N° 7502

CHAMBRE DES DEPUTES

Session ordinaire 2019-2020

P R O J E T D E L O I

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

* * *

(Dépôt: le 6.12.2019)

SOMMAIRE:

*

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 Malte relatif à la protection réciproque et à l'échange d'informations classifiées, fait à New York, le 26 septembre 2019.

Palais de Luxembourg, le 4 décembre 2019

Le Ministre des Affaires étrangères et européennes,
Jean ASSELBORN

HENRI

*

TEXTE DU PROJET DE LOI

Article unique. Est approuvé l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la République de Malte relatif à la protection réciproque et à l'échange d'informations classifiées, fait à New York, le 26 septembre 2019.

*

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 notre sécurité, on peut citer 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 du pays, il convient aussi de mentionner l'espionnage industriel et technologique.

La conjugaison de certains de ces éléments pourrait nous exposer 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 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 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 la mise en vigueur de cette loi, la protection des secrets était essentiellement organisée de manière répressive. Par le biais de la loi précitée, le législateur accorde aux autorités limitativement énumérées à l'article 5 le droit de procéder à la classification, la dé-classification et au déclassement de pièces afin de protéger les intérêts relevés par l'article 3 de ladite loi.

Ces mêmes autorités doivent dès lors s'assurer de la protection de ces pièces à l'occasion de leur transmission à des autorités étrangères de même que celles-ci doivent être rassurées sur la protection par le Luxembourg de leurs propres pièces classifiées qu'elles passent aux autorités luxembourgeoises, faute de quoi ces échanges ne pourront juridiquement s'effectuer. Les accords bilatéraux que le Gouvernement se propose de conclure sont appelés à y pourvoir juridiquement.

En conclusion, l'échange et la protection réciproque d'informations classifiées visées par les présents accords bilatéraux seront régis désormais par ces accords ainsi que par les lois de base nationales, 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 accords bilatéraux relatifs à l'échange et à la protection réciproque d'informations classifiées déjà approuvés :

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 22 novembre 2011.
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 1er 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 :
   1° de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la République de Bulgarie relatif à l'échange et à la protection réciproque d'informations classifiées, fait à Sofia, le 29 janvier 2018 ;
   2° de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Conseil des Ministres de la République d'Albanie relatif à la protection réciproque d'informations classifiées, fait à Luxembourg, le 25 juin 2018 ;
   3° de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de Hongrie relatif à l'échange et à la protection réciproque d'informations classifiées, fait à Budapest, le 5 septembre 2018 ;
   4° de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la République de Macédoine relatif à l'échange et à la protection réciproque d'informations classifiées, fait à Skopje, le 6 septembre 2018 ;
   5° de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la République fédérative du Brésil concernant l'échange et la protection réciproque d'informations classifiées, fait à New York, le 25 septembre 2018

*

COMMENTAIRES DES ARTICLES

Les premiers articles **(Art. 1-4)** visent à définir le champ d'application, à établir des définitions communes des termes utilisés, à établir des équivalences entre les différents niveaux de classification nationaux, ainsi qu'à définir les autorités nationales de sécurité compétentes.

Sont définies ensuite les mesures applicables à la protection d'informations classifiées, ainsi qu'au transfert, à la reproduction et traduction, ainsi qu'à la destruction de celles-ci **(Art. 5-8)**. L'**Art. 9** porte sur les modalités de conclusion et d'exécution de contrats classifiés (le terme « contrat classifié » étant défini dans l'Art. 2). Dans le cadre de leur coopération, les autorités nationales de sécurité peuvent effectuer des visites mutuelles, selon les règles établies dans l'**Art. 10**.

En cas d'infraction à la sécurité, l'autorité nationale concernée doit en informer immédiatement l'autorité nationale de l'autre partie et prendre toutes les mesures nécessaires afin de limiter les conséquences, conformément à **l'Art. 11**. Enfin, les derniers articles **(Art. 12-14)** contiennent des dispositions relatives aux frais, au règlement des litiges, ainsi qu'à l'entrée en vigueur, la durée et la modification de l'Accord.

*

FICHE D'EVALUATION D'IMPACT

Mesures législatives et réglementaires

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 Malte relatif à la protection réciproque et à l'échange d'informations classifiées, fait à New York, le 26 septembre 2019**
Ministère initiateur:	**Ministère des Affaires étrangères et européennes**
Auteur:	**Steve Hoscheit**
Tél. :	**247-72488**
Courriel:	**steve.hoscheit@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 Malte.**
Autre(s) Ministère(s)/Organisme(s)/Commune(s)impliqué(e)(s):	
Ministère d'Etat, Autorité nationale de Sécurité (ANS)	
Date:	**16 octobre 2019**

Mieux légiférer

1. Partie(s) prenante(s) (organismes divers, citoyens,…) consultée(s): Oui: ☐ Non: ☒[1]
   Si oui, laquelle/lesquelles:
   Remarques/Observations:

2. Destinataires du projet:
   – Entreprises/Professions libérales: Oui: ☐ Non: ☒
   – Citoyens: Oui: ☐ Non: ☒
   – Administrations: Oui: ☒ Non: ☐

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

3. 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:

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 administrative[3] 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 administratif[4] par destinataire)

7. a) Le projet prend-il recours à un échange de données inter-administratif (national ou international) plutôt que de demander l'information au destinataire? Oui: ☐ Non: ☐ N.a.: ☒
Si oui, de quelle(s) donnée(s) et/ou administration(s) s'agit-il?

   b) Le projet en question contient-il des dispositions spécifiques concernant la protection des personnes à l'égard du traitement des données à caractère personnel? 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 communautaires, le principe « la directive, rien que la directive » est-il respecté? Oui: ☐ Non: ☐ N.a.: ☒
Sinon, pourquoi?

---

2 N.a.: non applicable.

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…).

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:

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:
    – 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 évaluation[5] ? — 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 transfrontaliers[6] ? — 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

*

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)

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'État.

*

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 a New York, le 26 septembre 2019

Le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la République de Malte, ci-après dénommés les « Parties »,

Reconnaissant qu'une coopération efficace dans les domaines politique, économique, militaire, de la sécurité ou de l'intelligence, et dans tout autre domaine, peut exiger l'échange d'informations classifiées entre les Parties,

Désirant établir un système régissant la protection réciproque d'informations classifiées, produites ou échangées dans le cadre d'une coopération entre les Parties, ou entre des instances du secteur public et du secteur privé relevant de leur juridiction.

CONVIENNENT ce qui suit :

Article 1

Objet et champ d'application

1.1. Le présent Accord a pour but de garantir la protection des informations classifiées généralement créées ou échangées entre les Parties, ou entre des instances du secteur public et du secteur privé relevant de leur juridiction, et soumises aux lois nationales applicables des Parties.

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

1.3. Les dispositions du présent Accord s'appliquent également aux informations classifiées déjà produites ou échangées dans le cadre d'une coopération entre les Parties avant l'entrée en vigueur des présentes.

