N° 6962

CHAMBRE DES DEPUTES

Session ordinaire 2015-2016

P R O J E T D E L O I

portant approbation

- **de l'Accord entre le Gouvernement du Grand-Duché du 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;**
- **de l'Accord entre le Gouvernement du Grand-Duché du 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**

* * *

(Dépôt: le 3.3.2016)

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 du 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;
– de l'Accord entre le Gouvernement du Grand-Duché du 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.

Palais de Luxembourg, le 23 février 2016

Le Ministre des Affaires étrangères et européennes,
Jean ASSELBORN

HENRI

*

TEXTE DU PROJET DE LOI

Art. 1er.– Est approuvé l'Accord entre le Gouvernement du Grand-Duché du 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.

Art. 2.– Est approuvé l'Accord entre le Gouvernement du Grand-Duché du 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.

*

EXPOSE DES MOTIFS

L'objet des accords conclus avec le Royaume-Uni et la République de Chypre consiste à créer la toile de fond et le cadre juridique dans lequel s'inscrit l'échange d'informations et de matériels classifiés.

Ces accords s'inscrivent dans le cadre de la liste des accords de sécurité déjà approuvés (reprise sub III) et de toute une série de projets bilatéraux que le Gouvernement se propose de conclure et dont la trame est identique.

Les accords se limitent à énoncer quelques principes de base qui ont traditionnellement cours en la matière ainsi que quelques règles d'ordre procédural et doit être mis en corrélation avec les législations nationales respectives des Etats parties relatives à la protection des informations classifiées au sens de l'accord auxquelles l'accord renvoit d'ailleurs expressément, et qui constituent la substantifique moelle du régime de protection des informations visées par ces accords bilatéraux.

Comme la loi luxembourgeoise relative à la classification des pièces et aux habilitations de sécurité est de date plutôt récente (15 juin 2004), le Luxembourg n'était pas encore en mesure jusqu'à présent de conclure un tel accord bilatéral faute de législation nationale servant d'ossature à la protection des documents classifiés transmis au Luxembourg par l'autre Etat-partie à l'accord bilatéral.

I. L'essentiel du contenu de l'accord de sécurité

Quant au régime de protection des documents classifiés, les Etats-Parties s'engagent à apporter aux informations leur transmises par l'autre Etat-Partie un niveau de protection équivalent à celui accordé à leurs propres informations classifiées nationales de niveau équivalent, tel que celui-ci est défini dans le cadre d'un tableau d'équivalence, en apposant, dès réception des informations classifiées en provenance de la partie d'origine, leur propre classification nationale conformément aux équivalences arrêtées par l'accord bilatéral.

Quant au fond de cet accord, le Gouvernement tient à mettre en exergue quelques règles substantielles qui en constituent la trame.

Concernant l'accès aux informations classifiées, les Parties tiennent à le réserver strictement aux ressortissants des Parties qui se sont vus accorder une habilitation de niveau approprié et dont la fonction rend l'accès essentiel sur la base du principe du besoin d'en connaître.

Par ailleurs, il y a lieu de relever que les Parties généralement reconnaissent mutuellement les habilitations de sécurité délivrées à leurs ressortissants dans le cadre de l'accès aux informations classifiées.

Il s'y ajoute que les informations classifiées ne peuvent être utilisées à des fins autres que celles pour lesquelles elles sont transmises, prévues par les accords ou instruments contractuels conclus entre les parties.

Quant à l'utilisation d'informations classifiées, une règle-clé est de rigueur à savoir celle qui interdit à la Partie destinataire de divulguer des informations classifiées échangées ou élaborées dans le cadre de ces accords à un Etat tiers, une organisation internationale, une entité ou à un ressortissant d'un Etat tiers; quel qu'il soit, sans le consentement écrit préalable de l'Autorité nationale de Sécurité ou des Autorités de Sécurité compétentes de la Partie d'origine.

Les visites aux installations de l'une des parties sont généralement régies par un article de l'accord.

Il en est de même des contrats classifiés définis comme étant tout accord dont l'exécution implique l'accès à des informations classsifiées ou la création de telles informations, à savoir tout contrat quel que soit son régime juridique ou sa dénomination dans lequel un candidat ou cocontractant public ou privé est amené à l'occasion de la passation du contrat ou de son exécution à connaître et à détenir dans ses locaux des informations ou supports protégés.

II. La nécessité des accords bilatéraux soumis à approbation

L'Europe reste confrontée de nos jours à de nouvelles menaces qui sont plus variées, moins visibles et moins prévisibles. Parmi les menaces qui pèsent sur notre sécurité, on citera le terrorisme, 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. Aujourd'hui, la sécurité de tout pays est plus que jamais étroitement liée à la protection de son patrimoine économique, industriel, scientifique et financier.

Dans ce contexte, le développement des programmes européens de haute technologie figure au premier plan des préoccupations des responsables de sécurité. Or, tout projet d'un programme européen de haute technologie se concrétise par un échange d'informations. Il représente un fonds commun d'innovations et de progrès.

La conjugaison de tous ces éléments pourrait nous exposer à une menace extrêmement sérieuse. 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.

Or, la prévention constitue une approche pour faire face à ces nouvelles menaces.

Au Luxembourg, la loi 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.

Dans le contexte de la menace persistante et dans une perspective de prévention, le législateur, par le biais de la loi précitée, accorde aux autorités limitativement énumérées à l'article 5 le droit de procéder à la classification, la déclassification et au déclassement de pièces afin de protéger les intérêts relevés par l'article 3 de ladite loi.

Des pièces peuvent partant être classifiées dans tous les domaines visés par l'article 3 et qui peuvent englober plus particulièrement des informations de nature politique militaire, économique ou encore technique.

Encore qu'une classification ne doive être attribuée à une pièce que dans la mesure de ce qui est indispensable en vue de la protection des intérêts dont question à l'article 3, chaque autorité visée par l'article 5, consciente des menaces qui persistent, pourra dans le cadre de la prévention, y mettre du sien, en classant les informations afférentes, avec toutes les conséquences juridiques qui s'y rattachent.

