LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère des Affaires étrangères
et européennes, de la Défense, de la
Coopération et du Commerce extérieur

Exposé des motifs

Le projet de loi vise à approuver l'accord signé le 21 avril 2026 entre le Grand-Duché de Luxembourg et le Royaume des Pays-Bas relatif à l'échange et la protection mutuelle des informations classifiées (ci-après « **l'Accord** »).

I. Genèse de l'Accord

Le Gouvernement du Grand-Duché de Luxembourg s'efforce de conclure de manière continue des accords relatifs à la protection réciproque et à l'échange d'informations classifiées avec tous les États membres de l'Union européenne et de l'Organisation du Traité de l'Atlantique Nord, ainsi qu'avec d'autres pays avec lesquels le Luxembourg doit être en mesure d'échanger des informations classifiées. La conclusion de tels accords s'inscrit dans le cadre d'une politique de sécurité globale que le Gouvernement a continuellement renforcée au cours des vingt dernières années, compte tenu notamment de la dégradation progressive du contexte sécuritaire international et des menaces croissantes auxquelles le Grand-Duché de Luxembourg doit faire face, telles que le terrorisme, la criminalité organisée, l'espionnage, la prolifération des armes de destruction massive et les cyber-attaques. Dans ce contexte, la prévention et la coopération internationale constituent des éléments fondamentaux pour réduire les risques liés aux menaces. Elles permettent également de renforcer les capacités de défense et d'assurer la résilience du Grand-Duché de Luxembourg face aux diverses menaces, y compris les menaces hybrides et les risques pesant sur le patrimoine économique et financier de l'Etat.

Le Luxembourg a conclu à ce jour 32 accords bilatéraux relatifs à la protection réciproque et à l'échange d'informations classifiées, auxquels s'ajoutent quatre accords conclus au niveau multilatéral (à savoir par l'Union européenne, l'Agence Spatiale Européenne, l'Organisation du Traité de l'Atlantique Nord et l'Organisation Conjointe de Coopération en matière d'Armement).

II. Nature de l'Accord

Il s'agit d'un accord bilatéral qui instaure le cadre juridique relatif à la protection réciproque et à l'échange d'informations classifiées entre le Grand-Duché de Luxembourg et le Royaume des Pays-Bas.

III. Contenu de l'Accord

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

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

Pour ce qui est du régime de protection des informations classifiées, chaque Partie s'engage, en vertu de l'Accord, à accorder aux informations qui lui sont transmises par l'autre Partie le même degré de protection que celui accordé à ses propres informations classifiées de niveau équivalent. Les Parties réservent l'accès aux informations classifiées aux seules personnes qui ont le besoin d'en connaître, qui ont été informées des règles de sécurité applicables au traitement et à la protection des informations classifiées et qui sont dûment autorisées à y accéder en vertu de leurs fonctions ou d'une habilitation de sécurité du niveau approprié, conformément aux lois et règlementations respectives des Parties. Les Parties reconnaissent mutuellement les habilitations de sécurité délivrées par elles. Il s'y ajoute que les Parties n'ont le droit d'utiliser les informations classifiées qu'aux fins pour lesquelles elles ont été communiquées et dans les limites fixées par la Partie d'origine. La Partie destinataire ne communique les informations classifiées à un tiers sans l'accord écrit préalable de la Partie d'origine. Sont également fixées les conditions qui régissent les visites des installations au sein desquelles sont stockées les informations classifiées. Enfin, l'Accord contient également des dispositions relatives aux contrats classifiés régissant notamment les vérifications à effectuer par les autorités compétentes en matière de sécurité et les exigences de sécurité à inclure dans tout contrat classifié. Les autorités compétentes en matière de sécurité s'engagent ainsi à s'informer mutuellement, sur demande, si un contractant a obtenu une habilitation de sécurité d'établissement pour le niveau de classification de sécurité requis par le contrat classifié. Avant toute proposition d'un contrat classifié impliquant l'accès à des informations classifiées par une Partie ou un contractant, une confirmation écrite est également nécessaire établissant que le contractant a obtenu une habilitation de sécurité d'établissement pour le niveau de classification de sécurité approprié.