Article 2

Définitions

Aux fins du présent Accord :

2.1. **« Infraction à la sécurité »** désigne tout acte, ou omission, contraire aux lois et réglementations nationales, entraînant ou étant susceptible d'entraîner la divulgation, la perte, la destruction, le détournement ou tout autre type de compromission d'informations classifiées ;

2.2. **« Contrat classifié »** désigne un accord entre deux contractants ou sous-traitants ou plus, qui contient ou implique des informations classifiées ;

2.3. Les **« informations classifiées »** désignent l'ensemble des informations, documents ou matériels, quelle qu'en soit la forme, échangés ou produits entre les Parties conformément aux lois et réglementations nationales de chacune des Parties, auxquels un niveau de classification de sécurité a été attribué et nécessitant une protection contre toute divulgation non autorisée, détournement ou perte, ou tout autre type de compromission ;

2.4. **« Contractant »** désigne toute personne physique ou morale dotée de la capacité juridique de conclure des contrats classifiés ;

2.5. **« Habilitation de sécurité d'établissement »** désigne toute décision de l'autorité de sécurité nationale confirmant que le contractant ou le sous-traitant satisfait aux exigences requises pour traiter des informations classifiées et définissant le niveau de classification de sécurité des informations classifiées qu'il est autorisé à traiter ;

2.6. **« 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 et de contrôler la protection des informations classifiées produites ou échangées en vertu des présentes ;

2.7. **« Besoin d'en connaître »** fait référence à la nécessité d'accéder à des informations classifiées dans le cadre de fonctions officielles déterminées et/ou en vue de l'accomplissement d'une mission spécifique ;

2.8. **« Partie d'origine »** désigne la Partie, en ce compris toute instance, qui fournit des informations classifiées conformément aux lois et réglementations nationales ;

2.9. **« Habilitation de sécurité individuelle »** désigne toute décision de l'autorité de sécurité nationale confirmant qu'un ressortissant est autorisé à accéder à des informations classifiées et définissant le niveau de classification de sécurité des informations classifiées auxquelles il est autorisé à accéder, conformément aux lois et réglementations nationales ;

2.10. **« Partie destinataire »** désigne la Partie, en ce compris toute instance, à laquelle la Partie d'origine transmet des informations classifiées ;

2.11. Un **« sous-traitant »** désigne tout contractant avec lequel le premier contractant conclut un contrat de sous-traitance ;

2.12. Une **« tierce partie »** désigne tout État, en ce compris les personnes physiques ou morales relevant de la juridiction de cet État, ou toute organisation internationale, qui n'est pas l'une des Parties au présent Accord.

Article 3

Niveaux de classification de sécurité

3.1. Les Parties s'engagent à protéger les informations classifiées qu'elles échangent et acceptent d'adopter des niveaux de classification de sécurité équivalents aux niveaux mentionnés ci-après :

Pour la République de Malte	*Pour le Grand-Duché de Luxembourg*	*Équivalent en anglais*
L-OGHLA SEGRETEZZA	TRÈS SECRET LUX	TOP SECRET
SIGRIET	SECRET LUX	SECRET
KUNFIDENZJALI	CONFIDENTIEL LUX	CONFIDENTIAL
RISTRETT	RESTREINT LUX	RESTRICTED

3.2. La Partie d'origine peut recourir à des marquages supplémentaires afin de signaler que des restrictions spéciales s'appliquent à l'utilisation d'informations classifiées. Les autorités nationales de sécurité s'informent mutuellement par écrit de l'utilisation de ces éventuels marquages supplémentaires.

Article 4

Autorités nationales de sécurité

4.1. Les autorités nationales de sécurité des Parties sont :

Pour la République de Malte :

Autorité nationale de sécurité

Ministère de l'Intérieur et de la Sécurité nationale (MHAS)

LA VALETTE

MALTE

Pour le Grand-Duché de Luxembourg :
Le Service de Renseignement de l'État
Autorité nationale de Sécurité
LUXEMBOURG

4.2. Les Parties se tiennent mutuellement informées, par la voie diplomatique, de toute modification affectant les autorités nationales de sécurité. Une telle notification de modification ne constitue pas un amendement officiel aux présentes, conformément au paragraphe 2 de l'article 14.

4.3. Les autorités nationales de sécurité se tiennent mutuellement informées des lois et réglementations en vigueur dans leur État, ainsi que de toute modification ayant trait à la protection des informations classifiées produites ou échangées conformément au présent Accord.

4.4. En vue d'appliquer et de maintenir des normes de sécurité équivalentes, les autorités nationales de sécurité se tiennent mutuellement informées des normes, procédures et pratiques de sécurité appliquées par chaque Partie en matière de protection des informations classifiées.

Article 5

Mesures applicables à la protection d'informations classifiées

5.1. Conformément aux dispositions des lois et réglementations nationales, les Parties prennent toutes les mesures appropriées afin de protéger les informations classifiées échangées ou produites en vertu du présent Accord. Elles garantissent auxdites informations classifiées un niveau de protection équivalent à celui qui est accordé à leurs informations classifiées nationales assorties du niveau de classification de sécurité correspondant, tel que défini à l'article 3 du présent Accord.

5.2. La Partie d'origine informe par écrit la Partie destinataire de toute modification apportée au niveau de classification de sécurité des informations classifiées transmises afin de mettre en œuvre les mesures de protection appropriées.

5.3. L'accès aux informations classifiées est exclusivement réservé aux personnes autorisées, en vertu des lois et réglementations nationales ou de par leurs fonctions, à accéder à des informations classifiées d'un niveau de classification de sécurité équivalent, qui ont besoin de connaître de telles informations et ont été informées en conséquence.

5.4. Aux fins du présent Accord, chacune des Parties reconnaît les habilitations de sécurité individuelles et d'établissement établies par l'autre Partie.

5.5. Sur demande, et conformément aux lois et réglementations nationales, les autorités nationales de sécurité peuvent s'assister mutuellement dans le cadre de la réalisation des procédures de vérification.

5.6. Aux fins 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, selon le cas.

5.7. Sur demande de l'autorité nationale de sécurité de la Partie d'origine, l'autorité nationale de sécurité de la Partie destinataire confirmera par écrit qu'une personne s'est vue octroyer une habilitation de sécurité individuelle ou qu'une entité juridique s'est vue octroyer une habilitation de sécurité d'établissement.

5.8. La Partie destinataire :

a) ne divulgue aucune information classifiée à une tierce partie sans l'accord écrit de la Partie d'origine délivré conformément aux lois et réglementations nationales ;

b) si cela s'avère approprié, classifie les informations reçues conformément au niveau de sécurité équivalent mentionné à l'article 3 ;

c) ne déclassifie aucune des informations classifiées fournies et s'interdit de leur octroyer un niveau de protection inférieur sans l'accord écrit de la Partie d'origine ; et

d) n'utilise les informations classifiées qu'aux fins prévues.

Article 6

Transfert d'informations classifiées

6.1. Les informations classifiées seront transférées par des coursiers diplomatiques ou militaires ou par tout autre moyen approuvé préalablement par les autorités nationales de sécurité, conformément aux lois et réglementations nationales.

6.2. La transmission électronique d'informations classifiées est effectuée par le biais de méthodes cryptographiques certifiées, acceptées par les Parties.

6.3. Si des informations classifiées transmises sont identifiées comme étant de niveau SIGRIET/ SECRET LUX ou d'un niveau supérieur, la Partie destinataire en confirmera la réception par écrit. La réception des autres informations classifiées sera confirmée sur demande.

Article 7

Reproduction et traduction d'informations classifiées

7.1. La traduction ou la reproduction d'informations classifiées de niveau SIGRIET / SECRET LUX, ou de niveau supérieur, sont autorisées uniquement dans des cas exceptionnels, avec l'accord écrit préalable de la Partie d'origine.

7.2. Toutes les reproductions et les traductions d'informations classifiées portent les marquages de classification originaux. Ces informations reproduites ou traduites sont soumises au même niveau de protection que les informations originales. Le nombre de reproductions ou de traductions est limité à celui requis pour un usage officiel.

7.3. La procédure définie ci-après s'applique aux traductions ou aux reproductions réalisées conformément aux alinéas (1) et (2) :

(a) le personnel chargé d'effectuer ces traductions et ces reproductions doit détenir une habilitation de sécurité appropriée, conformément aux lois nationales applicables ; et

(b) les traductions indiquent clairement dans la langue de traduction qu'elles contiennent des informations classifiées reçues de la Partie d'origine.

Article 8

Destruction d'informations classifiées

8.1. Les informations classifiées de niveau L-OGHLA SEGRETEZZA / TRÈS SECRET LUX ne seront pas détruites, sauf dans les cas mentionnés au paragraphe 4 du présent article. Ces informations classifiées seront renvoyées à la Partie d'origine dès lors que les Parties les jugent inutiles.

8.2. Dès lors que la Partie destinataire n'en a plus l'utilité, les informations classifiées de niveau SIGRIET / SECRET LUX ou de niveau inférieur seront détruites dans la mesure requise pour empêcher leur reconstruction en tout ou partie.