Or, ces mêmes autorités doivent dès lors s'assurer de la protection, notamment physique de ces pièces, plus particulièrement 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.

Or, c'est précisément l'accord bilatéral que le Gouvernement se propose de conclure qui, est appelé à y pourvoir juridiquement.

En conclusion, l'échange de pièces classifiées visés par les présents accords bilatéraux sera régi désormais par cet accord ainsi que par les lois de base nationales que les Etats s'engagent à créer, à l'exception des pièces classifiées tombant sous l'empire d'un régime de protection qui leur est propre, généralement dans un cadre multilatéral, (OTAN, UE, …).

III. La liste des accords de sécurité du Grand-Duché de Luxembourg déjà approuvés en matière de protection des pièces classifiées

1) Loi du 15 juin 2004 portant approbation de l'Accord sur la Sécurité des Informations entre les Parties au Traité de l'Atlantique Nord avec ses annexes 1, 2, et 3 signé par le Luxembourg le 14 juillet 1998.
2) Loi du 14 juin 2005 portant approbation
   - de la Convention portant création d'une Agence spatiale européenne, faite à Paris, le 30 mai 1975;
   - de l'Accord entre les Etats parties à la Convention portant création d'une Agence spatiale européenne et l'Agence spatiale européenne concernant la protection et l'échange d'informations classifiées, fait à Paris, le 19 août 2002;
   - de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et l'Agence spatiale européenne relatif à l'adhésion du Grand-Duché de Luxembourg à la Convention portant création de l'Agence spatiale européenne et des clauses et conditions s'y rapportant, fait à Paris, le 6 mai 2004.
3) Loi du 16 décembre 2008 portant approbation de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la République fédérale d'Allemagne concernant la protection réciproque des informations classifiées, signé à Berlin le 17 janvier 2006.
4) Loi du 16 décembre 2008 portant approbation de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la République française concernant l'échange et la protection réciproque des informations classifiées, signé à Luxembourg, le 24 février 2006.
5) Loi du 16 décembre 2008 portant approbation de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la République de Lettonie concernant l'échange et la protection réciproque des informations classifiées, signé à Luxembourg, le 13 septembre 2007.
6) Loi du 13 mars 2009 portant approbation de l'Accord entre le Grand-Duché de Luxembourg et la République portugaise concernant l'échange et la protection réciproque des informations classifiées, signé à Luxembourg, le 22 février 2008.

7) Loi du 24 juillet 2011 portant approbation de l'Accord entre le Grand-Duché de Luxembourg et le Royaume d'Espagne concernant l'échange et la protection réciproque des informations classifiées, signé à Luxembourg, le 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) Projet de loi portant approbation de
   – Accord de sécurité entre le Gouvernement du Grand-Duché de Luxembourg et la République d'Autriche concernant l'échange et la protection réciproque des informations classifiées entre le Gouvernement du Grand-Duché de Luxembourg, signé à Vienne, le 13 novembre 2014 (1er vote 14 octobre 2015)
   – Accord de sécurité entre le Gouvernement du Grand-Duché de Luxembourg et la République de Croatie concernant l'échange et la protection réciproque des informations classifiées, signé à Luxembourg, le 13 mars 2014 (1er vote 14 october 2015)
12) Projet de loi 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) la protection réciproque des informations classifiées, signé à Luxembourg, le 6 janvier 2015 (1er vote 14 octobre 2015).

*

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

Le Gouvernement du Grand-Duché de Luxembourg

et

le Gouvernement de la République de Chypre

(ci-après dénommés conjointement les „Parties" ou individuellement la „Partie"),

Reconnaissant la nécessité d'établir des règles sur la protection d'Informations classifiées (telles que définies ci-après) échangées dans le cadre de la coopération politique, militaire, économique, juridique, scientifique et technologique ou toute autre sorte de coopération, concernant les intérêts et la sécurité nationaux, ainsi que d'Informations classifiées créées au cours du processus d'une telle coopération,

Entendant assurer la protection réciproque de toutes les Informations classifiées, qui ont été classifiées par l'une des Parties et transférées à l'autre Partie ou généralement créées au cours de la coopération entre les Parties,

Souhaitant établir un cadre juridique sur la protection réciproque d'Informations classifiées échangées entre les Parties,

Compte tenu des intérêts communs dans la protection d'Informations classifiées, conformément à la législation des Parties,

CONVIENNENT ce qui suit:

Article 1

Objectif

Le présent Accord a pour but de garantir la protection des Informations classifiées généralement créées ou échangées entre les Parties.

Article 2

Définitions

Aux fins du présent Accord:

a) *„Infraction à la sécurité"* désigne tout acte ou omission contraire au présent Accord ou à la législation nationale des Parties, susceptible d'entraîner la divulgation, la perte, la destruction, le détournement ou tout autre type de compromission d'Informations classifiées.

b) *„Contrat classifié"* désigne un accord entre deux Contractants ou plus, lequel contient des Informations classifiées ou la mise en oeuvre duquel nécessite l'accès aux Informations classifiées;

c) *„Informations classifiées"* désigne toute information, indépendamment de sa forme ou de sa nature, qui demande une protection contre toute manipulation non autorisée, qui a été classifiée conformément à la législation nationale des Parties et qui a été désignée comme telle selon un niveau de classification de sécurité;

d) *„Autorité compétente"* désigne l'Autorité nationale de sécurité et toute autre instance compétente qui, conformément à la législation nationale des Parties, est responsable de la mise en oeuvre du présent Accord;

e) *„Contractant“* désigne toute personne physique ou morale dotée de la capacité juridique pour conclure des Contrats classifiés;

f) *„Habilitation de sécurité d'établissement“* désigne toute décision de l'Autorité compétente selon laquelle la personne morale et/ou physique possède la capacité physique et organisationnelle de traiter et de stocker des Informations classifiées conformément à sa législation nationale;