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

1) Loi du 15 juin 2004 portant approbation de l'Accord sur la Sécurité des Informations entre les Parties au **Traité de l'Atlantique Nord** avec ses annexes 1, 2, et 3 signé par le Luxembourg le 14 juillet 1998.

2) Loi du 14 juin 2005 portant approbation
   - de la Convention portant création d'une Agence spatiale européenne, faite à Paris, le 30 mai 1975

- de l'Accord entre les Etats parties à la Convention portant création d'une **Agence spatiale européenne** et l'Agence spatiale européenne concernant la protection et l'échange d'informations classifiées, fait à Paris, le 19 août 2002
- de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et l'Agence spatiale européenne relatif à l'adhésion du Grand-Duché de Luxembourg à la Convention portant création de l'Agence spatiale européenne et des clauses et conditions s'y rapportant, fait à Paris, le 6 mai 2004.

3) Loi du 16 décembre 2008 portant approbation de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la **République fédérale d'Allemagne** concernant la protection réciproque des informations classifiées, signé à Berlin le 17 janvier 2006.

4) Loi du 16 décembre 2008 portant approbation de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la **République française** concernant l'échange et la protection réciproque des informations classifiées, signé à Luxembourg, le 24 février 2006.

5) Loi du 16 décembre 2008 portant approbation de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la **République de Lettonie** concernant l'échange et la protection réciproque des informations classifiées, signé à Luxembourg, le 13 septembre 2007.

6) Loi du 13 mars 2009 portant approbation de l'Accord entre le Grand-Duché de Luxembourg et la **République portugaise** concernant l'échange et la protection réciproque des informations classifiées, signé à Luxembourg, le 22 février 2008.

7) Loi du 24 juillet 2011 portant approbation de l'Accord entre le Grand-Duché de Luxembourg et le **Royaume d'Espagne** concernant l'échange et la protection réciproque des informations classifiées, signé à Luxembourg, le 12 novembre 2009.

8) Loi du 8 mai 2013 portant approbation des Accords entre le Gouvernement du Grand-Duché de Luxembourg et certains pays concernant l'échange et la protection réciproque des informations classifiées.
   - 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.
   - 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.
   - 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.
   - 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.
   - Accord de sécurité entre le Grand-Duché de Luxembourg et le **Royaume de Belgique**, signé à Luxembourg, le 9 février 2012.
   - 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.
   - Accord de sécurité entre le Grand-Duché de Luxembourg et la **République d'Estonie**, signé à Bruxelles, le 23 juillet 2012.

- Accord de sécurité entre le Gouvernement du Grand-Duché de Luxembourg et le **Gouvernement de Géorgie**, signé à Luxembourg, le 15 octobre 2012.

9) Loi du 18 juillet 2014 portant approbation de l'Accord de sécurité entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement du **Royaume de Norvège** concernant l'échange et la protection réciproque d'informations classifiées, signé à Bruxelles, le 21 février 2013.

10) Loi du 18 juillet 2014 portant approbation de l'Accord entre les **Etats membres de l'Union européenne**, réunis au sein du Conseil, relatif à la protection des informations classifiées échangées dans l'intérêt de l'Union européenne, signé à Bruxelles, le 25 mai 2011.

11) Loi du 27 novembre 2015 portant approbation
    - de l'Accord de sécurité entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la **République d'Autriche** concernant l'échange et la protection réciproque des informations classifiées, signé à Vienne, le 13 novembre 2014
    - de l'Accord de sécurité entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la **République de Croatie** concernant l'échange et la protection réciproque des informations classifiées, signé à Luxembourg, le 13 mars 2014.

12) Loi du 3 décembre 2015 portant approbation de l'Accord de sécurité entre le Gouvernement du Grand-Duché de Luxembourg et l'**Organisation Conjointe de Coopération en matière d'Armement (OCCAR)** sur la protection des informations classifiées, fait à Luxembourg, le 6 janvier 2015.

13) Loi du 29 mars 2016 portant approbation de l'Accord de sécurité entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la **République de Pologne** concernant la protection réciproque d'informations classifiées, signé à Varsovie, le 12 mai 2015.