8.3. La Partie destinataire informe la Partie d'origine de la destruction des informations classifiées SIGRIET /SECRET LUX.

8.4. Dans le cas d'une situation de crise rendant impossible la protection ou le renvoi des informations classifiées produites ou échangées en vertu du présent Accord, les informations classifiées sont détruites immédiatement. La Partie destinataire avise dès que possible les autorités nationales de sécurité des deux Parties d'une telle destruction.

Article 9

Contrats classifiés

9.1. Les contrats classifiés seront conclus et exécutés conformément aux lois et réglementations nationales.

9.2. Sur demande, l'autorité nationale de sécurité de la Partie destinataire confirmera qu'un Contractant proposé s'est vu octroyer une habilitation de sécurité individuelle ou d'établissement appropriée. Si le Contractant proposé ne détient pas l'habilitation de sécurité appropriée, l'autorité nationale de sécurité de la Partie d'origine peut demander à celle de la Partie destinataire d'établir une telle habilitation.

9.3. Il incombe à l'autorité nationale de sécurité 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. Des inspections périodiques de la sécurité pourront être effectuées par les autorités nationales de sécurité.

9.4. Une annexe relative à la sécurité fera partie intégrante de chaque contrat ou contrat de sous-traitance classifié. Dans cette annexe, la Partie d'origine spécifiera les informations classifiées qui doivent être divulguées à la Partie destinataire, le niveau de classification de sécurité qui leur a été attribué, ainsi que les obligations qui incombent au contractant eu égard à la protection des informations classifiées. Une copie de l'annexe relative à la sécurité sera transmise à l'autorité nationale de sécurité de la Partie d'origine.

9.5. Avant de transmettre aux contractants ou aux contractants éventuels de l'une des Parties toute information classifiée transmise par l'autre Partie, conformément à ses lois et réglementations nationales, la Partie destinataire s'assure que les contractants ou les contractants éventuels sont en mesure de protéger de façon appropriée les informations classifiées et :

a) exécute une procédure d'habilitation de sécurité d'établissement appropriée à l'égard des contractants et des sous-traitants ;

b) exécute une procédure d'habilitation de sécurité individuelle appropriée à l'égard de tous les membres du personnel dont les fonctions requièrent un accès à des informations classifiées ;

c) s'assure que toutes les personnes ayant accès à des informations classifiées sont tenues informées de leurs responsabilités ;

d) réalise des inspections de sécurité périodiques au sein des établissements pertinents ayant obtenu une habilitation.

9.6. Les sous-traitants engagés au titre de contrats classifiés se conforment aux exigences de sécurité applicables aux contractants.

9.7. Des visites peuvent être convenues entre les autorités nationales de sécurité afin d'analyser l'efficacité des mesures adoptées par un contractant pour garantir la protection des informations classifiées impliquées dans un contrat classifié.

Article 10

Visites

10.1. Les visites impliquant l'accès à des informations classifiées sont soumises à l'autorisation préalable de l'autorité nationale de sécurité de la Partie hôte.

10.2. La demande de visite doit être soumise au minimum trois (3) semaines avant la visite et contenir :

a) le nom, le prénom, la date et le lieu de naissance, et la nationalité du visiteur ;

b) le numéro du passeport ou de la carte d'identité du visiteur ;

c) la qualité du visiteur et le nom de l'organisation représentée ;

d) le niveau de l'habilitation de sécurité individuelle du visiteur, le cas échéant ;

e) le but de la visite ainsi que le programme de travail proposé et la date prévue ;

f) les noms des organisations et des établissements objets de la visite ;

g) le nombre de visites requises et la période concernée ;

h) toutes autres données convenues par les autorités nationales de sécurité.

10.3. Chacune des Parties garantit la protection des données personnelles des visiteurs conformément à ses lois et réglementations nationales.

Article 11

Infraction à la sécurité

11.1. L'autorité nationale de sécurité de la Partie destinataire informe sans délai l'autorité nationale de sécurité de la Partie d'origine de toute infraction à la sécurité avérée ou suspectée.

11.2. L'autorité nationale de sécurité de la Partie destinataire prend toutes les mesures appropriées possibles, conformément à ses lois et réglementations nationales, afin de limiter les conséquences de toute infraction à la sécurité et d'empêcher toute violation ultérieure, et veille à mener une enquête appropriée. Sur demande, l'autorité nationale de sécurité de la Partie d'origine apporte son aide dans le cadre de l'enquête. L'autorité nationale de sécurité de la Partie destinataire communique par écrit à l'autorité nationale de sécurité de la Partie d'origine le résultat des procédures et les mesures correctives entreprises à la suite de la violation.

Article 12

Frais

Chacune des Parties supporte les frais propres encourus du fait de l'application du présent Accord.

Article 13

Règlement des litiges

Tout litige quant à l'interprétation ou l'application du présent Accord est exclusivement résolu par voie de consultation et négociation entre les Parties. Les Parties conviennent que les litiges ne seront pas renvoyés à un quelconque tribunal national ou international aux fins de leur règlement. Dans l'attente de l'accord amiable, les Parties continueront à exécuter leurs obligations découlant du présent Accord.

Article 14

Dispositions finales

14.1. Le présent Accord prend effet le premier jour du deuxième mois qui suit la réception de la dernière des notifications écrites par lesquelles les Parties se sont tenues mutuellement informées, par la voie diplomatique, de l'accomplissement des exigences légales nationales requises pour son entrée en vigueur.

14.2. Le présent Accord peut être modifié d'un commun accord par écrit entre les Parties. Les modifications apportées aux présentes font partie intégrante du présent Accord. Ces modifications entrent en vigueur conformément aux dispositions du paragraphe 1 du présent article.

14.3. Le présent Accord est conclu pour une durée indéterminée. Chaque Partie pourra mettre fin au présent Accord en informant l'autre Partie par écrit via les voies diplomatiques. Dans un tel cas, l'Accord prendra fin au terme d'un délai de six (6) mois à partir de la date de réception de la notification correspondante par l'autre Partie.

14.4. En cas de résiliation du présent Accord, toutes les informations classifiées échangées en vertu des présentes resteront protégées conformément aux clauses des présentes et seront, sur demande, restituées à la Partie d'origine.

FAIT à New York, le 26 septembre 2019, en double exemplaire, chacun en langues française et anglaise, 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 Malte*
Jean ASSELBORN	Carmelo ABELA
Ministre des Affaires étrangères et européennes	*Ministre des Affaires étrangères et de la Promotion du Commerce*

*

AGREEMENT

between the Government of the Grand Duchy of Luxembourg and the Government of the Republic of Malta on mutual protection and exchange of classified information, done at New York, on 26 september 2019

The Government of the Grand Duchy of Luxembourg and the Government of the Republic of Malta (hereinafter referred to as "the Parties"),

Recognizing that effective co-operation in political, economic, military, security, intelligence and any other area may require exchange of Classified Information between the Parties,

Desiring to establish a system regulating the mutual protection of Classified Information generated or exchanged in the course of the cooperation between the Parties or between public and private entities under their jurisdiction.

HAVE AGREED as follows:

Article 1

Objective and Scope

1.1. The objective of this Agreement is to ensure the protection of Classified Information that is commonly generated or exchanged between the Parties or between public and private entities under their jurisdiction and shall be subject to the applicable national laws of the Parties.

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

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

Article 2

Definitions

For the purposes of this Agreement:

2.1. **"Breach of Security"** means an act, or omission, contrary to the national laws and regulations, the result of which leads, or may lead, to disclosure, loss, destruction, misappropriation or any other type of compromise of Classified Information;

2.2. **"Classified Contract"** means an agreement between two or more Contractors or Sub-contractors, which contains or involves Classified Information;

2.3. **"Classified Information"** means any information, document or material regardless of its form, which is exchanged or generated between the Parties in accordance with national laws and regulations of either Party, to which a security classification level has been attributed, which requires protection against unauthorized disclosure, misappropriation, loss; or other kind of compromise.