g) *„Autorité nationale de sécurité“* désigne l'autorité gouvernementale de chacune des Parties, laquelle conformément à sa législation nationale est responsable de la mise en oeuvre et de la supervision générales du présent Accord; les autorités respectives des Parties sont énumérées à l'article 4, paragraphe I du présent Accord;

h) *„Besoin d'en connaître“* désigne la nécessité d'accéder à des Informations classifiées spécifiques dans le cadre d'une fonction officielle déterminée en vue de l'accomplissement d'une mission spécifique;

i) *„Partie d'origine“* désigne la Partie qui a créé les Informations classifiées;

j) *„Habilitation de sécurité individuelle“* désigne toute décision de l'Autorité compétente selon laquelle le ressortissant est autorisé à accéder à des Informations classifiées conformément à sa législation nationale;

k) *„Partie destinataire“* désigne la Partie à laquelle la Partie d'origine transmet les Informations classifiées;

l) *„Tierce partie“* désigne tout État, y compris instance publique ou privée, organisation, personne physique ou morale, qui n'est pas l'une des Parties au présent Accord.

Article 3

Niveaux de classification de sécurité

1. Toute Information classifiée délivrée en vertu du présent Accord est désignée par un niveau de classification de sécurité approprié conformément aux lois et réglementations nationales des Parties.

2. Les Parties reconnaissent que les niveaux de classification de sécurité suivants sont équivalents et correspondent aux niveaux de classification de sécurité spécifiés dans leur législation nationale:

Pour le Grand-Duché de Luxembourg	*Pour la République de Chypre*	*Equivalent en anglais*
TRES SECRET LUX	ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	TOP SECRET
SECRET LUX	ΑΠΟΡΡΗΤΟ	SECRET
CONFIDENTIEL LUX	ΕΜΠΙΣΤΕΥΤΙΚΟ	CONFIDENTIAL
RESTREINT LUX	ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	RESTRICTED

Article 4

Autorités compétentes

1. Les autorités nationales de sécurité des Parties sont:

Pour le Gouvernement du Grand-Duché de Luxembourg:

Service de Renseignement de l'Etat

Autorité nationale de Sécurité

Pour la République de Chypre:

Autorité nationale de Sécurité

Ministère de la défense de la République de Chypre

2. Les Parties se tiennent mutuellement informées, par voie diplomatique, de toute modification apportée concernant les Autorités nationales de sécurité.

3. Sur demande, les Autorités nationales de sécurité s'informent mutuellement sur les autres Autorités compétentes.

4. Les Autorités nationales de sécurité se tiennent mutuellement informées de leur législation nationale respective traitant des Informations classifiées ainsi que de toute modification significative à celle-ci, et échangent des informations relatives aux normes, procédures et pratiques de sécurité qu'elles appliquent en matière de protection d'Informations classifiées.

Article 5

Mesures de protection et accès aux Informations classifiées

1. Conformément à leur législation nationale, les Parties prennent toutes les mesures appropriées afin de protéger les Informations classifiées échangées ou créées en vertu du présent Accord. Elles apportent auxdites Informations classifiées un niveau de protection au minimum équivalent à celui qui est accordé à leurs Informations classifiées nationales de même niveau de classification de sécurité, conformément à l'article 3.

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.

3. L'accès aux Informations classifiées est réservé aux personnes autorisées, sur la base du „Besoin d'en connaître", à accéder aux Informations classifiées d'un niveau de sécurité équivalent, conformément à la législation nationale des Parties.

4. Dans le cadre du présent Accord, chacune des Parties reconnaît les Habilitations de sécurité individuelles et d'établissement délivrées conformément à la législation nationale de l'autre Partie. Les habilitations de sécurité respectent les équivalences définies à l'article 3.

5. Sur demande et conformément à la législation nationale, les autorités compétentes se prêtent mutuellement assistance dans le cadre de la mise en oeuvre des procédures d'habilitation requises en vertu du présent Accord.

6. Dans le cadre du présent Accord, les Autorités compétentes des Parties se tiennent mutuellement informées sans délai de toute modification apportée aux Habilitations de sécurité individuelles et d'établissement, en particulier de tout déclassement ou déclassification.

7. La Partie destinataire:

a) ne transmet aucune Information classifiée à une Tierce partie sans l'accord écrit préalable de la Partie d'origine;

b) classifie les informations reçues conformément à l'article 3;

c) n'utilise les Informations classifiées qu'aux fins prévues.

Article 6

Transmission des Informations classifiées

1. Les Informations classifiées sont transmises par la voie diplomatique, sauf dispositions contraires convenues par les Autorités nationales de sécurité. La Partie destinataire confirme par écrit la réception des Informations classifiées.

2. La transmission électronique d'Informations classifiées est effectuée par le biais de méthodes cryptographiques certifiées acceptées par les Autorités nationales de sécurité.

Article 7

Reproduction et traduction d'Informations classifiées

1. La traduction et la reproduction d'Informations classifiées se font conformément à la législation nationale de la Partie destinataire et aux procédures suivantes:

a) les traductions et les reproductions sont classifiées et protégées de la même manière que les Informations classifiées originales;

b) les traductions et le nombre de copies sont limités à ceux requis pour un usage officiel;

c) les traductions sont accompagnées d'une note appropriée dans la langue de traduction, indiquant qu'elles contiennent des Informations classifiées reçues de la Partie d'origine.

2. La traduction ou la reproduction des Informations classifiées SECRET LUX/ΑΠΟΡΡΗΤΟ/SECRET ou de niveau supérieur sont autorisées uniquement avec l'accord écrit préalable de la Partie d'origine.

Article 8

Destruction d'Informations classifiées

1. Les Informations classifiées sont détruites de manière à empêcher leur reconstitution intégrale ou partielle.

2. Les Informations classifiées jusqu'au niveau SECRET LUX/ΑΠΟΡΡΗΤΟ/SECRET sont détruites conformément à la législation nationale.

