

N° 6812

CHAMBRE DES DEPUTES

Session ordinaire 2014-2015

PROJET DE LOI

portant approbation des Accords de sécurité entre le Gouvernement du Grand-Duché de Luxembourg et certains pays concernant l'échange et la protection réciproque des informations classifiées (Accords de sécurité avec l'Autriche 13.11.2014 et la Croatie 13.03.2014)

* * *

*(Dépôt: le 5.5.2015)***SOMMAIRE:**

	<i>page</i>
1) Arrêté Grand-Ducal de dépôt (30.4.2015).....	1
2) Texte du projet de loi.....	2
3) Exposé des motifs.....	2
4) Abkommen zwischen der Regierung des Großherzogtums Luxemburg und der Österreichischen Bundesregierung über den Austausch und gegenseitigen Schutz klassifizierter Informationen.....	4
5) Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la République de Croatie concernant la protection d'informations classifiées.....	9
6) Fiche financière.....	15

*

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 est autorisé à déposer en Notre nom à la Chambre des Députés le projet de loi portant approbation des Accords de sécurité entre le Gouvernement du Grand-Duché de Luxembourg et certains pays concernant l'échange et la protection réciproque des informations classifiées (Accord de sécurité avec l'Autriche 13.11.2014 et la Croatie 13.03.2014).

Château de Berg, le 30 avril 2015

*Le Ministre des Affaires étrangères
et européennes,*

Jean ASSELBORN

HENRI

TEXTE DU PROJET DE LOI

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

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

*

EXPOSE DES MOTIFS

L'objet des accords conclus avec la République d'Autriche et la République de Croatie consiste à créer la toile de fond et le cadre juridique dans lequel s'inscrit l'échange d'informations et de matériels classifiés, notions que les auteurs de l'accord prennent soin de définir dans l'article introductif.

Ces accords s'inscrivent dans le cadre de toute une série de projets bilatéraux que le Gouvernement se propose de conclure et dont la trame est identique.

Ces accords se limitent à énoncer quelques principes de base qui ont traditionnellement cours en la matière ainsi que quelques règles d'ordre procédural doivent être mises en corrélation avec les législations nationales respectives des Etats parties relatives à la protection des informations classifiées au sens de l'accord auxquelles les accords renvoient 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 de conclure de tels accords bilatéraux 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.

Quant au régime de protection des documents classifiés, les Etats parties s'engagent à apporter aux informations leurs 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 vu 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 des accords.

Il en est de même des contrats classifiés définis comme étant tout contrat quels que soient son régime juridique ou sa dénomination dans lesquels 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.

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 déclasserement 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, ...).

ABKOMMEN
zwischen der Regierung des Großherzogtums
Luxemburg und der Österreichischen Bundes-
regierung über den Austausch und gegenseitigen
Schutz klassifizierter Informationen

Die Regierung des Großherzogtums Luxemburg und die Österreichische Bundesregierung (im Weiteren „die Parteien“ genannt)

In der Absicht, den Schutz aller klassifizierten Informationen zu gewährleisten, die gemäß dem innerstaatlichen Recht einer der Parteien als solche eingestuft und gekennzeichnet wurden und an die andere Partei übermittelt wurden,

Von dem Wunsch geleitet, Regeln zum gegenseitigen Schutz der übermittelten oder im Zuge der Zusammenarbeit zwischen den Parteien entstandenen klassifizierten Informationen vorzusehen,

sind wie folgt ÜBEREINGEKOMMEN:

Artikel 1

Begriffsbestimmungen

Im Sinne dieses Abkommens bedeutet:

- a) „Klassifizierte Informationen“ Informationen, unabhängig von ihrer Darstellungsform, die gemäß dem nationalen Recht einer der Parteien als klassifiziert eingestuft und gekennzeichnet wurden, um ihren Schutz vor unberechtigter Preisgabe, widerrechtlicher Verwendung oder Verlust zu gewährleisten;
- b) „Zuständige Behörde“ die in Artikel 13 genannten nationalen Behörden;
- c) „Sicherheitsunbedenklichkeitsbescheinigung für Personen“ die Feststellung durch eine zuständige Behörde, dass eine natürliche Person zum Zugang zu klassifizierten Informationen gemäß nationalem Recht berechtigt ist;
- d) „Sicherheitsunbedenklichkeitsbescheinigung für Unternehmen“ die Feststellung durch eine zuständige Behörde, dass eine juristische Person über die physische und organisatorische Fähigkeit verfügt, die Bedingungen für den Zugang zu und den Umgang mit klassifizierten Informationen gemäß dem nationalen Recht zu erfüllen;
- e) „Klassifizierter Vertrag“ ein Vertrag oder Untervertrag zwischen einer juristischen oder natürlichen Person einer Partei und einer juristischen oder natürlichen Person der anderen Partei, dessen Erfüllung den Zugang zu oder die Herstellung von klassifizierten Informationen erfordert;
- f) „Herausgeber“ die herausgebende Partei sowie jede der Hoheitsgewalt der betreffenden Partei unterstehende juristische oder natürliche Person, die klassifizierte Informationen herausgibt;
- g) „Empfänger“ die empfangende Partei sowie jede der Hoheitsgewalt der betreffenden Partei unterstehende juristische oder natürliche Person, die klassifizierte Informationen empfängt;
- h) „Dritter“ eine juristische oder natürliche Person, die nicht Herausgeber oder Empfänger der klassifizierten Information ist, die gemäß diesem Abkommen übermittelt wurde, oder eine Regierung, die nicht Partei dieses Abkommens ist, oder eine internationale Organisation;
- i) „Sicherheitsverletzung“ eine mutwillige oder zufällige Handlung oder Unterlassung, die gegen das nationale Recht und dieses Abkommen verstößt, deren Ergebnis zu tatsächlich oder mutmaßlich unberechtigter Preisgabe von klassifizierten Informationen führen kann, einschließlich aber nicht beschränkt auf Verlust, Zerstörung, Schädigung oder Missbrauch.

*Artikel 2****Gleichwertigkeit der Klassifizierungsstufen***

Die Parteien legen fest, dass folgende Klassifizierungsstufen gleichwertig sind:

<i>Großherzogtum Luxemburg:</i>	<i>Republik Österreich:</i>
TRES SECRET LUX	STRENG GEHEIM
SECRET LUX	GEHEIM
CONFIDENTIEL LUX	VERTRAULICH
RESTREINT LUX	EINGESCHRÄNKT

*Artikel 3****Kennzeichnung***

- (1) Zu übermittelnde klassifizierte Informationen werden vom Herausgeber in Übereinstimmung mit der entsprechenden Klassifizierungsstufe gekennzeichnet. Der Empfänger kennzeichnet erhaltene klassifizierte Informationen mit der Klassifizierungsstufe, die der Kennzeichnung des Herausgebers entspricht.
- (2) Die Kennzeichnungspflicht gilt auch für klassifizierte Informationen, die im Zuge der unter dieses Abkommen fallenden Zusammenarbeit erzeugt, vervielfältigt oder übersetzt werden.
- (3) Die Klassifizierungsstufe darf ausschließlich mit schriftlicher Zustimmung des Herausgebers geändert oder aufgehoben werden. Der Herausgeber informiert den Empfänger unverzüglich über jede Änderung oder Aufhebung der Klassifizierungsstufe der übermittelten klassifizierten Informationen.

*Artikel 4****Grundsätze des Schutzes klassifizierter Informationen***

- (1) Die Parteien treffen alle geeigneten Maßnahmen, um den Schutz der übermittelten klassifizierten Informationen gemäß dem nationalen Recht zu gewährleisten, und sorgen für die erforderliche Kontrolle dieses Schutzes.
- (2) Die Parteien gewähren den übermittelten klassifizierten Informationen mindestens den gleichen Schutzstandard, wie sie ihren eigenen klassifizierten Informationen der gleichwertigen Klassifizierungsstufe gewähren.
- (3) Übermittelte klassifizierte Informationen dürfen nur zu dem Zweck, für den sie herausgegeben wurden, verwendet werden.
- (4) Übermittelte klassifizierte Informationen werden nur natürlichen Personen zugänglich gemacht, die gemäß dem nationalen Recht zum Zugang zu klassifizierten Informationen der gleichwertigen Klassifizierungsstufe ermächtigt sind und die den Zugang für die Ausübung ihrer Aufgaben benötigen.
- (5) Eine Partei macht Dritten ohne vorherige schriftliche Zustimmung der zuständigen Behörde des Herausgebers klassifizierte Informationen nicht zugänglich.
- (6) Klassifizierte Informationen, die im Zuge der unter dieses Abkommen fallenden Zusammenarbeit erzeugt werden, genießen den gleichen Schutz wie übermittelte klassifizierte Informationen.