14) Loi du 31 août 2016 portant approbation de
    - l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le **Gouvernement du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord** concernant la protection réciproque d'informations classifiées, signé à Londres, le 8 septembre 2015
    - l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la **République de Chypre** concernant l'échange et la protection réciproque d'informations classifiées, signé à Luxembourg, le 3 septembre 2015.

15) Loi du 6 juin 2018 portant approbation de
    - l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la **République italienne** concernant l'échange et la protection réciproque d'informations classifiées, fait à Rome le 20 avril 2017 ;
    - l'Accord de sécurité entre le Gouvernement du Grand-Duché de Luxembourg et le **Gouvernement de Roumanie** sur la protection réciproque des informations classifiées, signé à Bucarest, le 24 mai 2017.

16) Loi du 26 octobre 2019 portant approbation
    1. de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la **République de Bulgarie** relatif à l'échange et à la protection réciproque d'informations classifiées, fait à Sofia, le 29 janvier 2018 ;
    2. de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Conseil des Ministres de la **République d'Albanie** relatif à la protection réciproque d'informations classifiées, fait à Luxembourg, le 25 juin 2018 ;
    3. de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le **Gouvernement de Hongrie** relatif à l'échange et à la protection réciproque d'informations classifiées, fait à Budapest, le 5 septembre 2018 ;
    4. de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la **République de Macédoine** relatif à l'échange et à la protection réciproque d'informations classifiées, fait à Skopje, le 6 septembre 2018 ;
    5. de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la **République fédérative du Brésil** concernant l'échange et la protection réciproque d'informations classifiées, fait à New York, le 25 septembre 2018.

17) Loi du 30 novembre 2020 portant approbation de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la **République de Malte** relatif à la protection réciproque et à l'échange d'informations classifiées, fait à New York, le 26 septembre 2019.

18) Loi du 30 novembre 2020 portant approbation de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la **République de Serbie** concernant l'échange et la protection réciproque d'informations classifiées, fait à Luxembourg, le 4 février 2020.

19) Loi du 28 février 2024 portant approbation de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la **République de Lituanie** concernant l'échange et la protection réciproque d'informations classifiées, fait à Bruxelles, le 7 décembre 2020.

20) Loi du 28 février 2024 portant approbation de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la **République française** concernant l'échange et la protection des informations classifiées, fait à Paris, le 1er juillet 2022[1].

21) Loi du 4 juillet 2025 portant approbation de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le **Conseil Fédéral Suisse** relatif à la protection réciproque et à l'échange d'informations classifiées, fait à Luxembourg, le 13 mai 2024.

22) Loi du 28 août 2025 portant approbation de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la **République hellénique** sur l'échange et la protection mutuelle des informations classifiées, fait à Athènes, le 24 octobre 2024.

[1] Et abrogeant l'accord cité sous 4).

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère des Affaires étrangères
et européennes, de la Défense, de la
Coopération et du Commerce extérieur

Texte du projet de loi

Projet de loi portant approbation de l'Accord entre le Grand-Duché de Luxembourg et le Royaume des Pays-Bas relatif à l'échange et la protection mutuelle des informations classifiées, fait à Luxembourg, le 21 avril 2026.

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

Le Conseil d'État entendu ;
Vu l'adoption par la Chambre des Députés ;
Vu la décision de la Chambre des Députés du [jj.mm.aaa] et celle du Conseil d'État du [jj.mm.aaaa] portant qu'il n'y a pas lieu à second vote ;

Avons ordonné et ordonnons :

Article unique.

Est approuvé l'Accord entre le Grand-Duché de Luxembourg et le Royaume des Pays-Bas relatif à l'échange et la protection mutuelle des informations classifiées, fait à Luxembourg, le 21 avril 2026.

Mandons et ordonnons que la présente loi soit insérée au Journal officiel du Grand-Duché de Luxembourg pour être exécutée et observée par tous ceux que la chose concerne.

