects suivants :

- a) les niveaux de classification de sécurité des informations devant être produites dans le cadre du contrat classifié, et une liste des informations classifiées devant être transmises au sous-traitant ;
- b) l'obligation pour le sous-traitant de restreindre la divulgation des informations classifiées aux personnes qui, conformément aux lois et réglementations nationales en vigueur, sont autorisées à accéder à des informations classifiées d'un niveau de sécurité équivalent, ont besoin de connaître de telles informations et sont employées ou engagées dans l'exécution du contrat classifié ;
- c) la procédure relative à la communication des modifications apportées aux niveaux de classification des informations ;
- d) les voies de communication et les moyens de transmission employés pour le transfert d'informations classifiées ;
- e) l'obligation d'utiliser les informations classifiées en vertu d'un contrat classifié aux seules fins liées à l'objet d'un tel contrat ;
- f) le strict respect des procédures applicables à la destruction d'informations classifiées ;
- g) l'obligation de signaler toute infraction à la sécurité avérée ou suspectée ;
- h) la procédure applicable à l'approbation des visites ou inspections des sites du sous-traitant.

(4) Pour tout contrat classifié, une copie des instructions de sécurité de projet sera transmise à l'autorité nationale de sécurité de la Partie sur le territoire de laquelle le contrat doit être exécuté en vue de garantir une supervision et un contrôle de sécurité appropriés.

(5) Sur demande, pour les contrats impliquant des informations classifiées RIBOTO NAUDOJIMO/ RESTREINT LUX/RESTRICTED, aucune habilitation de sécurité d'établissement ne sera délivrée. L'autorité nationale de sécurité de chaque Partie fournira par écrit les informations attestant qu'un sous-traitant proposé satisfait aux exigences nationales relatives à la protection d'informations classifiées identifiées comme étant de niveau RIBOTO NAUDOJIMO / RESTREINT LUX / RESTRICTED.

*Article 9****Visites***

(1) Les visites impliquant l'accès à des informations classifiées seront soumises à l'autorisation de l'autorité nationale de sécurité ou de l'autorité compétente de la Partie objet de la visite.

- (2) En règle générale, toute demande de visite doit être soumise au minimum deux semaines avant la visite.
- (3) Toute demande de visite comportera les informations suivantes :
- a) les noms et prénoms, la date et le lieu de naissance, le numéro de passeport ou de la carte d'identité du visiteur ;
 - b) la nationalité du visiteur ;
 - c) le titre du poste du visiteur et le nom de l'organisation qu'il représente ;
 - d) le certificat attestant de la délivrance d'une habilitation de sécurité individuelle au visiteur, ainsi que le niveau et la date d'expiration de cette habilitation ;
 - e) le but de la visite ainsi que le programme de travail proposé et la date prévue ;
 - f) les noms et les référents des organisations et sites qui doivent être visités.
- (4) Chacune des Parties s'engage à garantir la protection des données personnelles des visiteurs conformément aux lois et réglementations nationales en vigueur.
- (5) Les autorités nationales de sécurité ou les autorités compétentes pourront établir des listes répertoriant le personnel autorisé à procéder à de multiples visites relativement à tout projet ou programme spécifique, conformément à des modalités convenues par les Parties.

Article 10

Infraction à la sécurité

- (1) En cas d'infraction à la sécurité, l'autorité nationale de sécurité de la Partie concernée par l'infraction informera l'autorité nationale de sécurité de l'autre Partie sans délai et veillera à mener une enquête appropriée. Si nécessaire, l'autre Partie coopèrera à cette enquête.
- (2) L'autre Partie sera tenue informée des résultats de l'enquête et recevra le rapport final sur les raisons et l'étendue des dommages qui ont été causés.

Article 11

Coûts

Chacune des Parties assume les frais engagés du fait de l'exécution de ses obligations en vertu du présent Accord.

Article 12

Règlement des litiges

Tout litige quant à l'interprétation ou l'application du présent Accord sera exclusivement résolu par voie de consultations entre les Parties.

Article 13

Dispositions finales

- (1) Le présent Accord est conclu pour une durée indéterminée.
- (2) Le présent Accord prend effet le premier jour qui suit la réception de la dernière des notifications, transmise par écrit et par voie diplomatique, confirmant le respect de l'ensemble des exigences légales nationales des deux Parties, telles que requises à cette fin.

(3) Le présent Accord peut être modifié d'un commun accord, par écrit, par les deux Parties. Les modifications ainsi apportées font partie intégrante du présent Accord et prennent effet conformément aux dispositions prévues au paragraphe 2 du présent article.

(4) Chaque Partie peut mettre fin au présent Accord via les voies diplomatiques en informant l'autre Partie au moyen d'une notification écrite. Une telle résiliation prend effet six mois après la date de réception de cette notification. Dans un tel cas, toutes les informations classifiées échangées seront restituées à la Partie d'origine. Si les informations classifiées ne peuvent être restituées, elles continueront d'être protégées conformément aux dispositions du présent accord, jusqu'à ce que la Partie d'origine dispense la Partie destinataire de cette obligation.

FAIT à Bruxelles, le 7 décembre 2020, en deux exemplaires originaux, chacun en langues française, lituanienne et anglaise et, tous les textes faisant également foi. Dans le cas d'un désaccord quant à l'interprétation des dispositions du présent Accord, le texte anglais prévaut.

*Pour le Gouvernement du
Grand-Duché de Luxembourg*

*Pour le Gouvernement de la
République de Lituanie*

*

AGREEMENT

between the Government of the Republic of Lithuania and the Government of the Grand Duchy of Luxembourg on exchange and mutual protection of Classified Information

The Government of the Republic of Lithuania and the Government of the Grand Duchy of Luxembourg (hereinafter referred together as the „Parties“ or individually as the „Party“),

wishing to further develop and strengthen their political, economic, technological and military co-operation,

desiring to promote mutual trust and confidence,

realizing that effective co-operation may require exchange of Classified Information between the Parties,

desiring to establish a set of rules regulating the mutual protection of Classified Information exchanged or generated in the course of the cooperation between the Parties,

HAVE AGREED as follows:

Article 1

Objective and scope

(1) The objective of this Agreement is to ensure protection of Classified Information (as defined below) that is exchanged or created in the process of co-operation between the Parties and to establish specific rules and procedures governing its mutual protection.