*Artikel 5****Sicherheitsunbedenklichkeitsbescheinigungen***

- (1) Im Rahmen dieses Abkommens anerkennt jede Partei die von der anderen Partei ausgestellten Sicherheitsunbedenklichkeitsbescheinigungen für Personen und Sicherheitsunbedenklichkeitsbescheinigungen für Unternehmen.
- (2) Die zuständigen Behörden unterstützen einander auf Ersuchen und gemäß dem jeweiligen nationalen Recht bei den für die Anwendung dieses Abkommens notwendigen Sicherheitsüberprüfungen.
- (3) Im Rahmen dieses Abkommens informieren die zuständigen Behörden einander unverzüglich über alle Änderungen von Sicherheitsunbedenklichkeitsbescheinigungen für Personen und Sicherheitsunbedenklichkeitsbescheinigungen für Unternehmen, insbesondere über einen Widerruf oder eine Änderung der Klassifizierungsstufe.
- (4) Auf Ersuchen der zuständigen Behörde des Herausgebers stellt die zuständige Behörde des Empfängers eine schriftliche Bestätigung aus, dass eine natürliche Person zum Zugang zu klassifizierten Informationen berechtigt ist.

*Artikel 6****Klassifizierte Verträge***

- (1) Ein klassifizierter Vertrag enthält Bestimmungen über die Sicherheitsanforderungen und Klassifizierungsstufe der herauszugebenden Information sowie Bestimmungen über die Verpflichtung, unverzüglich im Fall einer Sicherheitsverletzung die zuständige Behörde zu informieren. Eine Kopie der Bestimmungen wird an die zuständige Behörde der Partei weitergeleitet, unter deren Zuständigkeit der klassifizierte Vertrag durchzuführen ist.
- (2) Auf Ersuchen bestätigen die zuständigen Behörden, dass die vorgeschlagenen Auftragnehmer sowie natürliche Personen, die an vorvertraglichen Verhandlungen oder die bei der Durchführung von klassifizierten Verträgen teilnehmen, über Sicherheitsunbedenklichkeitsbescheinigungen für Personen und Sicherheitsunbedenklichkeitsbescheinigungen für Unternehmen verfügen oder dass die entsprechenden Verfahren eingeleitet wurden, sowie über die Sicherheitsanforderungen für die betroffenen klassifizierten Informationen.
- (3) Die zuständigen Behörden informieren einander über klassifizierte Verträge, die unter dieses Abkommen fallen.
- (4) Der Herausgeber übermittelt dem Empfänger und der zuständigen Behörde des Empfängers eine Liste der klassifizierten Informationen, die gemäß dem klassifizierten Vertrag zu übermitteln sind.
- (5) Ein Auftragnehmer kann einen Subunternehmer heranziehen, um einen Teil des klassifizierten Vertrags zu erfüllen. Subunternehmer unterliegen den gleichen Sicherheitserfordernissen wie der Auftragnehmer.

*Artikel 7****Übermittlung***

- (1) Klassifizierte Informationen werden auf diplomatischem Weg oder auf jedem anderen zwischen den Vertragsparteien vereinbarten Weg übermittelt. Der Empfang von als CONFIDENTIEL LUX/VERTRAULICH oder höher gekennzeichneten klassifizierten Informationen ist schriftlich zu bestätigen. Als TRES SECRET LUX/STRENG GEHEIM gekennzeichnete klassifizierte Informationen werden ausschließlich auf diplomatischem Weg oder mittels eines befugten persönlichen Kuriers übermittelt.
- (2) Erfolgt die Übermittlung auf elektronischem Weg, dürfen nur Verschlüsselungssysteme eingesetzt werden, die von den Parteien vereinbart wurden.