3. Les Informations classifiées TRES SECRET LUX/ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ/TOP SECRET ne sont pas détruites, et sont renvoyées à l'Autorité compétente de la Partie d'origine.

4. Un rapport relatif à la destruction d'Informations classifiées est rédigé et sa traduction en langue anglaise est transmise à l'autorité compétente de la Partie d'origine.

5. Dans le cas d'une situation de crise rendant impossible la protection ou la rétrocession d'Informations classifiées, ces dernières sont immédiatement détruites. La Partie destinataire avise dès que possible l'Autorité de sécurité compétente de la Partie d'origine d'une telle destruction.

Article 9

Contrats classifiés

1. L'Autorité nationale de sécurité d'une Partie qui souhaite conclure un Contrat classifié avec un Contractant de l'autre Partie, ou qui souhaite autoriser l'un de ses propres Contractants à conclure un Contrat classifié sur le territoire de l'autre Partie, reçoit au préalable l'assurance écrite de l'Autorité nationale de sécurité de l'autre Partie que le Contractant proposé est titulaire d'une Habilitation de sécurité d'établissement du niveau de classification de sécurité approprié.

2. Le Contractant soumet toute information concernant d'éventuels sous-contractants en vue de leur approbation par l'Autorité nationale de Sécurité, sur le territoire de laquelle la mission doit être accomplie.

3. Chaque Contrat classifié conclu en vertu du présent Accord inclut:

a) l'engagement du Contractant de garantir que ses locaux disposent des conditions nécessaires au traitement et au stockage d'Informations classifiées d'un niveau de classification de sécurité approprié;

b) l'engagement du Contractant de garantir que les personnes qui exécutent des tâches nécessitant l'accès aux Informations classifiées sont autorisées conformément à la législation nationale à avoir accès aux Informations classifiées d'un niveau de classification de sécurité équivalent;

c) la condition que le Contractant garantisse que toutes les personnes ayant accès aux Informations classifiées sont informées de leurs responsabilités concernant la protection des Informations classifiées, conformément à leur législation nationale;

d) la liste des Informations classifiées et la liste des domaines dans lesquels des Informations classifiées sont susceptibles d'apparaître;

e) la procédure relative à la communication des modifications apportées aux niveaux de classification de sécurité des Informations classifiées;

f) les moyens de communication et les moyens de transmission électroniques;

g) la procédure relative à la transmission d'Informations classifiées;

h) l'engagement du Contractant de communiquer toute infraction à la sécurité avérée ou suspectée;

i) l'engagement du Contractant de transmettre une copie du Contrat classifié à sa propre autorité compétente;

j) l'engagement du sous-traitant de satisfaire aux mêmes obligations de sécurité que celles du Contractant.

4. Dès que les négociations précontractuelles commencent entre les Contractants éventuels, l'Autorité nationale de Sécurité de la Partie d'origine informe l'Autorité nationale de sécurité de l'autre Partie du niveau de classification de sécurité attribué aux Informations classifiées liées auxdites négociations précontractuelles.

5. Une copie de chaque Contrat classifié est transmise à l'Autorité nationale de Sécurité de la Partie sur le territoire de laquelle la mission doit être accomplie en vue de garantir une supervision et un contrôle de sécurité appropriés.

Article 10

Visites

1. Les visites liées aux Contrats classifiés impliquant l'accès à des Informations classifiées sont soumises à l'autorisation écrite préalable de l'Autorité compétente de la Partie hôte.

2. L'Autorité compétente de la Partie hôte reçoit la demande de visite au moins dix jours à l'avance.

3. En cas d'urgence, l'Autorité compétente peut convenir que la demande de visite soit transmise dans un délai plus court.

4. Toute demande de visite contient les renseignements suivants:

a. nom et prénom, date et lieu de naissance, citoyenneté, numéro du passeport ou du document d'identité du visiteur;

b. nom de l'entité juridique que représente le visiteur et fonction du visiteur au sein de l'entité juridique;

c. nom, adresse et coordonnées de l'entité juridique à visiter;

d. confirmation de l'habilitation de sécurité individuelle du visiteur et validité et niveau de cette dernière;

e. objet et but de la visite;

f. date et durée prévues de la visite requise. Dans le cas de visites récurrentes, il convient d'indiquer la période totale couverte par les visites;

g. date, signature et sceau officiel de l'Autorité compétente.

5. Une fois la visite autorisée, l'Autorité compétente de la Partie hôte fournit une copie de la demande de visite aux responsables de la sécurité de l'entité juridique à visiter.

6. L'autorisation de visite est valable un an au maximum.

7. Les Autorités compétentes des Parties peuvent dresser des listes de personnes autorisées à effectuer des visites récurrentes. Les listes sont valides pour une période initiale de douze mois. Les conditions générales des visites respectives sont directement fixées par les points de contact appropriés de l'entité juridique que ces personnes doivent visiter, conformément aux modalités convenues.

Article 11

Infraction à la sécurité

1. En cas d'infraction à la sécurité, l'Autorité nationale de Sécurité de la Partie destinataire en avise dès que possible l'Autorité nationale de sécurité de la Partie d'origine et lance une enquête appropriée.

2. Sur demande, la Partie d'origine coopère à l'enquête, conformément au paragraphe 1.

3. La Partie d'origine est tenue informée des résultats de l'enquête et reçoit le rapport final sur les raisons et l'étendue des dommages.

Article 12

Frais

Chacune des Parties supporte les frais propres encourus du fait de la mise en oeuvre et de la supervision 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 négociation entre les Parties.

Si aucun accord ne peut être conclu selon les modalités énoncées au paragraphe 1, ledit litige devra être résolu par voie diplomatique.

Article 14

Dispositions finales

1. Le présent Accord est conclu pour une durée indéterminée et 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.

2. Le présent Accord peut être modifié à tout moment moyennant l'accord écrit commun des Parties. Les modifications entrent en vigueur conformément au paragraphe 1.