ACCORD

ENTRE

LE GRAND-DUCHÉ DE LUXEMBOURG

ET

LE ROYAUME DES PAYS-BAS

RELATIF À L'ÉCHANGE ET LA PROTECTION MUTUELLE DES INFORMATIONS CLASSIFIÉES

Le Grand-Duché de Luxembourg

et

le Royaume des Pays-Bas,

Ci-après dénommés conjointement les « Parties » et individuellement une « Partie »,

Désirant mettre en place un système régissant la protection des Informations classifiées produites ou échangées dans le cadre de la coopération entre les Parties ou entre des entités publiques et privées relevant de leur juridiction,

Souhaitant assurer la protection mutuelle des Informations classifiées, ont convenu, dans l'intérêt de la sécurité nationale, de ce qui suit :

Article 1er
Objet et champ d'application

1. Le présent Accord a pour objet d'assurer la protection des Informations classifiées échangées entre les Parties, entre une Partie et un Contractant relevant de la juridiction de l'autre Partie ou entre des Contractants relevant des juridictions respectives des Parties, ou produites dans le cadre du présent Accord. Le présent Accord définit les procédures et les mesures de sécurité permettant d'assurer cette protection.

2. Les Parties s'engagent à prendre toutes les mesures appropriées dans le respect de leurs lois et réglementations nationales afin de garantir la protection des Informations classifiées conformément au présent Accord.

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

4. Le présent Accord ne constitue pas un fondement permettant de contraindre les Parties à fournir ou à échanger des Informations classifiées.

Article 2
Définitions

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

a) **« Accord »** désigne le présent document, y compris son annexe.

b) **« Contrat classifié »** désigne tout accord juridiquement contraignant visant à fournir des biens ou des services, conclu par l'une des Parties ou un Contractant relevant de sa juridiction avec un Contractant relevant de la juridiction de l'autre Partie, qui contient des Informations classifiées ou dont l'exécution nécessite l'accès à des Informations classifiées. Ce terme comprend tout contrat de sous-traitance ou toute activité précontractuelle.

c) **« Informations classifiées »** désigne toute information, tout document ou tout objet, quelle que soit sa forme ou sa nature, ou toute partie de ceux-ci, qui a été classifié par l'une des Parties et dont la divulgation, la modification, la compromission ou la perte non autorisées pourraient entraîner des dommages ou des préjudices de gravité variable aux intérêts de l'une ou des deux Parties.

d) **« Autorité compétente en matière de sécurité »** désigne l'autorité publique d'une Partie, ou toute autorité de sécurité compétente déléguée dans un domaine militaire, chargée de superviser la mise en œuvre du présent Accord conformément aux lois et réglementations nationales.

e) **« Contractant »** désigne toute personne physique autre que celles liées par un contrat de travail avec une Partie ou toute personne morale relevant de la juridiction d'une Partie, qui conclut ou est liée par un Contrat classifié, y compris un Sous-traitant.

f) **« Habilitation de sécurité d'établissement »** désigne une décision positive, confirmée par l'Autorité compétente en matière de sécurité, selon laquelle un établissement dispose de mesures de sécurité appropriées pour accéder et traiter des Informations classifiées jusqu'à un niveau de classification de sécurité spécifié, conformément à ses lois et réglementations nationales.

g) **« Besoin d'en connaître »** désigne l'exigence pour une personne physique ou morale d'accéder à des Informations classifiées, d'en avoir connaissance ou d'en détenir pour l'exécution de leurs tâches ou services officiels.

h) **« Partie d'origine »** désigne la Partie sous l'autorité de laquelle les Informations classifiées ont été créées.

i) **« Habilitation de sécurité du personnel »** désigne une décision positive, confirmée par l'Autorité compétente en matière de sécurité, selon laquelle une personne est autorisée à accéder et traiter des Informations classifiées jusqu'à un niveau de classification spécifié, conformément à ses lois et réglementations nationales.

j) **« Entité émettrice »** désigne la Partie ou le Contractant relevant de sa juridiction qui communique des Informations classifiées à l'Entité destinataire en vertu du présent Accord.

k) **« Entité destinataire »** désigne la Partie ou le Contractant relevant de sa juridiction qui reçoit des Informations classifiées de la part de l'Entité émettrice dans le cadre du présent Accord.

l) **« Guide de classification de sécurité »** désigne un document annexé à un Contrat classifié qui précise les niveaux de classification de sécurité applicables à chaque élément dudit Contrat classifié.

m) **« Incident de sécurité »** désigne toute divulgation, modification, compromission, perte, accès, traitement, stockage ou destruction non autorisés d'Informations classifiées, contraires aux lois et réglementations nationales de l'Entité destinataire ou au présent Accord.

n) **« Sous-traitant »** désigne un Contractant auquel un Contractant principal attribue un contrat de sous-traitance.

o) « **Tiers** » désigne tout État, y compris toute entité publique ou privée relevant de sa juridiction, ou toute organisation internationale qui n'est pas l'une des Parties au présent Accord.