*Artikel 8****Vervielfältigung und Übersetzung***

- (1) Die Vervielfältigung und Übersetzung klassifizierter Informationen kann vom Herausgeber eingeschränkt oder ausgeschlossen werden.
- (2) Als TRES SECRET LUX/STRENG GEHEIM gekennzeichnete klassifizierte Informationen dürfen weder vervielfältigt noch übersetzt werden. Zusätzliche Originale können beim Herausgeber schriftlich beantragt werden.
- (3) Als SECRET LUX/GEHEIM gekennzeichnete klassifizierte Informationen dürfen nur mit schriftlicher Zustimmung des Herausgebers vervielfältigt oder übersetzt werden.
- (4) Klassifizierte Informationen werden nur von Personen übersetzt, die zum Zugang zu klassifizierten Informationen der jeweiligen Klassifizierungsstufe berechtigt sind.
- (5) Kopien und Übersetzungen sind wie Originale zu schützen.

*Artikel 9****Vernichtung***

- (1) Klassifizierte Informationen werden auf eine Weise vernichtet, die eine vollständige oder teilweise Wiederherstellung nicht zulässt. Die Vernichtung klassifizierter Informationen ab der Stufe CONFIDENTIEL LUX/VERTRAULICH hat nachweislich zu erfolgen.
- (2) Als TRES SECRET LUX/STRENG GEHEIM gekennzeichnete klassifizierte Informationen werden nicht vernichtet, sondern an den Herausgeber rückübermittelt.
- (3) Als SECRET LUX/GEHEIM gekennzeichnete klassifizierte Informationen dürfen, sofern nicht ein Fall des Absatz 4 vorliegt, nur mit schriftlicher Zustimmung des Herausgebers vernichtet werden.
- (4) Im Falle einer Krisensituation, in der es unmöglich ist, klassifizierte Informationen, die in Anwendung dieses Abkommens übermittelt oder erzeugt wurden, zu schützen oder rückzuübermitteln, werden die klassifizierten Informationen umgehend vernichtet. Der Empfänger informiert die zuständige Behörde des Herausgebers sobald wie möglich über diese Vernichtung.

*Artikel 10****Besuche***

- (1) Besuche, die den Zugang zu klassifizierten Informationen erfordern, unterliegen der vorherigen Genehmigung durch die zuständige Behörde der gastgebenden Partei. Die Genehmigung wird nur natürlichen Personen erteilt, die gemäß dem nationalen Recht zum Zugang zu klassifizierten Informationen der entsprechenden Klassifizierungsstufe ermächtigt sind.
- (2) Besuchsanträge werden mindestens zwanzig Arbeitstage vor dem Besuch bei der zuständigen Behörde der gastgebenden Partei gestellt, in dringenden Fällen innerhalb eines kürzeren Zeitraums. Die zuständigen Behörden informieren einander über die Einzelheiten des Besuchs und gewährleisten den Schutz personenbezogener Daten.
- (3) Besuchsanträge werden in deutscher oder englischer Sprache gestellt und enthalten insbesondere folgende Angaben:
 - a) Zweck, vorgesehene Datum und Dauer des Besuchs;
 - b) Vor- und Familienname, Geburtsdatum und -ort, Staatsangehörigkeit und Pass oder Personalausweisnummer des Besuchers;

- c) Funktion des Besuchers und Name der vertretenen Behörde oder Stelle oder des vertretenen Unternehmens;
 - d) Gültigkeit und Klassifizierungsstufe der Sicherheitsunbedenklichkeitsbescheinigung für Personen des Besuchers;
 - e) Name, Adresse, Telefon- und Faxnummer, E-Mail-Adresse und Ansprechpartner der Behörden, Stellen oder Einrichtungen, die besucht werden sollen;
 - f) Datum des Antrags und Unterschrift der zuständigen Behörde.
- (4) Die zuständigen Behörden der Parteien können Listen von Personen erstellen, die zu wiederholten Besuchen ermächtigt sind. Diese Listen sind für einen Zeitraum von höchstens 12 Monaten gültig. Die Details der jeweiligen Besuche werden direkt mit den Ansprechpartnern in den Behörden, Stellen oder Einrichtungen, die von diesen Personen besucht werden sollen, festgelegt.