2.4. **"Contractor"** means an individual, or legal entity, possessing the legal capacity to conclude classified contracts;

2.5. **"Facility Security Clearance"** means the determination by the National Security Authority confirming, in accordance with national laws and regulations, that as to whether the Contractor or Sub-contractor meets the conditions for handling Classified Information and up to which security classification level such contractor or sub-contractor shall be allowed to handle;

2.6. **"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 and for the control of protection of Classified Information generated or exchanged according to this Agreement;

2.7. **"Need-to-know"** means the necessity to have access to Classified Information in the scope of given official duties and/or for the performance of a specific task;

2.8. **"Originating Party"** means the Party, including any entity, which provides Classified Information in accordance with national laws and regulations;

2.9. **"Personnel Security Clearance"** means the determination by the National Security Authority confirming, in accordance with national laws and regulations, as to whether an individual is eligible to have access to Classified Information and up to which security classification level such individual shall be eligible to have access to;

2.10. **"Receiving Party"** means the Party, including any entity, to which Classified Information of the Originating Party is transmitted;

2.11. **"Sub-contractor"** means a Contractor to whom a prime Contractor grants a sub-contract;

2.12. **"Third Party"** means any State, including legal entities and individuals under its jurisdiction, or international organization, which is not a party to this agreement.

Article 3

Security Classification Levels

3.1. The Parties undertake to protect Classified Information exchanged between them and agree to adopt the equivalence of the following security classification levels:

For the Republic of Malta	*For the Grand Duchy of Luxembourg*	*English equivalent*
L-OGHLA SEGRETEZZA	TRÈS SECRET LUX	TOP SECRET
SIGRIET	SECRET LUX	SECRET
KUNFIDENZJALI	CONFIDENTIEL LUX	CONFIDENTIAL
RISTRETT	RESTREINT LUX	RESTRICTED

3.2. The Originating Party may use additional markings indicating special limitations for use of Classified Information. National Security Authorities shall inform each other in writing of any such additional markings.

Article 4

National Security Authorities

4.1. The National Security Authorities of the Parties are:

For the the Republic of Malta:
National Security Authority
Ministry for Home Affairs and National Security (MHAS)
VALLETTA
MALTA

For the Grand Duchy of Luxembourg:
Service de renseignement de l'État
Autorité nationale de Sécurité
LUXEMBOURG

4.2. The Parties shall notify each other through diplomatic channels on changes of the National Security Authorities. Such notice shall not constitute a formal amendment to this Agreement in accordance with Article 14 paragraph 2.

4.3. The National Security Authorities shall inform each other of the laws and regulations in force in their states, as well as any changes regarding the protection of Classified Information generated or exchanged in accordance with this Agreement.

4.4. In order to achieve and maintain equivalent standards of security, the National Security Authorities may provide each other with information about the security standards, procedures and practises for the protection of Classified Information employed by the respective Party.

Article 5

Measures for the protection of Classified Information

5.1. In accordance with national laws and regulations, the Parties shall take all appropriate measures for the protection of Classified Information, which is exchanged or generated under this Agreement. The same level of protection shall be ensured for such Classified Information of the equivalent security classification levels, as defined in Article 3 of this Agreement.

5.2. The Originating Party shall inform the Receiving Party in writing about any change of the security classification level of the transmitted Classified Information, in order to apply the appropriate protection measures.

5.3. Classified Information shall only be made accessible to individuals who are authorized in accordance with national laws and regulations to have access to Classified Information of the equivalent security classification level and who have a Need-to-know or are otherwise duly authorised by virtue of their functions, and who have been briefed accordingly.

5.4. For the purposes of this Agreement, each Party shall recognize the Personnel and Facility Security Clearances issued by the other Party.

5.5. The National Security Authorities may assist each other upon request and in accordance with national laws and regulations in carrying out vetting procedures.

5.6. For the purposes of this Agreement, the National Security Authorities shall inform each other without delay about any revocations of Personnel and Facility Security Clearances, or the alteration of the security classification level, as the case may be.

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

5.8. The Receiving Party shall:

a) not disclose Classified Information to a Third Party without the prior written consent of the Originating Party issued in accordance with national laws and regulations;

b) if deemed appropriate, mark the received Classified Information in accordance with the equivalence set forth in Article 3;

c) not declassify or downgrade the provided Classified Information without the prior written consent of the Originating Party; and

d) use Classified Information only for the purposes that it has been provided for.

Article 6

Transfer of Classified Information

6.1. Classified Information shall be transferred by means of diplomatic or military couriers, or by other means agreed upon in advance by the National Security Authorities, in accordance with national laws and regulations.

6.2. Electronic transmission of Classified Information shall be carried out through certified cryptographic means agreed upon by the Parties.

6.3. If transferred Classified Information is marked SIGRIET / SECRET LUX and above, the Receiving Party shall confirm the receipt in writing. The receipt of other Classified Information shall be confirmed on request.

Article 7

Reproduction and Translation of Classified Information

7.1. Information classified as SIGRIET / SECRET LUX, or above, shall be translated, or reproduced, only in exceptional cases and upon the prior written consent of the Originating Party.

7.2. All reproductions and translations of Classified Information shall be marked with the original markings. Such reproduced or translated information shall be protected in the same way as the original information. The number of reproductions or translations shall be limited to that required for official purposes.

7.3. When making translations and reproductions in accordance with sub-articles (1) and (2), the following procedure shall apply:

(a) the personnel making such translations and reproductions shall be granted the appropriate security clearance; in accordance with their national laws; and

(b) the translations shall clearly indicate in the language of the translation that it contains Classified Information received from the Originating Party.

Article 8

Destruction of Classified Information

8.1. Information classified as L-OGHLA SEGRETEZZA / TRÈS SECRET LUX shall not be destroyed, except in cases referred to in paragraph 4 of this Article. Such Classified Information shall be returned to the Originating Party after it is no longer considered necessary by the Parties.

8.2. Information classified as SIGRIET / SECRET LUX or below shall be destroyed after having been recognized as no longer necessary by the Receiving Party, insofar as to prevent its reconstruction in whole or in part.

8.3. The Receiving Party shall notify the Originating Party about the destruction of information classified as SIGRIET / SECRET LUX.

8.4. In case of a crisis situation, which makes it impossible to protect or return Classified Information generated or exchanged under this Agreement, the Classified Information shall be destroyed immediately. The Receiving Party shall notify the National Security Authorities of both Parties about this destruction as soon as possible.

Article 9

Classified Contracts

9.1. Classified Contracts shall be concluded and implemented in accordance with national laws and regulations.

9.2. Upon request, the National Security Authority of the Receiving Party shall confirm that a proposed Contractor has been issued an appropriate Personnel or Facility Security Clearance. If the proposed Contractor does not hold an appropriate security clearance, the National Security Authority of the Originating Party may request the National Security Authority of the Receiving Party to issue the appropriate security clearance.

9.3. The National Security Authority in which state's territory 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. Periodical security inspections may be carried out by the National Security Authorities.

9.4. A security annex shall be an integral part of each Classified Contract, or sub-contract, by which the Originating Party shall specify which Classified Information is to be released to the Receiving Party, which security classification level has been assigned to that information and the Contractor's obligations to protect the Classified Information. A copy of the security annex shall be sent to the National Security Authority of the Originating Party.

9.5. Prior to release to either Party's Contractors or prospective Contractors of any Classified Information received from the other Party, the Receiving Party shall , in accordance with its national laws and regulations, ensure that Contractors or prospective Contractors can afford adequate security protection to Classified Information and:

a) perform an appropriate Facility Security Clearance procedure of the Contractors and Sub-contractors;

b) perform an appropriate Personnel Security Clearance procedure for all personnel whose duties require access to Classified Information;

c) ensure that all persons having access to Classified Information are informed of their responsibilities;

d) carry out periodic security inspections of relevant security-cleared facilities.

9.6. Sub-contractors engaged in Classified Contracts shall comply with the security requirements applied to the Contractors.