3. Chacune des Parties peut, à tout moment, dénoncer le présent Accord moyennant une notification écrite transmise par la voie diplomatique, auquel cas la dénonciation prend effet six (6) mois à compter de la date de réception de la notification correspondante.

4. Nonobstant la dénonciation du présent Accord, les Parties garantissent que toutes les Informations classifiées continuent d'être protégées jusqu'à ce que la Partie d'origine dispense la Partie destinataire de cette obligation.

5. Le présent Accord ne porte pas préjudice aux droits et obligations des Parties relevant d'autres conventions internationales.

6. Des modalités d'application peuvent être convenues dans le cadre de l'application du présent Accord.

7. A la suite de l'entrée en vigueur du présent Accord, la Partie sur le territoire de laquelle l'Accord est signé prend immédiatement les mesures requises pour procéder à l'enregistrement de ce dernier auprès du Secrétariat des Nations Unies, conformément à l'article 102 de la Charte des Nations Unies et informe l'autre Partie de cet enregistrement et de son numéro d'enregistrement dans le Recueil des traités des Nations Unies dès son émission.

EN FOI DE QUOI, les soussignés, dûment autorisés par leurs Gouvernements respectifs, ont signé le présent Accord.

FAIT à Luxembourg, le 3 septembre 2015 en trois exemplaires, chacun en langues française, grecque 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
(signature)

Pour le Gouvernement de la République de Chypre
(signature)

*

AGREEMENT

between the Government of the Grand Duchy of Luxembourg and the Government of the United Kingdom of Great Britain and Northern Ireland concerning the protection of Classified Information

The Government of the Grand Duchy of Luxembourg and the Government of the United Kingdom of Great Britain and Northern Ireland („the UK") (referred to jointly as the „Parties" or individually as the „Party"), wishing to ensure the protection of Classified Information generated by and/or exchanged between the two Parties or commercial and industrial organisations in either the UK or Luxembourg, through approved channels, have, in the interests of national security, established the following arrangements which are set out in this Agreement.

Article 1

Purpose

The purpose of this Agreement is to ensure the protection of Classified Information (as defined in Article 2 of this Agreement) generated by and/or exchanged between the Parties, between their Contractors (as defined in Article 2 of this Agreement) or between a Party and any Contractor of the other Party, and set out security procedures and arrangements for such protection.

Article 2

Definitions

For the purposes of this Agreement:

a) *„Classified Information"* means any information of whatever form, nature or method of transmission determined, either individually by one Party or jointly by both of the Parties, to require protection against unauthorised disclosure, misappropriation or loss, to which a security classification has been applied and which has been marked accordingly under the national laws and regulations of one or both of the Parties.

b) *„Classified Contract"* means any contract or sub-contract, including any pre-contractual negotiations, which contains or involves access to Classified Information.

c) *„Competent Security Authority (CSA)“* means a government authority which is responsible for implementing the security requirements covered by this Agreement.

d) *„Contract“* means an agreement between two or more parties creating and defining legally enforceable rights and obligations between the parties.

e) *„Contractor“* means a legal entity or person possessing the legal capability to undertake contracts or sub-contracts.

f) *„Facility Security Clearance (FSC)“* means a determination following an investigative procedure stating that a Contractor is authorised to either receive, process or store Classified Information up to a certain classification level.

g) *„Need to Know“* means the necessity for an individual to have access to Classified Information to fulfil their official duties and/or for the performance of a specific task.

h) *„Originator“* means the Party, as well as any public or private legal entity under its authority, which originates and provides the Classified Information. Classified Information produced by a Contractor is owned by a Party.

i) *„Recipient“* means the Party as well as any public or private legal entity under its authority to which the Classified Information is provided by the Originator.

j) *„Personnel Security Clearance (PSC)“* means a determination following an investigative procedure stating that an individual is eligible to have access to Classified Information up to a certain classification level.

k) *„Security Incident“* means an act or omission contrary to national laws and regulations, which may result in the unauthorised access, disclosure, compromise or destruction of Classified Information.

l) *„Third Party“* means a State, international organisation or any other entity which is not a Party to this Agreement or an individual that is not under the jurisdiction of either Party.

Article 3

Security Authorities

1. The security authorities designated by the Parties as ultimately responsible for the security of Classified Information received under this Agreement are the following:

In the United Kingdom of Great Britain and Northern Ireland	*In the Grand Duchy of Luxembourg*
National Security Authority Cabinet Office	Service de Renseignement Autorite nationale de Securite

2. The Parties may designate CSAs which shall be responsible for the implementation of aspects of this Agreement.

3. For the purposes of implementing this Agreement the Parties shall notify each other in writing of their respective CSAs and any significant changes to the CSAs.

Article 4

Security Classification Levels

1. Any Classified Information generated and/or exchanged under this Agreement shall be marked with the appropriate security classification level according to the national laws and regulations of the Party providing the information.

2. The Parties agree that the following security classification levels shall correspond to one another and be considered as equivalent:

In the United Kingdom of Great Britain and Northern Ireland	*In the Grand Duchy of Luxembourg*
UK TOP SECRET	TRES SECRET LUX
UK SECRET	SECRET LUX
No equivalent (see paragraph 3 of this Article)	CONFIDENTIEL LUX
UK OFFICIAL-SENSITIVE	RESTREINT LUX

3. The UK shall afford CONFIDENTIEL LUX Classified Information an equivalent level of protection as it would for UK SECRET Classified Information.

4. In the event that Classified Information at the UK TOP SECRET or TRES SECRET LUX level needs to be generated and/or exchanged, additional arrangements (as provided for in Article 15 of the Agreement) may be agreed between the Parties.

5. Luxembourg shall continue to handle UK CONFIDENTIAL Classified Information generated and/or exchanged by the Parties prior to 2 April 2014 as CONFIDENTIEL LUX, and UK RESTRICTED Classified Information as RESTREINT LUX.

6. The Recipient shall ensure that security classification markings are not altered or revoked, except with the prior written authorisation of the Originator.