(2) This Agreement shall be applicable to any activities, contracts or agreements involving Classified Information, that will be conducted or concluded between the Parties in future or have been conducted or concluded until entering into force of this Agreement.

*Article 2***Definitions**

For the purpose of this Agreement:

- (1) **„Breach of Security“** means any act or an omission contrary to the national laws and regulations in force or this Agreement, the result of which may lead to disclosure, loss, destruction, misappropriation or any other type of compromise of Classified Information.
- (2) **„Classified Contract“** means a contract, a sub-contract or a project, the implementation of which requires access to or generation of Classified Information.
- (3) **„Classified Information“** means the information, regardless of the form, nature or method of transfer, whether prepared or being prepared and which in the interest of national security and in accordance with the national laws and regulations, requires protection against Breach of security and has been so designated by a security classification level.
- (4) **„Competent Authority“** means any state authority except National Security Authority, which in accordance with national laws and regulations in force is responsible for the implementation of delegated tasks under this Agreement.
- (5) **„Contractor“** means an individual or a legal entity possessing the legal capacity to conclude a Classified Contract under the provisions of this Agreement.
- (6) **„Facility Security Clearance“** means a positive determination of the National Security Authority or Competent Authority in the form of a document that confirms that a Contractor is authorized to execute actions related to the use of Classified Information up to a certain security classification level in accordance with national laws and regulations.
- (7) **„National Security Authority“** means the national authority which in accordance with national laws and regulations is responsible for the supervision of the implementation of this Agreement. Such authorities are listed in Article 5 of this Agreement.
- (8) **„Need-to-know“ principle** means the necessity to have access to Classified Information in connection with official duties and/or for the performance of a concrete official task.
- (9) **„Originating Party“** means the Party, including any entity which provides Classified Information, in accordance with national laws and regulations.
- (10) **„Personnel Security Clearance“** means a positive determination of the National Security Authority or Competent Authority in the form of a document which confirms the loyalty and trustworthiness of an individual as well as other security aspects in accordance with national laws and regulations, which grants an access to Classified Information up to a certain security classification level.
- (11) **„Receiving Party“** means the Party, including any entity under its jurisdiction, to which Classified Information of the Originating Party is transmitted, in accordance with national laws and regulations.
- (12) **„Third Party“** means any state, including any public or private entities, international organization, legal entity, or individual which is not a Party to this Agreement.

*Article 3***Security Classifications**

- (1) The Parties agree that the following Security Classifications are equivalent and correspond to one another as follows:

<i>For the Republic of Lithuania</i>	<i>Equivalent in English</i>	<i>For the Grand Duchy of Luxembourg</i>
VISIŠKAI SLAPTAI	TOP SECRET	TRES SECRET LUX
SLAPTAI	SECRET	SECRET LUX
KONFIDENCIALIAI	CONFIDENTIAL	CONFIDENTIEL LUX
RIBOTO NAUDOJIMO	RESTRICTED	RESTREINT LUX

(2) The Receiving Party shall mark the received Classified Information with its own equivalent security classification marking. The Receiving Party shall not declassify received Classified Information or alter its Security Classification level without the prior written consent of the Originating Party.

(3) The Originating Party shall inform in writing the Receiving Party of any changes in classification of the exchanged information without delay.

Article 4

Protection of Classified Information

(1) In compliance with their national laws and regulations in force, the Parties shall implement all appropriate measures for the protection of Classified Information, which is commonly generated or exchanged under this Agreement. At least the same level of protection shall be assigned to such Classified Information as is provided for the national Classified Information of the equivalent corresponding security classification marking as laid down in Article 3.

(2) Access to Classified Information shall be granted only to persons on a Need-to-Know basis who are authorized in accordance with the national laws and regulations in force to have access to Classified Information of the equivalent Security Classification Level.

(3) The Receiving Party is obligated:

- a) not to disclose Classified Information to a Third Party without a prior written consent of the National Security Authority of the Originating Party;
- b) not to use Classified Information for other purposes than those it has been provided for,
- c) to guarantee the private rights such as patent rights, copyrights or trade secrets that are involved in Classified Information.

(4) The Parties mutually recognize the Personnel Security Clearance and Facility Security Clearance Certificates, released in accordance with the national laws and regulations in force.

(5) Within the scope of this Agreement, the National Security Authorities shall inform each other without delay about revocation of Personnel and Facility Security Clearances or the alteration of the security classification level.

(6) If any other Agreement concluded between the Parties contains stricter regulations regarding the exchange or protection of Classified Information, these regulations shall apply.

Article 5

National Security Authorities

(1) The National Security Authorities of the Parties are:

<i>For the Republic of Lithuania</i>	<i>For the Grand Duchy of Luxembourg</i>
Commission for secrets protection co-ordination	Service de renseignement de l'Etat Autorité nationale de Sécurité

(2) The Parties shall notify each other through diplomatic channels of any subsequent changes of their National Security Authorities.

(3) Upon request, the National Security Authorities shall inform each other of the national laws and regulations in force regulating the protection of Classified Information and/or any significant amendments thereto.

(4) Upon request the National Security Authorities shall notify each other about Competent Authorities that are responsible for the implementation of delegated tasks under this Agreement.

- (5) In order to ensure close co-operation in the implementation of the present Agreement, the National Security Authorities may hold consultations at the request made by one of them.
- (6) In order to achieve and maintain comparable standards of security, the National Security Authorities shall, on request, provide each other with information about the security standards, procedures and practices for protection of Classified Information employed by the respective Party.
- (7) The respective National Security Authorities may conclude implementing arrangements on the basis of this Agreement.
- (8) The Competent Authorities shall assist each other upon request and in accordance with the national laws and regulations in force in carrying out vetting procedures.
- (9) Within the scope of this Agreement, the National Security Authorities shall inform each other without delay about any alteration with regard to Personnel Security Clearances or Facility Security Clearances, in particular about their revocation or alteration of the classification level.

Article 6

Transfer of Classified Information

- (1) As a rule, Classified Information shall be transferred by means of diplomatic or military couriers or by other means approved in advance by the Competent Authorities of the Parties. The Receiving Party shall confirm in writing the receipt of Classified Information marked SLAPTAI/SECRET LUX/SECRET and above.
- (2) Classified Information may be transmitted via protected telecommunication systems, networks or other electromagnetic means approved in accordance with national laws and regulations in force and holding a duly issued certificate.
- (3) Other approved means of transfer of Classified Information may only be used if agreed upon between the National Security Authorities of the Parties.