9.7. Visits can be arranged between the National Security Authorities in order to analyze the efficiency of the measures adopted by a Contractor for the protection of Classified Information involved in a Classified Contract.

Article 10

Visits

10.1. Visits that require access to Classified Information shall be subject to the prior written consent by the National Security Authority of the host Party.

10.2. The request for visit shall be submitted at least three (3) weeks prior to the visit and shall contain:

a) visitor's name and surname, date and place of birth, nationality;
b) passport number or another identification card number of the visitor;
c) position of the visitor and name of the organization represented;
d) level of the Personnel Security Clearance of the visitor, if applicable;
e) purpose, proposed working program and planned date of the visit;
f) names of organizations and facilities requested to be visited;
g) number of visits and period required;
h) other data, agreed upon by the National Security Authorities.

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

Article 11

Breach of Security

11.1. The National Security Authority of the Receiving Party shall immediately notify the National Security Authority of the Originating Party of any suspicion or discovery of a Breach of Security.

11.2. The National Security Authority of the Receiving Party shall undertake all possible appropriate measures in accordance with its national laws and regulations so as to limit the consequences of the Breach of Security and to prevent further violations and ensure the appropriate investigation. On request, the National Security Authority of the Originating Party shall provide investigative assistance. The National Security Authority of the Receiving Party shall inform the National Security Authority of the Originating Party of the outcome of the proceedings and the corrective measures undertaken due to the violation.

Article 12

Costs

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

Article 13

Settlement of Disputes

Any dispute regarding the interpretation or application of this Agreement shall be settled exclusively by consultations and negotiations between the Parties. The Parties agree that disputes shall not be referred to any national or international tribunal or court or to any third party for settlement. Meanwhile, the Parties will continue to fulfil the provisions set forth in this Agreement.

Article 14

Final Provisions

14.1. This Agreement shall enter into force on the first day of the second month after the date of the receipt of the latest written notification by which the Parties have notified each other, through diplo-

matic channels, that their national legal requirements necessary for its entry into force have been fulfilled.

14.2. This Agreement may be amended by mutual written consent of the Parties. The amendments shall form an integral part of this Agreement. Such amendments shall enter into force in accordance with the provision of paragraph 1 of this Article.

14.3. This Agreement is being concluded for an indefinite period of time. Either Party may terminate this Agreement by giving the other Party written notice through diplomatic channels. In that case, termination shall take effect six (6) months from the date on which the other Party has received the notice.

14.4. In case of termination of this Agreement, all Classified Information exchanged pursuant to this Agreement shall continue to be protected in accordance with the provisions set forth herein and, upon request, returned to the Originating Party.

DONE at New York, on 26 September 2019, in two originals, each in the French and English languages, all texts being equally authentic. In case of any divergence of interpretation, the English text shall prevail.

For the Government of the Grand Duchy of Luxembourg	*For the Government of the Republic of Malta*
Jean ASSELBORN	Carmelo ABELA
Minister of Foreign and European Affairs	*Minister for Foreign Affairs and Trade Promotion*

*

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 a New York, le 26 septembre 2019

Le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la République de Malte, ci-après dénommés les « Parties »,

Reconnaissant qu'une coopération efficace dans les domaines politique, économique, militaire, de la sécurité ou de l'intelligence, et dans tout autre domaine, peut exiger l'échange d'informations classifiées entre les Parties,

Désirant établir un système régissant la protection réciproque d'informations classifiées, produites ou échangées dans le cadre d'une coopération entre les Parties, ou entre des instances du secteur public et du secteur privé relevant de leur juridiction.

CONVIENNENT ce qui suit :

Article 1

Objet et champ d'application

1.1. Le présent Accord a pour but de garantir la protection des informations classifiées généralement créées ou échangées entre les Parties, ou entre des instances du secteur public et du secteur privé relevant de leur juridiction, et soumises aux lois nationales applicables des Parties.

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

1.3. Les dispositions du présent Accord s'appliquent également aux informations classifiées déjà produites ou échangées dans le cadre d'une coopération entre les Parties avant l'entrée en vigueur des présentes.

Article 2

Définitions

Aux fins du présent Accord :

2.1. **« Infraction à la sécurité »** désigne tout acte, ou omission, contraire aux lois et réglementations nationales, entraînant ou étant susceptible d'entraîner la divulgation, la perte, la destruction, le détournement ou tout autre type de compromission d'informations classifiées ;

2.2. **« Contrat classifié »** désigne un accord entre deux contractants ou sous-traitants ou plus, qui contient ou implique des informations classifiées ;

2.3. Les **« informations classifiées »** désignent l'ensemble des informations, documents ou matériels, quelle qu'en soit la forme, échangés ou produits entre les Parties conformément aux lois et réglementations nationales de chacune des Parties, auxquels un niveau de classification de sécurité a été attribué et nécessitant une protection contre toute divulgation non autorisée, détournement ou perte, ou tout autre type de compromission ;

2.4. **« Contractant »** désigne toute personne physique ou morale dotée de la capacité juridique de conclure des contrats classifiés ;

2.5. **« Habilitation de sécurité d'établissement »** désigne toute décision de l'autorité de sécurité nationale confirmant que le contractant ou le sous-traitant satisfait aux exigences requises pour traiter des informations classifiées et définissant le niveau de classification de sécurité des informations classifiées qu'il est autorisé à traiter ;

2.6. **« 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 et de contrôler la protection des informations classifiées produites ou échangées en vertu des présentes ;

2.7. **« Besoin d'en connaître »** fait référence à la nécessité d'accéder à des informations classifiées dans le cadre de fonctions officielles déterminées et/ou en vue de l'accomplissement d'une mission spécifique ;

2.8. **« Partie d'origine »** désigne la Partie, en ce compris toute instance, qui fournit des informations classifiées conformément aux lois et réglementations nationales ;

2.9. **« Habilitation de sécurité individuelle »** désigne toute décision de l'autorité de sécurité nationale confirmant qu'un ressortissant est autorisé à accéder à des informations classifiées et définissant le niveau de classification de sécurité des informations classifiées auxquelles il est autorisé à accéder, conformément aux lois et réglementations nationales ;

2.10. **« Partie destinataire »** désigne la Partie, en ce compris toute instance, à laquelle la Partie d'origine transmet des informations classifiées ;

2.11. Un **« sous-traitant »** désigne tout contractant avec lequel le premier contractant conclut un contrat de sous-traitance ;

2.12. Une **« tierce partie »** désigne tout État, en ce compris les personnes physiques ou morales relevant de la juridiction de cet État, ou toute organisation internationale, qui n'est pas l'une des Parties au présent Accord.

Article 3

Niveaux de classification de sécurité

3.1. Les Parties s'engagent à protéger les informations classifiées qu'elles échangent et acceptent d'adopter des niveaux de classification de sécurité équivalents aux niveaux mentionnés ci-après :

Pour la République de Malte	*Pour le Grand-Duché de Luxembourg*	*Équivalent en anglais*
L-OGHLA SEGRETEZZA	TRÈS SECRET LUX	TOP SECRET
SIGRIET	SECRET LUX	SECRET
KUNFIDENZJALI	CONFIDENTIEL LUX	CONFIDENTIAL
RISTRETT	RESTREINT LUX	RESTRICTED

3.2. La Partie d'origine peut recourir à des marquages supplémentaires afin de signaler que des restrictions spéciales s'appliquent à l'utilisation d'informations classifiées. Les autorités nationales de sécurité s'informent mutuellement par écrit de l'utilisation de ces éventuels marquages supplémentaires.

Article 4

Autorités nationales de sécurité

4.1. Les autorités nationales de sécurité des Parties sont :

Pour la République de Malte :

Autorité nationale de sécurité

Ministère de l'Intérieur et de la Sécurité nationale (MHAS)

LA VALETTE

MALTE

Pour le Grand-Duché de Luxembourg :

Le Service de Renseignement de l'État

Autorité nationale de Sécurité

LUXEMBOURG

4.2. Les Parties se tiennent mutuellement informées, par la voie diplomatique, de toute modification affectant les autorités nationales de sécurité. Une telle notification de modification ne constitue pas un amendement officiel aux présentes, conformément au paragraphe 2 de l'article 14.