Article 3
Autorités compétentes en matière de sécurité

1. Les Autorités compétentes en matière de sécurité des Parties sont énumérées à l'annexe du présent Accord.

2. Les Autorités compétentes en matière de sécurité se fournissent mutuellement leurs coordonnées officielles et s'informent de toute modification les concernant.

Article 4
Niveaux de classification de sécurité

1. Les Parties s'engagent à protéger les Informations classifiées qu'elles échangent entre elles et conviennent que les niveaux de classification de sécurité suivants sont équivalents. La traduction anglaise des niveaux de classification de sécurité respectifs des Parties est informelle, ne fait pas partie des lois et réglementations nationales des Parties et ne peut pas être utilisée pour marquer les Informations classifiées.

Pour le Royaume des Pays-Bas	**Pour le Grand-Duché de Luxembourg**	**En langue anglaise**
Stg. ZEER GEHEIM	TRES SECRET LUX	TOP SECRET
Stg. GEHEIM	SECRET LUX	SECRET
Stg. CONFIDENTIEEL	CONFIDENTIEL LUX	CONFIDENTIAL
DEPARTEMENTAAL VERTROUWELIJK	RESTREINT LUX	RESTRICTED

Article 5
Mesures de sécurité

1. Conformément à leurs lois et réglementations nationales, les Parties s'engagent à mettre en œuvre des mesures appropriées pour protéger les Informations classifiées produites ou échangées dans le cadre du présent Accord. Chaque Partie accorde à ces Informations classifiées au moins le même niveau de protection que celui accordé à ses propres Informations classifiées ayant un niveau de classification de sécurité équivalent, tel que défini à l'article 4 du présent Accord.

2. Lorsque ces Informations classifiées sont traitées, stockées ou transmises au moyen de systèmes de communication et d'information, ces mesures garantissent la confidentialité, l'intégrité, la disponibilité, la non-répudiation, l'authenticité et la traçabilité de l'accès aux Informations classifiées. Les Parties veillent à ce que ces Informations classifiées soient stockées et traitées conformément à leurs lois et réglementations nationales.

3. Toute Information classifiée communiquée dans le cadre du présent Accord est marquée du niveau de classification de sécurité approprié, conformément aux lois et réglementations nationales de la Partie d'origine.

4. L'Entité destinataire appose son propre niveau de classification de sécurité à toutes les Informations classifiées reçues de la Partie émettrice dans le cadre du présent Accord, au niveau de classification de sécurité équivalent conformément au tableau figurant à l'article 4, de sorte que l'identité de la Partie d'origine soit toujours clairement identifiable.

5. Lorsque la forme ou la nature des Informations classifiées ne permet pas à l'Entité destinataire d'apposer un tel marquage à son propre niveau de classification de sécurité correspondant, les Autorités compétentes en matière de sécurité déterminent si le marquage réalisé par la Partie d'origine est suffisant.

6. L’Entité destinataire ne peut pas modifier ni supprimer la classification de sécurité des Informations classifiées reçues en vertu du présent Accord sans l'accord écrit de la Partie d'origine.

7. La Partie d'origine s'assure que l’Entité destinataire est informée de toute modification du niveau de classification de sécurité des Informations classifiées fournies, afin d'appliquer les mesures de protection appropriées.

8. La Partie d’origine peut ajouter en anglais sur les Informations classifiées des exigences concernant leur traitement afin de préciser toute restriction relative à leur utilisation, leur divulgation, leur communication et leur accès par l’Entité destinataire.