Article 7

Translation, reproduction, destruction of Classified Information

- (1) Classified Information marked SLAPTAI/SECRET LUX/SECRET and above shall be translated or reproduced only by written permission of the Originating Party.
- (2) All translations of Classified Information shall be made by individuals who hold an appropriate Personnel Security Clearance. Such translation shall bear all original security classification markings.
- (3) When Classified Information is reproduced, all original classification markings and additional handling instructions thereon shall also be reproduced or marked on each copy. Such reproduced Classified Information shall be placed under the same control as the original Classified Information. The number of copies shall be limited to that required for official purposes.
- (4) Classified Information marked SLAPTAI/SECRET LUX/SECRET and below may be destroyed after it is no longer needed in accordance with national laws and regulations in force. The Classified Information shall be destroyed as to prevent its reconstruction in whole or in part. The copy of the report on destruction of such Classified Information shall be delivered to the Originating Party.
- (5) Classified Information marked VISIŠKAI SLAPTAI/ TRES SECRET LUX/TOP SECRET shall not be destroyed. As a rule, it shall be returned to the Originating Party.

(6) In case of emergency, which makes it impossible to protect and return Classified Information generated or transferred according to the present Agreement, the Classified Information shall be destroyed immediately. The Receiving Party shall notify the Originating Party on destruction of such Classified Information as soon as possible.

Article 8

Classified Contracts

(1) Classified Contracts shall be concluded and implemented in accordance with national laws and regulations of each Party. Upon request the National Security Authority of each Party shall furnish information whether a proposed Contractor and its respective employees has been issued an appropriate security clearance, corresponding to the security classification of the Classified Information to be handled. If the proposed Contractor or its respective employees does not hold an appropriate security clearance, the National Security Authority may request for that Contractor or its respective employees to be security cleared. An appropriate security clearance shall be issued to the Contractor or its respective employees before the Classified Contract is concluded.

(2) The National Security Authority of the Party in which the Classified Contract is to be performed, shall assume the responsibility for prescribing and administering security measures for the Classified Contract under the same standards and requirements that govern the protection of its own Classified Contracts.

(3) Security instructions shall be an integral part of each Classified Contract. These security instructions shall include the following aspects:

- a) security classification levels of the information that will be generated in the course of Classified Contract, and list of Classified Information that will be transmitted to the Contractor;
- b) an obligation that the Contractor shall disclose the Classified Information only to a person who is authorized in accordance with the national laws and regulations in force to have access to Classified Information of the equivalent security classification level, who has a „Need-to-know“ and who is employed or engaged in the carrying out of the Classified Contract;
- c) procedure for the communication of changes in the classification of information;
- d) communication channels and means for transmission of Classified Information ;
- e) an obligation to use the Classified Information under the Classified Contract only for the purposes related to the subject matter of the Classified Contract;
- f) strict adherence to the procedures for destruction of the Classified Information;
- g) an obligation to notify any actual or suspected Breach of security;
- h) the procedure for the approval of visits or inspection to facilities of the Contractor.

(4) Copy of the Project Security Instruction of any Classified Contract shall be forwarded to the National Security Authority of the Party where the classified contract is to be performed to allow adequate security supervision and control.

(5) Upon request, for contracts involving Classified Information RIBOTO NAUDOJIMO/ RESTREINT LUX/RESTRICTED no Facility Security Clearance will be issued. The National Security Authority of each Party shall furnish information in writing declaring whether a proposed Contractor meets the national requirements for protection of Classified Information marked RIBOTO NAUDOJIMO/ RESTREINT LUX/RESTRICTED.

Article 9

Visits

(1) Visits that require access to Classified Information shall be allowed only with a written permission issued by the National Security Authority or Competent Authority of the Party to be visited.

- (2) As a rule, the request for visit shall be sent at least two weeks before the visit.
- (3) The request for visit shall contain the following information:
 - a) visitors first and last names, date and place of birth, passport or identification document number;
 - b) citizenship of the visitor;
 - c) position title of the visitor and name of the organization he represents;
 - d) certification of Personnel Security Clearance of the visitor, its level and validity;
 - e) purpose, proposed working program and planned date of the visit;
 - f) names and points of contacts of the organizations and facilities requested to be visited.
- (4) Each Party shall guarantee protection of personal data of the visitors, according to the national laws and regulations in force.
- (5) National Security Authorities or Competent Authorities may draw up lists of personnel authorized to make multiple visits in respect of any particular project or program in accordance with the terms and conditions commonly agreed.

Article 10

Breach of Security

- (1) In case of a Breach of Security, the National Security Authority of the Party in which a Breach of Security occurred shall inform the National Security Authority of the other Party immediately and shall ensure the appropriate investigation. The other Party shall, if required, cooperate in the investigation.
- (2) The other Party shall be informed of the results of the investigation and shall receive the final report on the reasons and extent of damage caused.

Article 11

Costs

Each Party shall bear the costs incurred in the course of implementing its obligations under this Agreement.

Article 12

Settlement of Disputes

Any dispute regarding the interpretation or application of this Agreement shall be exclusively settled through consultations between the Parties.

Article 13

Final Provisions

- (1) This Agreement is concluded for an indefinite period of time.
- (2) The present Agreement shall enter into force on the first day following the receipt of the last notification, in writing and through diplomatic channels, stating that all the national legal requirements of both Parties necessary to that effect have been fulfilled.
- (3) This Agreement may be amended on the basis of mutual written consent by both Parties. Such amendments are integral part of this Agreement and shall enter into force in accordance with Paragraph 2 of this Article.

(4) Each Party may terminate this Agreement through diplomatic channels by written notice forwarded to the other Party. The termination shall enter into force six months after the date of receipt of the notification. In such case, all exchanged classified information shall be returned to the Originating Party. If the exchanged Classified Information could not be returned, it shall continue to be protected in accordance with the provisions of this Agreement, until the Originating Party dispenses the Receiving Party from this obligation.

DONE at Brussels, on the 7th of December 2020, in three original copies, each in the Lithuanian, English and French languages, and all texts being equally authentic. In case of any divergence of interpretation, the English language text shall prevail.