4.3. Les autorités nationales de sécurité se tiennent mutuellement informées des lois et réglementations en vigueur dans leur État, ainsi que de toute modification ayant trait à la protection des informations classifiées produites ou échangées conformément au présent Accord.

4.4. En vue d'appliquer et de maintenir des normes de sécurité équivalentes, les autorités nationales de sécurité se tiennent mutuellement informées des normes, procédures et pratiques de sécurité appliquées par chaque Partie en matière de protection des informations classifiées.

Article 5

Mesures applicables à la protection d'informations classifiées

5.1. Conformément aux dispositions des lois et réglementations nationales, les Parties prennent toutes les mesures appropriées afin de protéger les informations classifiées échangées ou produites en vertu du présent Accord. Elles garantissent auxdites informations classifiées un niveau de protection équivalent à celui qui est accordé à leurs informations classifiées nationales assorties du niveau de classification de sécurité correspondant, tel que défini à l'article 3 du présent Accord.

5.2. La Partie d'origine informe par écrit la Partie destinataire de toute modification apportée au niveau de classification de sécurité des informations classifiées transmises afin de mettre en œuvre les mesures de protection appropriées.

5.3. L'accès aux informations classifiées est exclusivement réservé aux personnes autorisées, en vertu des lois et réglementations nationales ou de par leurs fonctions, à accéder à des informations classifiées

d'un niveau de classification de sécurité équivalent, qui ont besoin de connaître de telles informations et ont été informées en conséquence.

5.4. Aux fins du présent Accord, chacune des Parties reconnaît les habilitations de sécurité individuelles et d'établissement établies par l'autre Partie.

5.5. Sur demande, et conformément aux lois et réglementations nationales, les autorités nationales de sécurité peuvent s'assister mutuellement dans le cadre de la réalisation des procédures de vérification.

5.6. Aux fins 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, selon le cas.

5.7. Sur demande de l'autorité nationale de sécurité de la Partie d'origine, l'autorité nationale de sécurité de la Partie destinataire confirmera par écrit qu'une personne s'est vue octroyer une habilitation de sécurité individuelle ou qu'une entité juridique s'est vue octroyer une habilitation de sécurité d'établissement.

5.8. La Partie destinataire :

a) ne divulgue aucune information classifiée à une tierce partie sans l'accord écrit de la Partie d'origine délivré conformément aux lois et réglementations nationales ;

b) si cela s'avère approprié, classifie les informations reçues conformément au niveau de sécurité équivalent mentionné à l'article 3 ;

c) ne déclassifie aucune des informations classifiées fournies et s'interdit de leur octroyer un niveau de protection inférieur sans l'accord écrit de la Partie d'origine ; et

d) n'utilise les informations classifiées qu'aux fins prévues.

Article 6

Transfert d'informations classifiées

6.1. Les informations classifiées seront transférées par des coursiers diplomatiques ou militaires ou par tout autre moyen approuvé préalablement par les autorités nationales de sécurité, conformément aux lois et réglementations nationales.

6.2. La transmission électronique d'informations classifiées est effectuée par le biais de méthodes cryptographiques certifiées, acceptées par les Parties.

6.3. Si des informations classifiées transmises sont identifiées comme étant de niveau SIGRIET/ SECRET LUX ou d'un niveau supérieur, la Partie destinataire en confirmera la réception par écrit. La réception des autres informations classifiées sera confirmée sur demande.

Article 7

Reproduction et traduction d'informations classifiées

7.1. La traduction ou la reproduction d'informations classifiées de niveau SIGRIET / SECRET LUX, ou de niveau supérieur, sont autorisées uniquement dans des cas exceptionnels, avec l'accord écrit préalable de la Partie d'origine.

7.2. Toutes les reproductions et les traductions d'informations classifiées portent les marquages de classification originaux. Ces informations reproduites ou traduites sont soumises au même niveau de protection que les informations originales. Le nombre de reproductions ou de traductions est limité à celui requis pour un usage officiel.

7.3. La procédure définie ci-après s'applique aux traductions ou aux reproductions réalisées conformément aux alinéas (1) et (2) :

(a) le personnel chargé d'effectuer ces traductions et ces reproductions doit détenir une habilitation de sécurité appropriée, conformément aux lois nationales applicables ; et

(b) les traductions indiquent clairement dans la langue de traduction qu'elles contiennent des informations classifiées reçues de la Partie d'origine.

Article 8

Destruction d'informations classifiées

8.1. Les informations classifiées de niveau L-OGHLA SEGRETEZZA / TRÈS SECRET LUX ne seront pas détruites, sauf dans les cas mentionnés au paragraphe 4 du présent article. Ces informations classifiées seront renvoyées à la Partie d'origine dès lors que les Parties les jugent inutiles.

8.2. Dès lors que la Partie destinataire n'en a plus l'utilité, les informations classifiées de niveau SIGRIET / SECRET LUX ou de niveau inférieur seront détruites dans la mesure requise pour empêcher leur reconstruction en tout ou partie.

8.3. La Partie destinataire informe la Partie d'origine de la destruction des informations classifiées SIGRIET /SECRET LUX.

8.4. Dans le cas d'une situation de crise rendant impossible la protection ou le renvoi des informations classifiées produites ou échangées en vertu du présent Accord, les informations classifiées sont détruites immédiatement. La Partie destinataire avise dès que possible les autorités nationales de sécurité des deux Parties d'une telle destruction.

Article 9

Contrats classifiés

9.1. Les contrats classifiés seront conclus et exécutés conformément aux lois et réglementations nationales.

9.2. Sur demande, l'autorité nationale de sécurité de la Partie destinataire confirmera qu'un Contractant proposé s'est vu octroyer une habilitation de sécurité individuelle ou d'établissement appropriée. Si le Contractant proposé ne détient pas l'habilitation de sécurité appropriée, l'autorité nationale de sécurité de la Partie d'origine peut demander à celle de la Partie destinataire d'établir une telle habilitation.

9.3. Il incombe à l'autorité nationale de sécurité 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. Des inspections périodiques de la sécurité pourront être effectuées par les autorités nationales de sécurité.

9.4. Une annexe relative à la sécurité fera partie intégrante de chaque contrat ou contrat de sous-traitance classifié. Dans cette annexe, la Partie d'origine spécifiera les informations classifiées qui doivent être divulguées à la Partie destinataire, le niveau de classification de sécurité qui leur a été attribué, ainsi que les obligations qui incombent au contractant eu égard à la protection des informations classifiées. Une copie de l'annexe relative à la sécurité sera transmise à l'autorité nationale de sécurité de la Partie d'origine.

9.5. Avant de transmettre aux contractants ou aux contractants éventuels de l'une des Parties toute information classifiée transmise par l'autre Partie, conformément à ses lois et réglementations nationales, la Partie destinataire s'assure que les contractants ou les contractants éventuels sont en mesure de protéger de façon appropriée les informations classifiées et :

a) exécute une procédure d'habilitation de sécurité d'établissement appropriée à l'égard des contractants et des sous-traitants ;

b) exécute une procédure d'habilitation de sécurité individuelle appropriée à l'égard de tous les membres du personnel dont les fonctions requièrent un accès à des informations classifiées ;

c) s'assure que toutes les personnes ayant accès à des informations classifiées sont tenues informées de leurs responsabilités ;

d) réalise des inspections de sécurité périodiques au sein des établissements pertinents ayant obtenu une habilitation.

9.6. Les sous-traitants engagés au titre de contrats classifiés se conforment aux exigences de sécurité applicables aux contractants.

9.7. Des visites peuvent être convenues entre les autorités nationales de sécurité afin d'analyser l'efficacité des mesures adoptées par un contractant pour garantir la protection des informations classifiées impliquées dans un contrat classifié.

Article 10

Visites

10.1. Les visites impliquant l'accès à des informations classifiées sont soumises à l'autorisation préalable de l'autorité nationale de sécurité de la Partie hôte.