Article 5

Protection of Classified Information

1. The Originator shall ensure that the Recipient is informed of
   a) The security classification level of the information provided, and any conditions of release or limitations on its use; and
   b) Any subsequent change in the security classification level.

2. The Recipient shall in accordance with its national laws and regulations:
   a) Provide the Classified Information with an equivalent level of protection as the Recipient would afford to its own information at the equivalent level of security classification;
   b) If deemed appropriate, ensure that Classified Information received is marked with its own equivalent security classification in accordance with Article 4 of this Agreement;
   c) Take all legally available steps to apply the principle of originator consent in accordance with its national laws and regulations;
   d) Ensure that such Classified Information is used solely for the purpose for which it has been provided (unless the Originator expressly consents in writing to a further or different specified use);
   e) Subject to Article 8 of this Agreement, not disclose Classified Information to a Third Party, without the prior written approval of the Originator, and
   f) Ensure that security classifications are not altered or revoked, except as authorised in writing by or on behalf of the Originator.

3. If considered necessary each Party shall allow representatives of the other Party to visit its territory in order to discuss procedures for the protection of Classified Information provided by the other Party.

Article 6

Access to Classified Information

1. Access to Classified Information at the UK TOP SECRET, TRES SECRET LUX, UK SECRET, SECRET LUX or CONFIDENTIEL LUX level shall be limited to those individuals who have a Need

to Know, who hold the nationality of a country of either Party, and who have been granted an appropriate PSC in accordance with national laws and regulations.

2. Access to Classified Information at the UK TOP SECRET, TRES SECRET LUX, UK SECRET, SECRET LUX or CONFIDENTIEL LUX level by an individual not holding the nationality of a country of either Party shall be on the condition that the individual has a Need To Know, has been granted an appropriate PSC in accordance with national laws and regulations, and the Originator has been consulted and given prior written approval for the individual to have access.

3. Access to Classified Information at the UK OFFICIAL-SENSITIVE or RESTREINT LUX level shall be limited to individuals who have a Need to Know. As a minimum, individuals having such access should be subjected to basic recruitment checks which should establish proof of identity; confirm that they satisfy all legal requirements for employment; and verify their employment record. Criminal record checks should also be conducted on the individual if permissible under national laws and regulations of the Recipient. These recruitment checks may be undertaken by Contractors and the requirement for these checks prior to granting access shall be included in the Contract.

4. Individuals who are given access to Classified Information shall be briefed on their responsibilities for the protection of such Classified Information.

Article 7

Transmission of Classified Information

1. Classified Information at the UK TOP SECRET, TRES SECRET LUX, UK SECRET, SECRET LUX or CONFIDENTIEL LUX level shall normally be transmitted between the Parties through official diplomatic Government-to-Government channels unless otherwise agreed by the relevant CSAs in advance.

2. Classified Information at the UK OFFICIAL-SENSITIVE or RESTREINT LUX level shall be transmitted physically in accordance with the national laws and regulations of the Originator, which may include the use of postal services or commercial courier companies.

3. Where large volumes of Classified Information at the UK TOP SECRET, TRES SECRET LUX, UK SECRET, SECRET LUX or CONFIDENTIEL LUX level are to be transmitted as freight, the means of transport, the route and any escort requirement shall be the subject of a transportation plan mutually agreed on a case-by-case basis by the relevant CSAs of both Parties.

4. If Classified Information is to be transmitted electronically within a Party it shall be protected by means applicable to the security classification level of the Classified Information being transmitted.

5. If Classified Information is to be transmitted electronically between the Parties it shall not be sent in clear text. Such transmissions shall be protected by cryptographic means that are mutually accepted by the relevant CSAs of both Parties. However, and only if the Originator approves, Classified Information at the UK OFFICIAL-SENSITIVE level may be transmitted in clear text if suitable cryptographic means are not available.

Article 8

Restrictions on Use and Disclosure

1. Subject to the provisions of paragraph 2 of this Article unless prior written consent is given to the contrary, the Recipient shall not use any Classified Information generated by and/or exchanged under this Agreement except for the purposes and within any limitations stated by or on behalf of the Originator.

2. Within the scope of national laws and regulations regarding public access to information the Recipient shall take all reasonable steps available to it to keep Classified Information generated and/

or exchanged under this Agreement free from disclosure. If there is any request to declassify or disclose any Classified Information generated and/or exchanged under this Agreement the Recipient shall immediately notify the Originator in writing, and both Parties shall consult each other before a decision is taken to release the information.

3. Subject to the provisions of paragraph 2 of this Article, and to the national laws and regulations of the Recipient, Classified Information generated and/or exchanged under this Agreement shall not be disclosed to a Third Party without the prior written approval of the Originator.

Article 9

Translation, Reproduction and Destruction of Classified Information

1. All translations or reproductions of Classified Information shall bear the same security classification markings as the original and be protected accordingly.

2. Individuals undertaking a translation must hold an appropriate PSC.

3. All translations shall contain a suitable annotation, in the language of translation, indicating that they contain Classified Information of the Originator.

4. Information classified as UK TOP SECRET or TRES SECRET LUX shall be reproduced or translated only after obtaining the prior written consent of the Originator.

5. The number of reproductions shall be limited to the minimum required for an official purpose or in the course of a Classified Contract, and shall be made only by individuals who hold an appropriate PSC.

6. When it is no longer considered necessary to retain information for the purpose for which it was provided Classified Information shall either be returned to the Originator, or be destroyed in accordance with the Recipient's national laws or regulations applicable to the security classification level of the information concerned.

7. If a crisis situation makes it impossible for a Recipient to protect Classified Information generated and/or exchanged under this Agreement the Classified Information shall be destroyed using any appropriate means to avoid a Security Incident. The Recipient shall notify the CSA of the Originator in writing should Classified Information provided under this Agreement need to be destroyed in a crisis situation.

8. The Originator may prohibit the creation of translations or reproductions, or the alteration or destruction of Classified Information by giving it an appropriate marking or by attaching a written notice.