*For the Government of the
Republic of Lithuania*

*For the Government of the
Grand Duchy of Luxembourg*

*

AGREEMENT

between the Government of the Grand Duchy of Luxembourg and the Government of the Republic of Lithuania on exchange and mutual protection of Classified Information

The Government of the Grand Duchy of Luxembourg and the Government of the Republic of Lithuania (hereinafter referred together as the „Parties“ or individually as the „Party“),

wishing to further develop and strengthen their political, economic, technological and military co-operation,

desiring to promote mutual trust and confidence,

realizing that effective co-operation may require exchange of Classified Information between the Parties,

desiring to establish a set of rules regulating the mutual protection of Classified Information exchanged or generated in the course of the cooperation between the Parties,

HAVE AGREED as follows:

Article 1

Objective and scope

(1) The objective of this Agreement is to ensure protection of Classified Information (as defined below) that is exchanged or created in the process of co-operation between the Parties and to establish specific rules and procedures governing its mutual protection.

(2) This Agreement shall be applicable to any activities, contracts or agreements involving Classified Information, that will be conducted or concluded between the Parties in future or have been conducted or concluded until entering into force of this Agreement.

Article 2

Definitions

For the purpose of this Agreement:

- (1) „**Breach of Security**“ means any act or an omission contrary to the national laws and regulations in force or this Agreement, the result of which may lead to disclosure, loss, destruction, misappropriation or any other type of compromise of Classified Information.

- (2) „**Classified Contract**“ means a contract, a sub-contract or a project, the implementation of which requires access to or generation of Classified Information.
- (3) „**Classified Information**“ means the information, regardless of the form, nature or method of transfer, whether prepared or being prepared and which in the interest of national security and in accordance with the national laws and regulations, requires protection against Breach of security and has been so designated by a security classification level.
- (4) „**Competent Authority**“ means any state authority except National Security Authority, which in accordance with national laws and regulations in force is responsible for the implementation of delegated tasks under this Agreement.
- (5) „**Contractor**“ means an individual or a legal entity possessing the legal capacity to conclude a Classified Contract under the provisions of this Agreement.
- (6) „**Facility Security Clearance**“ means a positive determination of the National Security Authority or Competent Authority in the form of a document that confirms that a Contractor is authorized to execute actions related to the use of Classified Information up to a certain security classification level in accordance with national laws and regulations.
- (7) „**National Security Authority**“ means the national authority which in accordance with national laws and regulations is responsible for the supervision of the implementation of this Agreement. Such authorities are listed in Article 5 of this Agreement.
- (8) „**Need-to-know principle**“ means the necessity to have access to Classified Information in connection with official duties and/or for the performance of a concrete official task.
- (9) „**Originating Party**“ means the Party, including any entity which provides Classified Information, in accordance with national laws and regulations.
- (10) „**Personnel Security Clearance**“ means a positive determination of the National Security Authority or Competent Authority in the form of a document which confirms the loyalty and trustworthiness of an individual as well as other security aspects in accordance with national laws and regulations, which grants an access to Classified Information up to a certain security classification level.
- (11) „**Receiving Party**“ means the Party, including any entity under its jurisdiction, to which Classified Information of the Originating Party is transmitted, in accordance with national laws and regulations.
- (12) „**Third Party**“ means any state, including any public or private entities, international organization, legal entity, or individual which is not a Party to this Agreement.

Article 3

Security Classifications

- (1) The Parties agree that the following Security Classifications are equivalent and correspond to one another as follows:

<i>For the Grand Duchy of Luxembourg</i>	<i>Equivalent in English</i>	<i>For the Republic of Lithuania</i>
TRES SECRET LUX	TOP SECRET	VISIŠKAI SLAPTAI
SECRET LUX	SECRET	SLAPTAI
CONFIDENTIEL LUX	CONFIDENTIAL	KONFIDENCIALIAI
RESTREINT LUX	RESTRICTED	RIBOTO NAUDOJIMO

- (2) The Receiving Party shall mark the received Classified Information with its own equivalent security classification marking. The Receiving Party shall not declassify received Classified Information or alter its Security Classification level without the prior written consent of the Originating Party.
- (3) The Originating Party shall inform in writing the Receiving Party of any changes in classification of the exchanged information without delay.

*Article 4****Protection of Classified Information***

- (1) In compliance with their national laws and regulations in force, the Parties shall implement all appropriate measures for the protection of Classified Information, which is commonly generated or exchanged under this Agreement. At least the same level of protection shall be assigned to such Classified Information as is provided for the national Classified Information of the equivalent corresponding security classification marking as laid down in Article 3.
- (2) Access to Classified Information shall be granted only to persons on a Need-to-Know basis who are authorized in accordance with the national laws and regulations in force to have access to Classified Information of the equivalent Security Classification Level.
- (3) The Receiving Party is obligated:
- a) not to disclose Classified Information to a Third Party without a prior written consent of the National Security Authority of the Originating Party;
 - b) not to use Classified Information for other purposes than those it has been provided for;
 - c) to guarantee the private rights such as patent rights, copyrights or trade secrets that are involved in Classified Information.
- (4) The Parties mutually recognize the Personnel Security Clearance and Facility Security Clearance Certificates, released in accordance with the national laws and regulations in force.
- (5) Within the scope of this Agreement, the National Security Authorities shall inform each other without delay about revocation of Personnel and Facility Security Clearances or the alteration of the security classification level.
- (6) If any other Agreement concluded between the Parties contains stricter regulations regarding the exchange or protection of Classified Information, these regulations shall apply.

*Article 5****National Security Authorities***

- (1) The National Security Authorities of the Parties are:

<i>For the Grand Duchy of Luxembourg</i>	<i>For the Republic of Lithuania</i>
Service de renseignement de l'État Autorité nationale de Sécurité	Commission for secrets protection co-ordination

- (2) The Parties shall notify each other through diplomatic channels of any subsequent changes of their National Security Authorities.
- (3) Upon request, the National Security Authorities shall inform each other of the national laws and regulations in force regulating the protection of Classified Information and/or any significant amendments thereto.
- (4) Upon request the National Security Authorities shall notify each other about Competent Authorities that are responsible for the implementation of delegated tasks under this Agreement.
- (5) In order to ensure close co-operation in the implementation of the present Agreement, the National Security Authorities may hold consultations at the request made by one of them.
- (6) In order to achieve and maintain comparable standards of security, the National Security Authorities shall, on request, provide each other with information about the security standards, procedures and practices for protection of Classified Information employed by the respective Party.