9. Les Parties prennent toutes les mesures appropriées pour garantir que l’Entité destinataire :

   a) veille à ce que les Informations classifiées ne soient pas divulguées ni communiquées à un Tiers sans le consentement écrit préalable de la Partie d'origine ;

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

Article 6
Accès aux informations classifiées

1. L'accès aux Informations classifiées n'est accordé qu'aux personnes ayant un Besoin d'en connaître, ayant été informées de leurs responsabilités en matière de protection des Informations classifiées et ayant reconnu leurs responsabilités en matière de protection des Informations classifiées en vertu des lois et réglementations nationales de l’Entité destinataire.

2. Outre les exigences énoncées au paragraphe 1 du présent article, l'accès aux Informations classifiées de niveau CONFIDENTIEL LUX/Stg. CONFIDENTIEEL et supérieur n’est accordé qu'aux personnes disposant d'une Habilitation de sécurité du personnel au moins au niveau équivalent ou qui ont été dûment autorisées à accéder à des Informations classifiées en raison de leurs fonctions, conformément aux lois et réglementations nationales de l’Entité destinataire.

Article 7
Contrats classifiés

1. À la demande de la Partie d'origine, l’Autorité compétente en matière de sécurité de l’Entité destinataire s'engage à informer l’Autorité compétente en matière de sécurité de la Partie d'origine si un Contractant, relevant de sa juridiction et participant à un Contrat classifié ou à des négociations précontractuelles concernant un Contrat classifié et nécessitant l'accès à des Informations classifiées, a obtenu une Habilitation de sécurité d’établissement au niveau de classification de sécurité requis. Si, à la réception de la demande, le Contractant ne détient pas d’Habilitation de sécurité d’établissement ou si celle-ci est d'un niveau inférieur à celui requis, l’Autorité compétente en matière de sécurité qui a présenté la demande en est informée.

2. Si une Partie ou un Contractant relevant de sa juridiction propose un Contrat classifié impliquant l'accès à des Informations classifiées de niveau CONFIDENTIEL LUX/Stg. CONFIDENTIEEL ou supérieur, à un Contractant relevant de la juridiction de l'autre Partie, l'Autorité compétente en matière de sécurité de l'autre Partie doit avoir confirmé au préalable par écrit que le Contractant a obtenu une Habilitation de sécurité d'établissement au niveau approprié. Pour les Contrats classifiés de niveau RESTREINT LUX/DEPARTEMENTAAL VERTROUWELIJK, une Habilitation de sécurité d'établissement peut être requise, conformément aux lois et réglementations nationales de la Partie dont relève le Contractant.

3. L'Autorité compétente en matière de sécurité de la Partie ayant juridiction sur le Contractant veille à ce que le Contractant :

   a) s'assure que toutes les personnes ayant accès à des Informations classifiées soient informées de leurs responsabilités en matière de protection des Informations classifiées, conformément à leurs lois et réglementations nationales et au présent Accord ;

   b) surveille la mise en œuvre des mesures de sécurité dans ses établissements ;

   c) notifie son Autorité compétente en matière de sécurité de tout incident de sécurité lié au Contrat classifié dans les plus brefs délais.

4. Outre les exigences énoncées au paragraphe 3 du présent article, pour les Contrats classifiés impliquant l'accès aux Informations classifiées de niveau CONFIDENTIEL LUX/Stg. CONFIDENTIEEL ou supérieur, l'Autorité compétente en matière de sécurité veille à ce que le contractant détienne une Habilitation de sécurité d'établissement au niveau de classification de sécurité correspondant afin de protéger les Informations classifiées et à ce que les personnes devant avoir accès à des Informations classifiées détiennent une Habilitation de sécurité du personnel au niveau de classification de sécurité correspondant.

5. Tout Contrat classifié inclut des exigences de sécurité précisant les aspects suivants :

   a) un Guide de classification de sécurité ;

   b) une procédure de notification des modifications du niveau de classification de sécurité, compte tenu de l'article 5 paragraphe 7 du présent Accord ;

   c) les canaux et procédures à utiliser pour le transport et/ou la transmission d'Informations classifiées ;

   d) les instructions relatives au traitement, au stockage, à la destruction et au renvoi d'Informations classifiées ;

   e) les coordonnées des Autorités compétentes en matière de sécurité chargées de superviser la protection des Informations classifiées liées au Contrat classifié ;