Article 10

Visits

1. If a Government official from a Party is required to visit a Government facility of the other Party where access to Classified Information marked UK TOP SECRET, TRES SECRET LUX, UK SECRET, SECRET LUX or CONFIDENTIEL LUX is involved, they must submit details of their PSC to the host facility ahead of such a visit.

2. If a Government official from a Party is required to visit a Contractor facility of the other Party or a Contractor under the jurisdiction of a CSA of one Party is required to visit a Government or Contractor facility where access to Classified Information marked UK TOP SECRET, TRES SECRET LUX, UK SECRET, SECRET LUX or CONFIDENTIEL LUX is involved, the procedure as set out in paragraphs 3, 4, 5 and 6 of this Article shall be applied.

3. Visitors, as referred to in paragraph 2 of this Article, who require access to Classified Information at the level of UK TOP SECRET, TRES SECRET LUX, UK SECRET, SECRET LUX or CONFIDENTIEL LUX shall only be allowed access where they have been:

a) granted an appropriate PSC by the CSA of the requesting Party, have a Need to Know, and are authorised to have access to Classified Information in accordance with the national laws and regulations of the host Party; and

b) authorised by the appropriate CSA of the requesting Party to conduct the required visit or visits.

4. Visit applications shall include at least the following information:

a) Full name of visitor, date and place of birth, nationality and passport or identity card number;

b) Official title of the visitor and the name of the establishment or contractor he/she represents;

c) Date and duration of the requested visit or visits;

d) Purpose of the visit(s) and subject(s) to be discussed;

e) Whether the visit is a Government or commercial initiative and whether the visit is being initiated by the requesting establishment or facility or by the establishment or facility to be visited;

f) Names of establishments and Contractors to be visited;

g) Names of persons in the host Party establishment or facility to be visited;

h) The full name and telephone number of the point of contact or the person with whom the arrangement for the visit has been made;

i) The anticipated security classification level of Classified Information to be involved; and

j) Confirmation and date of expiry of the visitor's PSC.

5. In cases involving a specific project or a particular Classified Contract it may be possible, subject to the approval of the relevant CSAs, to establish recurring visitor lists. These lists shall be valid for an initial period not exceeding 12 months (from the date of authorisation) and may be extended for further periods subject to the prior approval of those CSAs. Such a list shall be submitted to the relevant CSA in accordance with paragraphs 3 and 4 of this Article. Once a recurring visitor list has been approved, visit arrangements may be made directly between the establishments or Contractors involved in respect of listed individuals.

6. The CSA of the requesting Party shall notify the CSA of the host Party of the details of visitors at least 20 working days prior to the planned visit. In urgent cases the requesting and host CSA may agree a shorter period.

7. All visitors shall be required to comply with the national laws and regulations of the host facility concerning the protection of Classified Information.

8. Any Classified Information which may be provided to visitors, or which may come to the notice of visitors, shall be treated by them as if such Classified Information has been provided in accordance with the provisions of this Agreement.

9. Visits involving access to Classified Information at the UK OFFICIAL-SENSITIVE or RESTREINT LUX levels shall be arranged directly between the sending facility and the facility to be visited.

Article 11

Classified Contracts

1. If a CSA of one Party proposes to place (or authorise a Contractor under its jurisdiction to place) a Classified Contract involving information at the UK TOP SECRET, TRES SECRET LUX, UK SECRET, SECRET LUX or CONFIDENTIEL LUX level with a Contractor under the jurisdiction of the other Party, it shall first obtain written confirmation of the relevant FSC from the CSA of that Party prior to entering into that Contract in accordance with Article 12.

2. A CSA which has granted a FSC shall be responsible for monitoring the security conduct of that Contractor in accordance with its national laws and regulations.

3. Contracts placed as a consequence of the pre-contract enquiries specified in paragraphs 1 and 2 of this Article shall contain a security requirements clause incorporating at least the following provisions:

a) The definition of the term Classified Information and the equivalent levels of security classification of the two Parties as set out in Article 4 of this Agreement;

b) The names of the CSA of each of the two Parties empowered to authorise the release and to co-ordinate the safeguarding of Classified Information related to the Contract;

c) The channels to be used for the transmission of the Classified Information in accordance with Article 7 of this Agreement;

d) The procedures for the translation, reproduction, and destruction of Classified Information in accordance with Article 9 of this Agreement;

e) The procedures and mechanisms for communicating changes that may arise in respect of Classified Information either because of changes in its security classification or because protection is no longer necessary;

f) The procedures for the approval of visits associated with Contract activity by personnel of one Party to Contractors of the other Party which are covered by the Contract in accordance with Article 10 of this Agreement; and

g) The requirement that the Contractor shall immediately notify its CSA of any actual or suspected Security Incident concerning Classified Information relating to the Classified Contract and take all reasonable steps to assist in mitigating the effects of such a Security Incident.

4. The CSA of the Originator shall pass a copy of the relevant parts of the Classified Contract to the relevant CSA of the Recipient to allow adequate security monitoring.

5. Each Contract shall contain a supplement/annex providing guidance on the security requirements and on the security classification of each aspect/element of the Contract. For the UK this guidance shall be contained in specific security clauses in the Contract and in a Security Aspects Letter (SAL). For Luxembourg this guidance shall be contained in a security annex to the Contract. The guidance must identify each classified aspect of the Contract, or any classified aspect which is to be generated by the Contractor, and allocate to it a specific security classification. Changes in the requirements or to the aspects/elements shall be notified to the other CSA as and when necessary. The Originator shall notify the Recipient when all or any of the information has been declassified.

6. Contracts involving UK OFFICIAL-SENSITIVE or RESTREINT LUX information shall include appropriate security clauses informing the Contractor of the minimum security requirements for the protection and handling of this information.

Article 12

Security Co-operation

1. When the requesting CSA requires confirmation of a Contractor's FSC they shall submit a formal written request to the CSA of the Contractor in the country of the Party where it is located providing at least the following information:

a) Full name of the Contractor;

b) Address of the Contractor; and

c) Full name, position, and contact details of the requesting CSA.