(7) The respective National Security Authorities may conclude implementing arrangements on the basis of this Agreement.

(8) The Competent Authorities shall assist each other upon request and in accordance with the national laws and regulations in force in carrying out vetting procedures.

(9) Within the scope of this Agreement, the National Security Authorities shall inform each other without delay about any alteration with regard to Personnel Security Clearances or Facility Security Clearances, in particular about their revocation or alteration of the classification level.

Article 6

Transfer of Classified Information

(1) As a rule, Classified Information shall be transferred by means of diplomatic or military couriers or by other means approved in advance by the Competent Authorities of the Parties. The Receiving Party shall confirm in writing the receipt of Classified Information marked SLAPTAI/SECRET LUX/SECRET and above.

(2) Classified Information may be transmitted via protected telecommunication systems, networks or other electromagnetic means approved in accordance with national laws and regulations in force and holding a duly issued certificate.

(3) Other approved means of transfer of Classified Information may only be used if agreed upon between the National Security Authorities of the Parties.

Article 7

Translation, reproduction, destruction of Classified Information

(1) Classified Information marked SLAPTAI/SECRET LUX/SECRET and above shall be translated or reproduced only by written permission of the Originating Party.

(2) All translations of Classified Information shall be made by individuals who hold an appropriate Personnel Security Clearance. Such translation shall bear all original security classification markings.

(3) When Classified Information is reproduced, all original classification markings and additional handling instructions thereon shall also be reproduced or marked on each copy. Such reproduced Classified Information shall be placed under the same control as the original Classified Information. The number of copies shall be limited to that required for official purposes.

(4) Classified Information marked SLAPTAI/SECRET LUX/SECRET and below may be destroyed after it is no longer needed in accordance with national laws and regulations in force. The Classified Information shall be destroyed as to prevent its reconstruction in whole or in part. The copy of the report on destruction of such Classified Information shall be delivered to the Originating Party.

(5) Classified Information marked VISIŠKAI SLAPTAI/ TRES SECRET LUX/TOP SECRET shall not be destroyed. As a rule, it shall be returned to the Originating Party.

(6) In case of emergency, which makes it impossible to protect and return Classified Information generated or transferred according to the present Agreement, the Classified Information shall be destroyed immediately. The Receiving Party shall notify the Originating Party on destruction of such Classified Information as soon as possible.

*Article 8**Classified Contracts*

- (1) Classified Contracts shall be concluded and implemented in accordance with national laws and regulations of each Party. Upon request the National Security Authority of each Party shall furnish information whether a proposed Contractor and its respective employees has been issued an appropriate security clearance, corresponding to the security classification of the Classified Information to be handled. If the proposed Contractor or its respective employees does not hold an appropriate security clearance, the National Security Authority may request for that Contractor or its respective employees to be security cleared. An appropriate security clearance shall be issued to the Contractor or its respective employees before the Classified Contract is concluded.
- (2) The National Security Authority of the Party in which the Classified Contract is to be performed, shall assume the responsibility for prescribing and administering security measures for the Classified Contract under the same standards and requirements that govern the protection of its own Classified Contracts.
- (3) Security instructions shall be an integral part of each Classified Contract. These security instructions shall include the following aspects:
- a) security classification levels of the information that will be generated in the course of Classified Contract, and list of Classified Information that will be transmitted to the Contractor;
 - b) an obligation that the Contractor shall disclose the Classified Information only to a person who is authorized in accordance with the national laws and regulations in force to have access to Classified Information of the equivalent security classification level, who has a „Need-to-know“ and who is employed or engaged in the carrying out of the Classified Contract;
 - c) procedure for the communication of changes in the classification of information;
 - d) communication channels and means for transmission of Classified Information ;
 - e) an obligation to use the Classified Information under the Classified Contract only for the purposes related to the subject matter of the Classified Contract;
 - f) strict adherence to the procedures for destruction of the Classified Information;
 - g) an obligation to notify any actual or suspected Breach of security;
 - h) the procedure for the approval of visits or inspection to facilities of the Contractor.
- (4) Copy of the Project Security Instruction of any Classified Contract shall be forwarded to the National Security Authority of the Party where the classified contract is to be performed to allow adequate security supervision and control.
- (5) Upon request, for contracts involving Classified Information RIBOTO NAUDOJIMO/RESTREINT LUX/RESTRICTED no Facility Security Clearance will be issued. The National Security Authority of each Party shall furnish information in writing declaring whether a proposed Contractor meets the national requirements for protection of Classified Information marked RIBOTO NAUDOJIMO/RESTREINT LUX/RESTRICTED.

*Article 9**Visits*

- (1) Visits that require access to Classified Information shall be allowed only with a written permission issued by the National Security Authority or Competent Authority of the Party to be visited.
- (2) As a rule, the request for visit shall be sent at least two weeks before the visit.
- (3) The request for visit shall contain the following information:
- a) visitors first and last names, date and place of birth, passport or identification document number;

- b) citizenship of the visitor;
- c) position title of the visitor and name of the organization he represents;
- d) certification of Personnel Security Clearance of the visitor, its level and validity;
- e) purpose, proposed working program and planned date of the visit;
- f) names and points of contacts of the organizations and facilities requested to be visited.

(4) Each Party shall guarantee protection of personal data of the visitors, according to the national laws and regulations in force.

(5) National Security Authorities or Competent Authorities may draw up lists of personnel authorized to make multiple visits in respect of any particular project or program in accordance with the terms and conditions commonly agreed.

Article 10

Breach of Security

(1) In case of a Breach of Security, the National Security Authority of the Party in which a Breach of Security occurred shall inform the National Security Authority of the other Party immediately and shall ensure the appropriate investigation. The other Party shall, if required, cooperate in the investigation.

(2) The other Party shall be informed of the results of the investigation and shall receive the final report on the reasons and extent of damage caused.

Article 11

Costs

Each Party shall bear the costs incurred in the course of implementing its obligations under this Agreement.

Article 12

Settlement of Disputes

Any dispute regarding the interpretation or application of this Agreement shall be exclusively settled through consultations between the Parties.