Artikel 11

Sicherheitsverletzungen

- (1) Im Falle einer Sicherheitsverletzung informiert die zuständige Behörde des Empfängers unverzüglich die zuständige Behörde des Herausgebers schriftlich.
- (2) Verletzungen der Bestimmungen über den Schutz von unter dieses Abkommen fallenden klassifizierten Informationen werden gemäß dem nationalen Recht untersucht und verfolgt. Die Parteien unterstützen einander auf Ersuchen.
- (3) Die Parteien informieren einander über das Ergebnis der Untersuchungen und über die getroffenen Maßnahmen.

Artikel 12

Kosten

Jede Partei trägt die Kosten, die ihr im Zuge der Durchführung dieses Abkommens entstehen.

Artikel 13

Zuständige Behörden

- (1) Die zuständigen Behörden sind:
Für das Großherzogtum Luxemburg:
Service de Renseignement/Autorité Nationale de Sécurité
Für die Republik Österreich:
1. Informationssicherheitskommission
2. Bundesministerium für Landesverteidigung und Sport/Abwehramt
- (2) Die Parteien teilen einander die Kontaktdaten der zuständigen Behörden schriftlich mit.

Artikel 14

Konsultationen

- (1) Die zuständigen Behörden informieren einander über das jeweilige nationale Recht über den Schutz klassifizierter Informationen und alle wesentlichen Änderungen.
- (2) Um eine enge Zusammenarbeit bei der Durchführung dieses Abkommens zu gewährleisten, konsultieren die zuständigen Behörden einander und erleichtern die notwendigen gegenseitigen Besuche.

*Artikel 15****Streitbeilegung***

Streitigkeiten über die Anwendung oder Auslegung dieses Abkommens werden im Wege direkter Gespräche zwischen den Parteien oder auf diplomatischem Wege beigelegt.

*Artikel 16****Schlussbestimmungen***

- (1) Dieses Abkommen wird auf unbestimmte Zeit geschlossen und tritt am ersten Tag des zweiten Monats nach dem Tag in Kraft, an dem die Parteien einander auf diplomatischem Wege den Abschluss der für das Inkrafttreten des Abkommens erforderlichen innerstaatlichen Verfahren mitgeteilt haben.
- (2) Dieses Abkommen kann im gegenseitigen schriftlichen Einvernehmen beider Parteien geändert werden. Änderungen treten gemäß Absatz 1 in Kraft.
- (3) Jede Partei kann dieses Abkommen jederzeit auf diplomatischem Wege kündigen. In einem solchen Fall tritt das Abkommen sechs Monate nach Erhalt der Kündigungsnote durch die andere Partei außer Kraft. Im Fall der Kündigung bleiben klassifizierte Informationen, die in Anwendung dieses Abkommens übermittelt oder hergestellt wurden, weiterhin nach den Bestimmungen dieses Abkommens geschützt.

GESCHEHEN zu Wien, am 13.11.2014 in zwei Urschriften in deutscher Sprache.

*Für die Regierung des
Großherzogtums Luxemburg,*
(Unterschrift)

*Für die Österreichische
Bundesregierung,*
(Unterschrift)

*

ACCORD

**entre le Gouvernement du Grand-Duché de Luxembourg
et le Gouvernement de la République de Croatie concer-
nant la protection d'informations classifiées**

Le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la République de Croatie (ci-après dénommés les „Parties“),

Conscients qu'une coopération efficace dans les domaines politique, économique, militaire, de la sécurité ainsi que dans tout autre domaine pourrait nécessiter un échange d'informations classifiées entre les Parties,

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

CONVIENNENT ce qui suit:

*Article 1****Objet et champ d'application***

1. Le présent Accord a pour but de garantir la protection des informations classifiées généralement produites ou échangées entre les Parties.
2. Le présent Accord s'applique, à compter de son entrée en vigueur, à toute activité ou à tout contrat ou accord impliquant des informations classifiées, mené ou conclu entre les Parties.