10.2. La demande de visite doit être soumise au minimum trois (3) semaines avant la visite et contenir :

a) le nom, le prénom, la date et le lieu de naissance, et la nationalité du visiteur ;

b) le numéro du passeport ou de la carte d'identité du visiteur ;

c) la qualité du visiteur et le nom de l'organisation représentée ;

d) le niveau de l'habilitation de sécurité individuelle du visiteur, le cas échéant ;

e) le but de la visite ainsi que le programme de travail proposé et la date prévue ;

f) les noms des organisations et des établissements objets de la visite ;

g) le nombre de visites requises et la période concernée ;

h) toutes autres données convenues par les autorités nationales de sécurité.

10.3. Chacune des Parties garantit la protection des données personnelles des visiteurs conformément à ses lois et réglementations nationales.

Article 11

Infraction à la sécurité

11.1. L'autorité nationale de sécurité de la Partie destinataire informe sans délai l'autorité nationale de sécurité de la Partie d'origine de toute infraction à la sécurité avérée ou suspectée.

11.2. L'autorité nationale de sécurité de la Partie destinataire prend toutes les mesures appropriées possibles, conformément à ses lois et réglementations nationales, afin de limiter les conséquences de toute infraction à la sécurité et d'empêcher toute violation ultérieure, et veille à mener une enquête appropriée. Sur demande, l'autorité nationale de sécurité de la Partie d'origine apporte son aide dans le cadre de l'enquête. L'autorité nationale de sécurité de la Partie destinataire communique par écrit à l'autorité nationale de sécurité de la Partie d'origine le résultat des procédures et les mesures correctives entreprises à la suite de la violation.

Article 12

Frais

Chacune des Parties supporte les frais propres encourus du fait de l'application du présent Accord.

Article 13

Règlement des litiges

Tout litige quant à l'interprétation ou l'application du présent Accord est exclusivement résolu par voie de consultation et négociation entre les Parties. Les Parties conviennent que les litiges ne seront pas renvoyés à un quelconque tribunal national ou international aux fins de leur règlement. Dans l'attente de l'accord amiable, les Parties continueront à exécuter leurs obligations découlant du présent Accord.

Article 14

Dispositions finales

14.1. Le présent Accord prend effet le premier jour du deuxième mois qui suit la réception de la dernière des notifications écrites par lesquelles les Parties se sont tenues mutuellement informées, par la voie diplomatique, de l'accomplissement des exigences légales nationales requises pour son entrée en vigueur.

14.2. Le présent Accord peut être modifié d'un commun accord par écrit entre les Parties. Les modifications apportées aux présentes font partie intégrante du présent Accord. Ces modifications entrent en vigueur conformément aux dispositions du paragraphe 1 du présent article.

14.3. Le présent Accord est conclu pour une durée indéterminée. Chaque Partie pourra mettre fin au présent Accord en informant l'autre Partie par écrit via les voies diplomatiques. Dans un tel cas, l'Accord prendra fin au terme d'un délai de six (6) mois à partir de la date de réception de la notification correspondante par l'autre Partie.

14.4. En cas de résiliation du présent Accord, toutes les informations classifiées échangées en vertu des présentes resteront protégées conformément aux clauses des présentes et seront, sur demande, restituées à la Partie d'origine.

FAIT à New York, le 26 septembre 2019, en double exemplaire, chacun en langues française et anglaise, 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 Malte*
Jean ASSELBORN	Carmelo ABELA
Ministre des Affaires étrangères et européennes	*Ministre des Affaires étrangères et de la Promotion du Commerce*

*

AGREEMENT

between the Government of the Grand Duchy of Luxembourg and the Government of the Republic of Malta on mutual protection and exchange of classified information, done at New York, on 26 september 2019

The Government of the Grand Duchy of Luxembourg and the Government of the Republic of Malta (hereinafter referred to as "the Parties"),

Recognizing that effective co-operation in political, economic, military, security, intelligence and any other area may require exchange of Classified Information between the Parties,

Desiring to establish a system regulating the mutual protection of Classified Information generated or exchanged in the course of the cooperation between the Parties or between public and private entities under their jurisdiction.

HAVE AGREED as follows:

Article 1

Objective and Scope

1.1. The objective of this Agreement is to ensure the protection of Classified Information that is commonly generated or exchanged between the Parties or between public and private entities under their jurisdiction and shall be subject to the applicable national laws of the Parties.

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

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

Article 2

Definitions

For the purposes of this Agreement:

2.1. **"Breach of Security"** means an act, or omission, contrary to the national laws and regulations, the result of which leads, or may lead, to disclosure, loss, destruction, misappropriation or any other type of compromise of Classified Information;

2.2. **"Classified Contract"** means an agreement between two or more Contractors or Sub-contractors, which contains or involves Classified Information;

2.3. **"Classified Information"** means any information, document or material regardless of its form, which is exchanged or generated between the Parties in accordance with national laws and regulations of either Party, to which a security classification level has been attributed, which requires protection against unauthorized disclosure, misappropriation, loss; or other kind of compromise.

2.4. **"Contractor"** means an individual, or legal entity, possessing the legal capacity to conclude classified contracts;

2.5. **"Facility Security Clearance"** means the determination by the National Security Authority confirming, in accordance with national laws and regulations, that as to whether the Contractor or Sub-contractor meets the conditions for handling Classified Information and up to which security classification level such contractor or sub-contractor shall be allowed to handle;

2.6. **"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 and for the control of protection of Classified Information generated or exchanged according to this Agreement;

2.7. **"Need-to-know"** means the necessity to have access to Classified Information in the scope of given official duties and/or for the performance of a specific task;

2.8. **"Originating Party"** means the Party, including any entity, which provides Classified Information in accordance with national laws and regulations;

2.9. **"Personnel Security Clearance"** means the determination by the National Security Authority confirming, in accordance with national laws and regulations, as to whether an individual is eligible to have access to Classified Information and up to which security classification level such individual shall be eligible to have access to;

2.10. **"Receiving Party"** means the Party, including any entity, to which Classified Information of the Originating Party is transmitted;

2.11. **"Sub-contractor"** means a Contractor to whom a prime Contractor grants a sub-contract;

2.12. **"Third Party"** means any State, including legal entities and individuals under its jurisdiction, or international organization, which is not a party to this agreement.

Article 3

Security Classification Levels

3.1. The Parties undertake to protect Classified Information exchanged between them and agree to adopt the equivalence of the following security classification levels:

For the Republic of Malta	*For the Grand Duchy of Luxembourg*	*English equivalent*
L-OGHLA SEGRETEZZA	TRÈS SECRET LUX	TOP SECRET
SIGRIET	SECRET LUX	SECRET
KUNFIDENZJALI	CONFIDENTIEL LUX	CONFIDENTIAL
RISTRETT	RESTREINT LUX	RESTRICTED

3.2. The Originating Party may use additional markings indicating special limitations for use of Classified Information. National Security Authorities shall inform each other in writing of any such additional markings.

Article 4

National Security Authorities

4.1. The National Security Authorities of the Parties are:

For the the Republic of Malta:
National Security Authority
Ministry for Home Affairs and National Security (MHAS)
VALLETTA
MALTA

For the Grand Duchy of Luxembourg:
Service de renseignement de l'État
Autorité nationale de Sécurité
LUXEMBOURG

4.2. The Parties shall notify each other through diplomatic channels on changes of the National Security Authorities. Such notice shall not constitute a formal amendment to this Agreement in accordance with Article 14 paragraph 2.

4.3. The National Security Authorities shall inform each other of the laws and regulations in force in their states, as well as any changes regarding the protection of Classified Information generated or exchanged in accordance with this Agreement.

4.4. In order to achieve and maintain equivalent standards of security, the National Security Authorities may provide each other with information about the security standards, procedures and practises for the protection of Classified Information employed by the respective Party.

Article 5

Measures for the protection of Classified Information

5.1. In accordance with national laws and regulations, the Parties shall take all appropriate measures for the protection of Classified Information, which is exchanged or generated under this Agreement.