Article 13

Final Provisions

- (1) This Agreement is concluded for an indefinite period of time.
- (2) The present Agreement shall enter into force on the first day following the receipt of the last notification, in writing and through diplomatic channels, stating that all the national legal requirements of both Parties necessary to that effect have been fulfilled.
- (3) This Agreement may be amended on the basis of mutual written consent by both Parties. Such amendments are integral part of this Agreement and shall enter into force in accordance with Paragraph 2 of this Article.
- (4) Each Party may terminate this Agreement through diplomatic channels by written notice forwarded to the other Party. The termination shall enter into force six months after the date of receipt of the notification. In such case, all exchanged classified information shall be returned to the Originating Party. If the exchanged Classified Information could not be returned, it shall continue to be protected

in accordance with the provisions of this Agreement, until the Originating Party dispenses the Receiving Party from this obligation.

DONE at Brussels, on the 7th of December 2020, in three original copies, each in the Lithuanian, English and French languages, and all texts being equally authentic. In case of any divergence of interpretation, the English language text shall prevail.

*For the Government of the
Grand Duchy of Luxembourg
(Signature)*

*For the Government of the
Republic of Lithuania
(Signature)*

*

ACCORD

entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la Répu- blique de Lituanie concernant l'échange et la protection réciproque d'informations classifiées

Le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la République de Lituanie et (ci-après dénommés les « Parties » ou individuellement la « Partie »),

souhaitant développer et renforcer leur coopération politique, économique, technologique et militaire,

désirant promouvoir la confiance mutuelle,

reconnaissant qu'une coopération efficace peut exiger l'échange d'informations classifiées entre les Parties,

désirant établir un ensemble de règles régissant la protection réciproque d'informations classifiées, produites ou échangées dans le cadre d'une coopération entre les Parties,

CONVIENNENT ce qui suit :

Article 1

Objet et champ d'application

(1) Le présent Accord a pour but de garantir la protection des informations classifiées (telles que définies ci-après) échangées ou produites dans le cadre de la coopération entre les Parties et d'établir un ensemble de règles et de procédures régissant leur protection réciproque.

(2) Le présent Accord est applicable à l'ensemble des activités, contrats ou accords impliquant des informations classifiées qui seront menés ou conclus entre les Parties à l'avenir ou ont été menés ou conclus avant la date d'entrée en vigueur des présentes.

Article 2

Définitions

Aux fins du présent Accord :

(1) Une « **infraction à la sécurité** » désigne tout acte ou omission contraire aux lois et réglementations nationales en vigueur ou au présent Accord, susceptible d'entraîner la divulgation, la perte, la destruction, le détournement ou tout autre type de compromission d'informations classifiées.

- (2) Un « **contrat classifié** » désigne un contrat, un contrat de sous-traitance ou un projet dont la mise en œuvre nécessite l'accès aux informations classifiées ou la production de telles informations.
- (3) Les « **informations classifiées** » désignent toute information, quelle qu'en soit la forme, la nature ou le mode de transfert, produite ou en cours de production et qui, à des fins de sécurité nationale et conformément aux lois et réglementations nationales, doit être protégée contre toute infraction à la sécurité et a été ainsi désignée par l'attribution d'un niveau de classification de sécurité.
- (4) Une « **autorité compétente** » désigne toute autorité gouvernementale, autre que l'autorité nationale de sécurité, qui, conformément aux lois et réglementations nationales en vigueur, est chargée de l'exécution des tâches déléguées en vertu du présent Accord.
- (5) Un « **contractant** » désigne toute personne physique ou morale dotée de la capacité juridique de conclure des contrats classifiés conformément aux modalités du présent Accord.
- (6) Une « **habilitation de sécurité d'établissement** » renvoie à une décision positive rendue par l'autorité nationale de sécurité, établie sous la forme d'un document confirmant qu'un sous-traitant est autorisé à exécuter des actions liées à l'utilisation d'informations classifiées jusqu'à un certain niveau de classification de sécurité, conformément aux lois et réglementations nationales.
- (7) « **L'Autorité nationale de sécurité** » désigne l'autorité nationale qui, conformément aux lois et réglementations nationales, est chargée de superviser la mise en œuvre du présent Accord. Ces autorités sont énumérées à l'article 5 du présent Accord.
- (8) Le « **principe du besoin d'en connaître** » renvoie à la nécessité d'accéder à des informations classifiées dans le cadre de devoirs officiels et/ou d'une mission officielle concrète.
- (9) La « **Partie d'origine** » désigne la Partie, en ce compris toute instance de sa juridiction, qui fournit des informations classifiées conformément aux lois et réglementations nationales.
- (10) Une « **habilitation de sécurité individuelle** » renvoie à une décision positive de l'autorité nationale de sécurité ou de l'autorité compétente, établie sous la forme d'un document attestant de la loyauté et la fiabilité d'une personne ainsi que d'autres aspects relatifs à la sécurité, conformément aux lois et réglementations nationales, et octroyant l'accès aux informations classifiées jusqu'à un certain niveau de classification de sécurité.
- (11) La « **Partie destinataire** » désigne la Partie, en ce compris toute instance relevant de sa juridiction, à laquelle sont transmises des informations classifiées de la Partie d'origine, conformément aux lois et réglementations nationales.
- (12) Une « **tierce partie** » désigne tout État, y compris toute instance publique ou privée, organisation internationale, personne physique ou morale, qui n'est pas l'une des Parties au présent Accord.

Article 3

Niveaux de sécurité

- (1) Les Parties reconnaissent que les niveaux de sécurité suivants sont équivalents et se correspondent comme suit :

<i>Pour le Grand-Duché de Luxembourg</i>	<i>Equivalent en anglais</i>	<i>Pour la République de Lituanie</i>
TRÈS SECRET LUX	TOP SECRET	VISISKAI SLAPTAI
SECRET LUX	SECRET	SLAPTAI
CONFIDENTIEL LUX	CONFIDENTIAL	KONFIDENCIALIAI
RESTREINT LUX	RESTRICTED	RIBOTO NAUDOJIMO

- (2) La Partie destinataire attribuera à l'information classifiée reçue le niveau de sécurité équivalent qui lui est propre. La Partie destinataire ne pourra déclassifier les informations classifiées reçues ou altérer leur niveau de sécurité sans l'accord écrit préalable de la Partie d'origine.

(3) La Partie d'origine informera la Partie destinataire, par écrit et sans délai, de toute modification apportée au niveau de classification des informations échangées.