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

Article 2

Définitions

Aux fins du présent Accord:

- (1) „*Information classifiée*“ désigne toute information, quelle qu'en soit la forme, transmise ou produite entre les Parties conformément aux lois et réglementations nationales de chacune des Parties, nécessitant une protection contre toute divulgation non autorisée, détournement ou perte, désignée et marquée en conséquence;
- (2) „*Besoin d'en connaître*“ fait référence à la nécessité d'accéder à des informations classifiées dans le cadre de fonctions officielles et/ou déterminées en vue de l'accomplissement d'une mission spécifique;
- (3) „*Infraction à la sécurité*“ désigne tout acte ou omission contraire aux lois et réglementations nationales, susceptible d'entraîner la divulgation, la perte, la destruction ou le détournement d'informations classifiées ou tout autre acte ou omission susceptible d'entraîner la perte de leur confidentialité, intégrité ou disponibilité;
- (4) „*Partie d'origine*“ désigne la Partie, y compris n'importe quelle entité, qui transmet des informations classifiées conformément aux lois et réglementations nationales;
- (5) „*Partie destinataire*“ désigne la Partie, y compris toute entité, qui reçoit des informations classifiées de la Partie d'origine;
- (6) „*Autorité nationale de sécurité*“ désigne l'autorité nationale qui, conformément aux lois et réglementations nationales, est chargée de contrôler l'application du présent Accord et la protection des informations classifiées produites ou échangées en vertu du présent Accord;
- (7) „*Contractant*“ désigne toute personne physique ou morale dotée de la capacité juridique de conclure des contrats classifiés;
- (8) „*Sous-traitant*“ désigne tout contractant avec lequel le premier contractant conclut un contrat de sous-traitance;
- (9) „*Contrat classifié*“ désigne tout accord entre deux ou plusieurs contractants ou sous-contractants qui contient des informations classifiées ou dont l'exécution implique la production ou l'échange d'informations classifiées;
- (10) „*Habilitation de sécurité individuelle*“ désigne toute décision de l'autorité nationale de sécurité selon laquelle le ressortissant est autorisé à accéder à des informations classifiées conformément aux lois et réglementations nationales jusqu'à un certain niveau de classification de sécurité;
- (11) „*Habilitation de sécurité d'établissement*“ désigne toute décision de l'autorité nationale de sécurité selon laquelle le contractant ou le sous-traitant remplit les conditions requises pour traiter des informations classifiées conformément aux lois et réglementations nationales jusqu'à un certain niveau de classification de sécurité;
- (12) „*Tierce partie*“ désigne tout Etat ou organisation internationale qui n'est pas l'une des Parties au présent Accord.

Article 3

Niveaux de sécurité

1. Les Parties reconnaissent que les niveaux de sécurité suivants sont équivalents conformément aux lois et réglementations nationales:

<i>Pour le Grand-Duché de Luxembourg</i>	<i>Pour la République de Croatie</i>
TRES SECRET LUX	VRLO TAJNO
SECRET LUX	TAJNO
CONFIDENTIEL LUX	POVJERLJIVO
RESTREINT LUX	OGRANIČENO

2. La Partie d'origine peut utiliser un marquage additionnel précisant des limites spécifiques applicables à l'utilisation d'informations classifiées. Les autorités nationales de sécurité se tiennent mutuellement informées d'un tel marquage additionnel.

Article 4

Autorités nationales de sécurité

1. Les autorités nationales de sécurité des Parties sont:

Pour le Grand-Duché de Luxembourg:

- Service de renseignement de l'Etat
Autorité nationale de Sécurité;

Pour la République de Croatie:

- Ured Vijeća za nacionalnu sigurnost.

2. Les Parties se tiennent mutuellement informées, par la voie diplomatique, des modifications apportées aux autorités nationales de sécurité. Cette notification ne constitue pas une modification formelle du présent Accord, conformément à l'article 14, paragraphe 2.

3. Les autorités nationales de sécurité se tiennent mutuellement informées de leurs lois et réglementations nationales ainsi que de toute modification apportée à celles-ci et susceptible d'avoir une incidence sur la protection des informations classifiées produites et échangées en vertu du présent Accord.

4. En vue d'appliquer et de conserver des normes de sécurité similaires, les autorités nationales de sécurité peuvent se tenir mutuellement informées des normes, procédures et pratiques de sécurité qu'elles appliquent respectivement en matière de protection d'informations classifiées.

Article 5

Mesures de protection d'informations classifiées

1. Conformément aux 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 apportent auxdites informations classifiées un niveau de protection équivalent à celui qui est accordé à leurs informations classifiées nationales de même niveau de sécurité, conformément à l'article 3 du présent Accord.