   f) l'obligation de signaler tout Incident de sécurité à l'Autorité compétente en matière de sécurité du Contractant et l'obligation pour les Contractants de prendre toutes les mesures raisonnables pour atténuer les effets d'une telle faille de sécurité, en consultation avec l'Autorité compétente en matière de sécurité ;

   g) dans le cas où un Contrat classifié est sous-traité en tout ou en partie à un Sous-traitant, l'obligation d'imposer au Sous-traitant toutes les stipulations concernant les Contractants figurant dans le présent Accord ;

h) une référence au présent Accord ;

i) une déclaration selon laquelle les Informations classifiées échangées ou produites dans le cadre du Contrat classifié sont protégées par le Contractant conformément aux lois et réglementations nationales applicables ainsi qu'au présent Accord.

6. Si un Contrat classifié est attribué, la Partie ou un Contractant relevant de sa juridiction transmet, par l'intermédiaire de son Autorité compétente en matière de sécurité, une copie des exigences de sécurité visées au paragraphe 5 du présent article à l'Autorité compétente en matière de sécurité de l'Entité destinataire, afin de faciliter la supervision de la sécurité du Contrat classifié.

7. Les procédures d'approbation des visites associées aux activités relevant des Contrats classifiés effectuées par le personnel d'une Partie auprès de l'autre Partie sont conformes à l'article 8 du présent Accord.

Article 8
Visites

1. Les visites nécessitant l'accès à des Informations classifiées de niveau CONFIDENTIEL LUX/Stg. CONFIDENTIEEL ou supérieur sont soumises à l'accord écrit préalable de l'Autorité compétente en matière de sécurité de la Partie hôte, sauf convention contraire des Autorités compétentes en matière de sécurité. Cet accord n'est donné qu'aux personnes visées à l'article 6 du présent Accord. En ce qui concerne les visites nécessitant l'accès à des informations classifiées portant la mention RESTREINT LUX/DEPARTEMENTAAL VERTROUWELIJK, l'accord écrit préalable de l'Autorité compétente en matière de sécurité de la Partie hôte peut être requis, conformément aux lois et réglementations nationales de la Partie sous la juridiction de laquelle la visite a lieu.

2. Le visiteur soumet sa demande de visite au moins dix jours calendaires avant la date proposée à son Autorité compétente en matière de sécurité, qui la transmet à l'Autorité compétente en matière de sécurité de l'autre Partie. En cas d'urgence, les Autorités compétentes en matière de sécurité peuvent convenir d'un délai plus court.

3. La demande de visite inclut :

a) le nom complet du visiteur, la date et le lieu de naissance, la nationalité et le numéro de passeport/carte d'identité ;

b) le titre officiel et la fonction actuelle du visiteur, ainsi que le nom de l'organisation qu'il représente ou à laquelle il appartient ;

c) la confirmation de l'Habilitation de sécurité du personnel du visiteur, de son niveau et de sa validité ;

d) la date et la durée de la visite. En cas de visites répétées, la durée totale couverte par les visites est indiquée ;

e) le but de la visite et le niveau de classification de sécurité le plus élevé prévu pour les Informations classifiées qui seront discutées ou consultées ;

f) le nom, l'adresse, le numéro de téléphone, l'adresse de courrier électronique du point de contact de l'établissement à visiter ;

g) la signature datée et tamponnée d'un représentant de l'Autorité compétente en matière de sécurité du visiteur.

4. Les Autorités compétentes en matière de sécurité peuvent convenir d'une liste de visiteurs autorisés à effectuer des visites régulières pendant une période n'excédant pas douze mois. Les Autorités compétentes en matière de sécurité s'accordent sur les modalités supplémentaires concernant les visites régulières.

5. L'Autorité compétente en matière de sécurité de la Partie hôte communique aux responsables de la sécurité de l'établissement qui fera l'objet de la visite les coordonnées des personnes dont la demande de visite a été approuvée. Une fois l'autorisation accordée, les modalités de visite pour les personnes autorisées à effectuer des visites régulières peuvent être convenues directement avec le responsable de l'établissement concerné.

6. Les Informations classifiées fournies à un visiteur ou obtenues par celui-ci doivent être traitées conformément aux dispositions du présent Accord.