Article 4

Protection des informations classifiées

(1) Conformément à leurs lois et réglementations nationales en vigueur, les Parties s'engagent à mettre en œuvre toutes les mesures appropriées afin de protéger les informations classifiées généralement produites ou échangées en vertu du présent Accord. Elles attribueront auxdites informations classifiées un niveau de protection au minimum équivalent à celui qui est accordé à leurs informations classifiées nationales de même niveau de classification de sécurité, conformément aux dispositions de l'article 3.

(2) L'accès aux informations classifiées sera exclusivement réservé aux personnes qui ont besoin de connaître de telles informations et qui disposent de l'autorisation appropriée, en vertu des lois et réglementations nationales en vigueur, pour accéder à des informations classifiées d'un niveau de classification de sécurité équivalent.

(3) La Partie destinataire s'engage :

- a) à ne délivrer aucune information classifiée à une tierce partie sans l'accord écrit de l'autorité nationale de sécurité de la Partie d'origine ;
- b) à ne pas utiliser d'informations classifiées à d'autres fins que celles auxquelles elles lui ont été transmises ;
- c) à préserver les droits privés, tels que les droits de brevets, les droits d'auteur ou les secrets commerciaux associés à des informations classifiées.

(4) Les Parties reconnaissent mutuellement leurs habilitations de sécurité individuelle et d'établissement délivrées conformément aux lois et réglementations nationales en vigueur.

(5) Dans le cadre du présent Accord, les autorités nationales de sécurité se tiennent mutuellement informées sans délai de toute révocation d'habilitation de sécurité individuelle et d'établissement ou de toute modification apportée au niveau de classification de sécurité.

(6) Si tout autre Accord conclu entre les Parties comporte des règles plus strictes eu égard à l'échange ou à la protection des informations classifiées, de telles règles s'appliquent.

Article 5

Autorités nationales de sécurité

(1) Les autorités nationales de sécurité des Parties sont :

<i>Pour le Grand-Duché de Luxembourg</i>	<i>Pour la République de Lituanie</i>
Service de renseignement de l'État Autorité nationale de sécurité	Commission for secrets protection co-ordination

(2) Les Parties se tiennent mutuellement informées, par la voie diplomatique, de toute modification apportée à leurs autorités nationales de sécurité.

(3) Sur demande, les autorités nationales de sécurité se tiennent mutuellement informées de leurs lois et réglementations nationales en vigueur en matière de protection des informations classifiées et/ou de toute modification significative qui leur est apportée.

(4) Sur demande, les autorités nationales de sécurité se communiquent mutuellement les informations se rapportant aux autorités compétentes chargées de l'exécution des tâches déléguées en vertu des présentes.

(5) Afin de garantir une coopération efficace dans l'exécution des présentes, les autorités nationales de sécurité pourront organiser des consultations si l'une d'entre elles en formule la demande.

(6) En vue d'appliquer et de maintenir des normes de sécurité similaires, les autorités nationales de sécurité se tiennent mutuellement informées, sur demande, des normes, procédures et pratiques de sécurité appliquées par chaque Partie en matière de protection des informations classifiées.

(7) Les autorités nationales de sécurité respectives pourront conclure des modalités de mise en œuvre sur la base du présent Accord.

(8) Sur demande, et conformément aux lois et réglementations nationales en vigueur, les autorités compétentes s'assisteront mutuellement dans le cadre de la réalisation des procédures de vérification.

(9) Dans le cadre du présent Accord, les autorités nationales de sécurité se tiennent mutuellement informées sans délai de toute modification apportée aux habilitations de sécurité individuelle ou d'établissement, notamment en cas de révocation ou de modification du niveau de classification.

Article 6

Transfert d'informations classifiées

(1) En règle générale, les informations classifiées seront transférées par des coursiers diplomatiques ou militaires ou par tout autre moyen approuvé préalablement par les autorités compétentes des Parties. La Partie destinataire confirmera par écrit la réception d'informations identifiées comme étant de niveau SLAPTAI/SECRET LUX/SECRET ou d'un niveau supérieur.

(2) Les informations classifiées pourront être transmises par le biais de systèmes, de réseaux ou d'autres moyens électromagnétiques de communication protégés, approuvés conformément aux lois et réglementations nationales en vigueur et assortis d'un certificat dûment établi.

(3) D'autres moyens ne pourront être utilisés pour le transfert d'informations classifiées que s'ils ont été approuvés par les autorités nationales de sécurité des Parties.

Article 7

Traduction, reproduction, destruction d'informations classifiées

(1) La traduction ou la reproduction d'informations classifiées SLAPTAI/SECRET LUX/SECRET sont autorisées uniquement avec l'accord écrit de la Partie d'origine.

(2) Toutes les traductions d'informations classifiées seront effectuées par des personnes disposant d'une habilitation de sécurité individuelle appropriée. Ces traductions porteront l'ensemble des marquages de classification de sécurité originaux.

(3) Lors de la reproduction d'informations classifiées, tous les marquages de classification des informations originales, ainsi que les instructions supplémentaires relatives à leur traitement, seront également reproduits ou indiqués sur chaque exemplaire. Les informations ainsi reproduites sont placées sous le même niveau de contrôle que les informations originales. Le nombre de copies est limité à celui requis pour un usage officiel.

(4) Les informations classifiées identifiées comme étant de niveau SLAPTAI/SECRET LUX/SECRET ou d'un niveau inférieur pourront être détruites dès lors qu'elles ne sont plus nécessaires, conformément aux lois et réglementations nationales en vigueur. Les informations classifiées seront détruites de la façon requise pour empêcher leur reconstruction en tout ou partie. Un exemplaire du rapport relatif à la destruction desdites informations classifiées sera remis à la Partie d'origine.

(5) Les informations classifiées VISISKAI SLAPTAI/ TRES SECRET LUX/TOP SECRET ne seront pas détruites. En règle générale, celles-ci doivent être renvoyées à la Partie d'origine.

(6) Dans le cas d'une situation d'urgence rendant impossible la protection et le renvoi des informations classifiées produites ou échangées en vertu du présent Accord, les informations classifiées seront détruites immédiatement. La Partie destinataire informera dès que possible la Partie d'origine de la destruction des informations classifiées.