The same level of protection shall be ensured for such Classified Information of the equivalent security classification levels, as defined in Article 3 of this Agreement.

5.2. The Originating Party shall inform the Receiving Party in writing about any change of the security classification level of the transmitted Classified Information, in order to apply the appropriate protection measures.

5.3. Classified Information shall only be made accessible to individuals who are authorized in accordance with national laws and regulations to have access to Classified Information of the equivalent security classification level and who have a Need-to-know or are otherwise duly authorised by virtue of their functions, and who have been briefed accordingly.

5.4. For the purposes of this Agreement, each Party shall recognize the Personnel and Facility Security Clearances issued by the other Party.

5.5. The National Security Authorities may assist each other upon request and in accordance with national laws and regulations in carrying out vetting procedures.

5.6. For the purposes of this Agreement, the National Security Authorities shall inform each other without delay about any revocations of Personnel and Facility Security Clearances, or the alteration of the security classification level, as the case may be.

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

5.8. The Receiving Party shall:

a) not disclose Classified Information to a Third Party without the prior written consent of the Originating Party issued in accordance with national laws and regulations;

b) if deemed appropriate, mark the received Classified Information in accordance with the equivalence set forth in Article 3;

c) not declassify or downgrade the provided Classified Information without the prior written consent of the Originating Party; and

d) use Classified Information only for the purposes that it has been provided for.

Article 6

Transfer of Classified Information

6.1. Classified Information shall be transferred by means of diplomatic or military couriers, or by other means agreed upon in advance by the National Security Authorities, in accordance with national laws and regulations.

6.2. Electronic transmission of Classified Information shall be carried out through certified cryptographic means agreed upon by the Parties.

6.3. If transferred Classified Information is marked SIGRIET / SECRET LUX and above, the Receiving Party shall confirm the receipt in writing. The receipt of other Classified Information shall be confirmed on request.

Article 7

Reproduction and Translation of Classified Information

7.1. Information classified as SIGRIET / SECRET LUX, or above, shall be translated, or reproduced, only in exceptional cases and upon the prior written consent of the Originating Party.

7.2. All reproductions and translations of Classified Information shall be marked with the original markings. Such reproduced or translated information shall be protected in the same way as the original information. The number of reproductions or translations shall be limited to that required for official purposes.

7.3. When making translations and reproductions in accordance with sub-articles (1) and (2), the following procedure shall apply:

(a) the personnel making such translations and reproductions shall be granted the appropriate security clearance; in accordance with their national laws; and

(b) the translations shall clearly indicate in the language of the translation that it contains Classified Information received from the Originating Party.

Article 8

Destruction of Classified Information

8.1. Information classified as L-OGHLA SEGRETEZZA / TRÈS SECRET LUX shall not be destroyed, except in cases referred to in paragraph 4 of this Article. Such Classified Information shall be returned to the Originating Party after it is no longer considered necessary by the Parties.

8.2. Information classified as SIGRIET / SECRET LUX or below shall be destroyed after having been recognized as no longer necessary by the Receiving Party, insofar as to prevent its reconstruction in whole or in part.

8.3. The Receiving Party shall notify the Originating Party about the destruction of information classified as SIGRIET / SECRET LUX.

8.4. In case of a crisis situation, which makes it impossible to protect or return Classified Information generated or exchanged under this Agreement, the Classified Information shall be destroyed immediately. The Receiving Party shall notify the National Security Authorities of both Parties about this destruction as soon as possible.

Article 9

Classified Contracts

9.1. Classified Contracts shall be concluded and implemented in accordance with national laws and regulations.

9.2. Upon request, the National Security Authority of the Receiving Party shall confirm that a proposed Contractor has been issued an appropriate Personnel or Facility Security Clearance. If the proposed Contractor does not hold an appropriate security clearance, the National Security Authority of the Originating Party may request the National Security Authority of the Receiving Party to issue the appropriate security clearance.

9.3. The National Security Authority in which state's territory 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. Periodical security inspections may be carried out by the National Security Authorities.

9.4. A security annex shall be an integral part of each Classified Contract, or sub-contract, by which the Originating Party shall specify which Classified Information is to be released to the Receiving Party, which security classification level has been assigned to that information and the Contractor's obligations to protect the Classified Information. A copy of the security annex shall be sent to the National Security Authority of the Originating Party.

9.5. Prior to release to either Party's Contractors or prospective Contractors of any Classified Information received from the other Party, the Receiving Party shall , in accordance with its national laws and regulations, ensure that Contractors or prospective Contractors can afford adequate security protection to Classified Information and:

a) perform an appropriate Facility Security Clearance procedure of the Contractors and Sub-contractors;

b) perform an appropriate Personnel Security Clearance procedure for all personnel whose duties require access to Classified Information;

c) ensure that all persons having access to Classified Information are informed of their responsibilities;

d) carry out periodic security inspections of relevant security-cleared facilities.

9.6. Sub-contractors engaged in Classified Contracts shall comply with the security requirements applied to the Contractors.

9.7. Visits can be arranged between the National Security Authorities in order to analyze the efficiency of the measures adopted by a Contractor for the protection of Classified Information involved in a Classified Contract.

Article 10

Visits

10.1. Visits that require access to Classified Information shall be subject to the prior written consent by the National Security Authority of the host Party.

10.2. The request for visit shall be submitted at least three (3) weeks prior to the visit and shall contain:

a) visitor's name and surname, date and place of birth, nationality;

b) passport number or another identification card number of the visitor;

c) position of the visitor and name of the organization represented;

d) level of the Personnel Security Clearance of the visitor, if applicable;

e) purpose, proposed working program and planned date of the visit;

f) names of organizations and facilities requested to be visited;

g) number of visits and period required;

h) other data, agreed upon by the National Security Authorities.

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

Article 11

Breach of Security

11.1. The National Security Authority of the Receiving Party shall immediately notify the National Security Authority of the Originating Party of any suspicion or discovery of a Breach of Security.

11.2. The National Security Authority of the Receiving Party shall undertake all possible appropriate measures in accordance with its national laws and regulations so as to limit the consequences of the Breach of Security and to prevent further violations and ensure the appropriate investigation. On request, the National Security Authority of the Originating Party shall provide investigative assistance. The National Security Authority of the Receiving Party shall inform the National Security Authority of the Originating Party of the outcome of the proceedings and the corrective measures undertaken due to the violation.

Article 12

Costs

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

Article 13

Settlement of Disputes

Any dispute regarding the interpretation or application of this Agreement shall be settled exclusively by consultations and negotiations between the Parties. The Parties agree that disputes shall not be referred to any national or international tribunal or court or to any third party for settlement. Meanwhile, the Parties will continue to fulfil the provisions set forth in this Agreement.

Article 14

Final Provisions

14.1. This Agreement shall enter into force on the first day of the second month after the date of the receipt of the latest written notification by which the Parties have notified each other, through diplomatic channels, that their national legal requirements necessary for its entry into force have been fulfilled.

14.2. This Agreement may be amended by mutual written consent of the Parties. The amendments shall form an integral part of this Agreement. Such amendments shall enter into force in accordance with the provision of paragraph 1 of this Article.

14.3. This Agreement is being concluded for an indefinite period of time. Either Party may terminate this Agreement by giving the other Party written notice through diplomatic channels. In that case, termination shall take effect six (6) months from the date on which the other Party has received the notice.

14.4. In case of termination of this Agreement, all Classified Information exchanged pursuant to this Agreement shall continue to be protected in accordance with the provisions set forth herein and, upon request, returned to the Originating Party.

DONE at New York, on 26 September 2019, in two originals, each in the French and English languages, all texts being equally authentic. In case of any divergence of interpretation, the English text shall prevail.

For the Government of the
Grand Duchy of Luxembourg
Jean ASSELBORN
Minister of Foreign
and European Affairs

For the Government of the
Republic of Malta
Carmelo ABELA
Minister for Foreign Affairs
and Trade Promotion

Impression: CTIE – Division Imprimés et Fournitures de bureau