2. La Partie d'origine informe par écrit la partie destinataire de toute modification apportée au niveau de sécurité des informations classifiées transmises afin de prendre les mesures de protection appropriées.

3. L'accès à des informations classifiées est réservé aux personnes ayant le besoin d'en connaître qui, conformément aux lois et réglementations nationales, sont autorisées à accéder aux informations classifiées d'un niveau de sécurité équivalent, et qui ont été informées en la matière.

4. Dans le cadre du présent Accord, chacune des Parties reconnaît les habilitations de sécurité individuelle et d'établissement délivrées par l'autre Partie.

5. Sur demande et conformément aux lois et réglementations nationales, les autorités nationales de sécurité se prêtent mutuellement assistance dans le cadre de la mise en oeuvre des procédures d'habilitation.
6. Dans le cadre du présent Accord, les autorités nationales de sécurité se tiennent mutuellement informées sans délai de la révocation de toute habilitation de sécurité individuelle ou d'établissement, ou de la modification du niveau de classification de sécurité.
7. A la demande de l'autorité nationale de sécurité de la Partie d'origine, l'autorité nationale de sécurité de la Partie destinataire délivre une confirmation écrite selon laquelle une habilitation de sécurité individuelle a été délivrée à un particulier ou selon laquelle une habilitation de sécurité d'établissement a été délivrée à une personne morale.
8. La Partie destinataire:
 - a) ne divulgue aucune information classifiée à une Tierce partie sans l'accord écrit préalable de la Partie d'origine, délivré conformément aux lois et réglementations nationales;
 - b) si elle le juge opportun, classifie les informations reçues sur la base des équivalences définies à l'article 3;
 - c) ne déclassifie ou ne déclasse pas les informations classifiées transmises sans l'accord écrit préalable de la Partie d'origine;
 - d) n'utilise des informations classifiées qu'aux fins prévues.

Article 6

Transmission d'informations classifiées

1. Les informations classifiées sont transmises par les services du courrier diplomatique ou militaire ou par d'autres moyens préalablement approuvés par les autorités nationales de sécurité, conformément aux lois et réglementations nationales.
2. La transmission électronique d'informations classifiées est effectuée par le biais de méthodes cryptographiques certifiées conformément aux lois et réglementations nationales.
3. En cas de transmission d'informations classifiées TAJNO/SECRET LUX ou de niveau supérieur, la Partie destinataire en confirme la réception par écrit. La réception d'autres informations est confirmée sur demande.
4. Les services de sécurité et de renseignement des Parties peuvent échanger directement des informations classifiées conformément aux lois et réglementations nationales.

Article 7

Reproduction et traduction d'informations classifiées

1. La traduction ou la reproduction des informations classifiées TAJNO/SECRET LUX ou de niveau supérieur sont autorisées uniquement dans des circonstances exceptionnelles avec l'accord écrit préalable de la Partie d'origine.
2. Toutes les reproductions et traductions d'informations classifiées portent les marques de classification de sécurité originales. Ces reproductions ou traductions sont protégées de la même manière que les informations originales. Le nombre de reproductions ou de traductions est limité au nombre requis pour un usage officiel.

*Article 8****Destruction d'informations classifiées***

1. Les informations classifiées VRLO TAJNO/TRES SECRET LUX ne sont pas détruites, sauf dans les cas visés au paragraphe 4 du présent article. Celles-ci sont renvoyées à la Partie d'origine dès lors que les Parties les jugent inutiles.
2. Les informations classifiées TAJNO/SECRET LUX ou d'un niveau inférieur sont détruites dès lors que la Partie destinataire les reconnaît inutiles, de manière à empêcher leur restauration totale ou partielle.
3. La Partie destinataire informe dès que possible la Partie d'origine de la destruction des informations classifiées TAJNO/SECRET LUX.
4. Dans le cas d'une situation de crise rendant impossible la protection ou le retour 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***