Article 8

Contrats classifiés

(1) Les contrats classifiés sont conclus et exécutés conformément aux lois et réglementations nationales de chaque Partie. Sur demande, l'autorité nationale de sécurité de chaque Partie fournira les informations attestant de la délivrance à un sous-traitant proposé et à ses employés respectifs d'une habilitation de sécurité appropriée correspondant au niveau de classification de sécurité des informations classifiées concernées. Si le sous-traitant proposé ou l'un de ses employés respectifs ne détient pas d'habilitation de sécurité appropriée, l'autorité nationale de sécurité peut demander que ce sous-traitant, ou ses employés respectifs, obtiennent une telle habilitation. Une habilitation de sécurité appropriée sera délivrée au sous-traitant ou à ses employés respectifs avant la conclusion du contrat classifié.

(2) Il incombe à l'autorité nationale de sécurité de la Partie dont le territoire est visé par l'exécution du contrat classifié de prescrire et d'administrer les mesures de sécurité applicables audit contrat selon les mêmes normes et les mêmes exigences que celles qui régissent la protection de ses propres contrats classifiés.

(3) Des instructions relatives à la sécurité feront partie intégrante de chaque contrat classifié. Ces instructions couvriront notamment les aspects suivants :

- a) les niveaux de classification de sécurité des informations devant être produites dans le cadre du contrat classifié, et une liste des informations classifiées devant être transmises au sous-traitant ;
- b) l'obligation pour le sous-traitant de restreindre la divulgation des informations classifiées aux personnes qui, conformément aux lois et réglementations nationales en vigueur, sont autorisées à accéder à des informations classifiées d'un niveau de sécurité équivalent, ont besoin de connaître de telles informations et sont employées ou engagées dans l'exécution du contrat classifié ;
- c) la procédure relative à la communication des modifications apportées aux niveaux de classification des informations ;
- d) les voies de communication et les moyens de transmission employés pour le transfert d'informations classifiées ;
- e) l'obligation d'utiliser les informations classifiées en vertu d'un contrat classifié aux seules fins liées à l'objet d'un tel contrat ;
- f) le strict respect des procédures applicables à la destruction d'informations classifiées ;
- g) l'obligation de signaler toute infraction à la sécurité avérée ou suspectée ;
- h) la procédure applicable à l'approbation des visites ou inspections des sites du sous-traitant.

(4) Pour tout contrat classifié, une copie des instructions de sécurité de projet sera transmise à l'autorité nationale de sécurité de la Partie sur le territoire de laquelle le contrat doit être exécuté en vue de garantir une supervision et un contrôle de sécurité appropriés.

(5) Sur demande, pour les contrats impliquant des informations classifiées RIBOTO NAUDOJIMO/ RESTREINT LUX/RESTRICTED, aucune habilitation de sécurité d'établissement ne sera délivrée. L'autorité nationale de sécurité de chaque Partie fournira par écrit les informations attestant qu'un sous-traitant proposé satisfait aux exigences nationales relatives à la protection d'informations

classifiées identifiées comme étant de niveau RIBOTO NAUDOJIMO / RESTREINT LUX / RESTRICTED.

Article 9

Visites

- (1) Les visites impliquant l'accès à des informations classifiées seront soumises à l'autorisation de l'autorité nationale de sécurité ou de l'autorité compétente de la Partie objet de la visite.
- (2) En règle générale, toute demande de visite doit être soumise au minimum deux semaines avant la visite.
- (3) Toute demande de visite comportera les informations suivantes :
 - a) les noms et prénoms, la date et le lieu de naissance, le numéro de passeport ou de la carte d'identité du visiteur ;
 - b) la nationalité du visiteur ;
 - c) le titre du poste du visiteur et le nom de l'organisation qu'il représente ;
 - d) le certificat attestant de la délivrance d'une habilitation de sécurité individuelle au visiteur, ainsi que le niveau et la date d'expiration de cette habilitation ;
 - e) le but de la visite ainsi que le programme de travail proposé et la date prévue ;
 - f) les noms et les référents des organisations et sites qui doivent être visités.
- (4) Chacune des Parties s'engage à garantir la protection des données personnelles des visiteurs conformément aux lois et réglementations nationales en vigueur.
- (5) Les autorités nationales de sécurité ou les autorités compétentes pourront établir des listes répertoriant le personnel autorisé à procéder à de multiples visites relativement à tout projet ou programme spécifique, conformément à des modalités convenues par les Parties.

Article 10

Infraction à la sécurité

- (1) En cas d'infraction à la sécurité, l'autorité nationale de sécurité de la Partie concernée par l'infraction informera l'autorité nationale de sécurité de l'autre Partie sans délai et veillera à mener une enquête appropriée. Si nécessaire, l'autre Partie coopèrera à cette enquête.
- (2) L'autre Partie sera tenue informée des résultats de l'enquête et recevra le rapport final sur les raisons et l'étendue des dommages qui ont été causés.

Article 11

Coûts

Chacune des Parties assume les frais engagés du fait de l'exécution de ses obligations en vertu du présent Accord.

Article 12

Règlement des litiges

Tout litige quant à l'interprétation ou l'application du présent Accord sera exclusivement résolu par voie de consultations entre les Parties.

*Article 13****Dispositions finales***

- (1) Le présent Accord est conclu pour une durée indéterminée.
- (2) Le présent Accord prend effet le premier jour qui suit la réception de la dernière des notifications, transmise par écrit et par voie diplomatique, confirmant le respect de l'ensemble des exigences légales nationales des deux Parties, telles que requises à cette fin.
- (3) Le présent Accord peut être modifié d'un commun accord, par écrit, par les deux Parties. Les modifications ainsi apportées font partie intégrante du présent Accord et prennent effet conformément aux dispositions prévues au paragraphe 2 du présent article.
- (4) Chaque Partie peut mettre fin au présent Accord via les voies diplomatiques en informant l'autre Partie au moyen d'une notification écrite. Une telle résiliation prend effet six mois après la date de réception de cette notification. Dans un tel cas, toutes les informations classifiées échangées seront restituées à la Partie d'origine. Si les informations classifiées ne peuvent être restituées, elles continueront d'être protégées conformément aux dispositions du présent accord, jusqu'à ce que la Partie d'origine dispense la Partie destinataire de cette obligation.

FAIT à Bruxelles, le 7 décembre 2020, en deux exemplaires originaux, chacun en langues française, lituanienne et anglaise et, tous les textes faisant également foi. Dans le cas d'un désaccord quant à l'interprétation des dispositions du présent Accord, le texte anglais prévaut.

*Pour le Gouvernement du
Grand-Duché de Luxembourg*
(Signature)

*Pour le Gouvernement de la
République de Lituanie*
(Signature)