2. When the requesting CSA requires confirmation of an individual's PSC they shall submit an official request to the appropriate CSA providing at least the following information:

a) Full name of the individual;

b) Date and place of birth;

c) Nationality of the individual; and

d) Name and address of the organisation or Contractor which employs the individual.

3. The relevant CSA in each Party shall notify the requesting CSA of the FSC/PSC status of a Contractor or individual in response to such a request.

4. If the Contractor or individual does not have a FSC/PSC, or the clearance is at a lower security level than that which has been requested, the requesting CSA shall be notified. If the original request asked for it, the notification shall state whether action is being taken to grant or upgrade the FSC/PSC.

5. On request, the CSAs shall, in accordance with national laws and regulations, assist each other in carrying out FSC/PSC checks.

6. If information comes to the attention of the CSA providing a FSC/PSC assurance which raises doubt as to whether the relevant Contractor or individual should continue to hold their current clearance status, the requesting CSA shall be notified promptly. The CSA that provided the FSC/PSC assurance shall conduct a review and advise the requesting CSA whether any changes to the FSC/PSC previously issued are proposed.

7. If either CSA suspends or takes action to revoke access which has been granted to a Contractor or individual of the other Party, the other Party shall be notified in writing.

Article 13

Security Incidents

1. Any suspected Security Incident concerning the Classified Information of the other Party shall be investigated immediately by the Party of the country where the incident occurs.

2. If a Security Incident concerning the Classified Information of the other Party is confirmed the relevant CSA of the Party of the country where the incident occurred shall take appropriate measures according to its national laws and regulations to limit the consequences. Where appropriate, that CSA shall institute disciplinary and/or legal proceedings in accordance with its national laws and regulations.

3. If a Security Incident results in the actual or suspected unauthorised disclosure or loss of Classified Information of the other Party the relevant CSA of the Party where the incident occurred shall inform the other relevant CSA of the outcome of the investigation in writing as soon as possible and of any actions taken to prevent a recurrence.

Article 14

Costs

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

Article 15

Implementing Arrangements

The Parties may develop detailed procedures as necessary for the implementation of this Agreement. Such procedures shall be agreed between the Parties through mutual consultation.

Article 16

Resolution of Disputes

Any dispute or disagreement between the Parties on the interpretation or application of this Agreement, or any other dispute or disagreement arising out of this Agreement, shall be resolved by means of consultations between the Parties and shall not be referred to any national or international tribunal or other body for settlement. During these consultations both Parties shall continue to fulfil all of their obligations under this Agreement.

Article 17

Final Provisions

1. Each Party shall notify the other once the internal procedures necessary for entry into force of this Agreement have been completed. This Agreement shall enter into force on the first day of the second month following the receipt of the later notification.

2. This Agreement may be amended with the mutual written consent of the Parties. Either Party may propose amendments to this Agreement at any time. If one Party so proposes, the Parties shall begin consultations on the amendment of the Agreement. Agreed amendments shall enter into force under the conditions laid down in paragraph 1 of this Article.

3. This Agreement shall remain in force until further notice. A Party may terminate this Agreement by written notification delivered to the other Party through diplomatic channels, observing a period of notice of 6 months from the date of the notification. If this Agreement is terminated, any Classified Information already transmitted and any Classified Information generated and/or exchanged under this Agreement shall be handled by the Parties in accordance with the provisions of this Agreement for as long as the security classification level remains valid.

4. After the entry into force of this Agreement, the Party in whose territory the Agreement is concluded shall take immediate measures so as to have the Agreement registered by the Secretariat of the United Nations in accordance with Article 102 of the UN Charter. The other Party shall be notified of the registration and of the registration number in the UN Treaty Series as soon as the UN Secretariat has issued it.

In WITNESS WHEREOF the duly authorised representatives of the Parties have signed this Agreement,

In London on the 8th of September 2015 in two original copies, each one in the English language.

For the Government of the Grand Duchy of Luxembourg:	*For the Government of the United Kingdom of Great Britain and Northern Ireland:*
(signature)	(signature)

*

FICHE D'EVALUATION D'IMPACT

Coordonnées du projet

Intitulé du projet:	**Projet de loi 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** **– de 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**
Ministère initiateur:	**Ministère des Affaires étrangères**
Auteur(s):	**Robert Steinmetz**
Tél:	
Courriel:	**robert.steinmetz@mae.etat.lu**
Objectif(s) du projet:	**Approbation de l'Accord de sécurité négocié et signé avec le Royaume-Uni (8.9.2015) et la Chypre (5.9.2015)**
Autre(s) Ministère(s)/Organisme(s)/Commune(s)impliqué(e)(s):	
Ministère d'Etat – Autorité nationale de Sécurité	
Carlo Mreches, Anouk Schroeder	
Date:	**16.11.2015**

Mieux légiférer

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

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

3. Le principe „Think small first" est-il respecté? Oui ☐ Non ☐ N.a.[1] ☒
   (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:
   Pas de nécessité d'avoir un texte coordonné ou guide pratique

1 N.a.: non applicable.

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: non applicable

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

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

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[4]? Oui ☒ Non ☐ N.a. ☐

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

   Données échangées conformément à l'application de l'Accord de sécurité

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. ☒

    Si non, pourquoi?

11. Le projet contribue-t-il en général à une:
    a) simplification administrative, et/ou à une Oui ☒ Non ☐
    b) amélioration de la qualité réglementaire? Oui ☐ Non ☒

    Remarques/Observations:

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

---

2 Il s'agit d'obligations et de formalités administratives imposées aux entreprises et aux citoyens, liées à l'exécution, l'application ou la mise en 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.

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

4 Loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (www.cnpd.lu)

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 et du Commerce extérieur:
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 et du Commerce extérieur:
www.eco.public.lu/attributions/dg2/d_consommation/d_march_int_rieur/Services/index.html

*

FICHE FINANCIERE

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

---

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

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