1. Tout contrat classifié est conclu et mis en oeuvre conformément aux lois et réglementations nationales.
2. Sur demande, l'autorité nationale de sécurité de la Partie destinataire confirme qu'une habilitation de sécurité individuelle ou d'établissement appropriée a été délivrée à un contractant proposé. Si le contractant proposé ne détient aucune habilitation de sécurité appropriée, l'autorité nationale de sécurité de la Partie d'origine peut demander à l'autorité nationale de sécurité de la Partie destinataire de délivrer l'habilitation de sécurité appropriée.
3. L'autorité nationale de sécurité sur le territoire de laquelle les contrats classifiés doivent être exécutés assume la responsabilité de l'établissement et de la gestion des mesures de sécurité relatives aux contrats classifiés selon les mêmes normes et conditions que celles qui régissent la protection de ses propres contrats classifiés. Les autorités nationales de sécurité peuvent procéder à des inspections de sécurité périodiques.
4. Tout Contrat ou Contrat de sous-traitance classifié doit contenir une annexe de sécurité dans laquelle la Partie d'origine précise les informations classifiées qui doivent être transmises à la Partie destinataire, le niveau de classification de sécurité à attribuer à ces informations et les obligations du contractant en matière de protection des informations classifiées. Une copie de l'annexe de sécurité est envoyée à l'autorité nationale de sécurité de la Partie d'origine.
5. Avant de transmettre aux contractants ou aux contractants éventuels de l'une des Parties toute information classifiée transmise par l'autre Partie, la Partie destinataire doit, conformément aux lois et réglementations nationales, s'assurer que les Contractants ou futurs Contractants sont en mesure de garantir une protection adéquate de la sécurité des informations classifiées, et:
 - a) exécuter une procédure d'habilitation de sécurité d'établissement appropriée à l'égard des contractants et des sous-traitants;
 - b) exécuter 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'assurer que toutes les personnes ayant accès à des informations classifiées sont tenues informées de leurs responsabilités;
 - d) réaliser des inspections de sécurité périodiques au sein des établissements pertinents ayant obtenu une habilitation.

6. Les sous-traitants engagés dans des contrats classifiés doivent satisfaire aux exigences de sécurité applicables aux contractants.

7. Les représentants des autorités nationales de sécurité peuvent effectuer des visites réciproques 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

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.

2. Toute demande de visite est présentée au moins 3 semaines avant la visite et contient les informations suivantes:

- a) nom et prénom, date et lieu de naissance, nationalité du visiteur;
- b) numéro du passeport ou de tout autre document d'identité du visiteur;
- c) qualité du visiteur et nom de l'organisation qu'il représente;
- d) niveau de l'habilitation de sécurité individuelle du visiteur, le cas échéant;
- e) objet de la visite, programme de travail proposé et date de la visite prévue;
- f) nom des organisations et des établissements à visiter;
- g) nombre de visites et période demandée;
- h) autres renseignements, tels que convenus par les autorités nationales de sécurité.

3. Chacune des Parties garantit la protection des données personnelles des visiteurs conformément aux lois et réglementations nationales.

Article 11

Infraction à la sécurité

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

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. Sur demande, l'autorité nationale de sécurité de la Partie destinataire communique à l'autorité nationale de sécurité de la Partie d'origine le résultat de la procédure 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 résolu par voie de consultation et de négociation entre les Parties.

*Article 14****Dispositions finales***

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.
2. Le présent Accord peut être modifié d'un commun accord par écrit entre les Parties. Les modifications font partie intégrante du présent Accord et prennent effet selon les modalités prévues au paragraphe 1 du présent article.
3. Le présent Accord est conclu pour une durée indéterminée. Chacune des Parties peut dénoncer le présent Accord moyennant l'envoi d'un préavis écrit à l'autre Partie par la voie diplomatique. Dans ce cas, le présent Accord prendra fin six mois à compter de la date de réception de la dénonciation par l'autre Partie.
4. En cas de dénonciation du présent Accord, toutes les informations classifiées échangées en vertu de ce dernier continuent d'être protégées conformément aux présentes dispositions et sont, sur demande, renvoyées à la Partie d'origine.
5. 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 l'Accord 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, tel qu'indiqué sur le certificat d'enregistrement délivré par le Secrétariat des Nations Unies.

FAIT à Luxembourg, le 13 mars 2014, en double exemplaire, chacun en langues française, croate 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 Croatie,*
(signature)

*

FICHE FINANCIERE

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