Article 9
Transfert d'informations classifiées

1. Les Informations classifiées de niveau CONFIDENTIEL LUX/Stg. CONFIDENTIEEL ou supérieur sont transférées par courrier diplomatique, gouvernemental ou militaire, ou par tout autre moyen convenu au préalable par les Autorités compétentes en matière de sécurité, conformément à leurs lois et réglementations nationales.

2. Les Informations classifiées de niveau RESTREINT LUX/DEPARTEMENTAAL VERTROUWELIJK peuvent être transférées par des services postaux conformément aux lois et réglementations nationales.

3. La transmission électronique d'Informations classifiées ne peut avoir lieu qu'en utilisant des moyens cryptographiques conformément aux procédures qui seront convenues par les Autorités compétentes en matière de sécurité.

4. Les Informations classifiées de niveau CONFIDENTIEL LUX/Stg. CONFIDENTIEEL ou supérieur sont enregistrées.

Article 10
Reproduction et traduction d'informations classifiées

1. Les originaux et les traductions d'Informations classifiées de niveau TRÈS SECRET LUX/Stg. ZEER GEHEIM ne sont pas reproduites ni traduites sans l'accord écrit préalable de la Partie d'origine.

2. Les reproductions et traductions d'Informations classifiées sont marquées du niveau de classification de sécurité des Informations classifiées originales et sont protégées de la même manière que les Informations classifiées originales.

3. Le nombre de reproductions et de traductions est limité au strict minimum pour l'utilisation prévue dans le cadre du présent Accord.

4. Les traductions indiquent expressément dans la langue de traduction qu'elles contiennent des Informations classifiées reçues de la Partie d'origine.

Article 11
Destruction des informations classifiées

1. Les Informations classifiées de niveau TRÈS SECRET LUX/Stg. ZEER GEHEIM ne peuvent être détruites qu'avec l'accord écrit préalable de la Partie d'origine. Par défaut, elles sont restituées à la Partie émettrice après avoir été reconnues par l'Entité destinataire comme n'étant plus nécessaires.

2. Les Informations classifiées de niveau SECRET LUX/Stg. GEHEIM ou inférieure sont détruites après avoir été reconnues par l'Entité destinataire comme n'étant plus nécessaires, de manière à empêcher leur reconstitution totale ou partielle.

3. Lorsqu'une situation de crise empêche une Entité destinataire de protéger les Informations classifiées fournies en vertu du présent Accord, celles-ci sont détruites immédiatement. L'Entité destinataire informe, par l'intermédiaire de son Autorité compétente en matière de sécurité, par écrit et dans les meilleurs délais l'Autorité compétente en matière de sécurité de la Partie d'origine de la destruction de ces Informations classifiées.

Article 12
Coopération en matière de sécurité

1. Les Autorités compétentes en matière de sécurité s'informent mutuellement, sur demande, des modifications apportées à leurs lois et réglementations nationales, à leurs politiques et à leurs pratiques en matière de protection des Informations classifiées.

2. À la demande de l'Autorité compétente en matière de sécurité d'une des Parties, l'Autorité compétente en matière de sécurité de l'autre Partie confirme par écrit la délivrance d'une Habilitation de sécurité du personnel à une personne physique ou d'une Habilitation de sécurité d'établissement à une personne morale.

3. Dans le cadre du présent Accord, chaque Partie reconnaît les Habilitations de sécurité du personnel et les Habilitations de sécurité d'établissement délivrées par l'autre Partie.

4. Sur demande et conformément à leurs lois et réglementations nationales, les Autorités compétentes en matière de sécurité se prêtent mutuellement assistance pour mener à bien les enquêtes relatives aux demandes d'Habilitations de sécurité du personnel et d'Habilitations de sécurité d'établissement.

5. Les Autorités compétentes en matière de sécurité se tiennent mutuellement informées sans délai par écrit des modifications apportées aux Habilitations de sécurité du personnel et aux Habilitations de sécurité d'établissement pour lesquelles une confirmation a été fournie.

6. Dans le cadre du présent Accord et nonobstant l'article 9, chaque Partie reconnaît un acte d'approbation formel délivré par l'autre Partie concernant les équipements et mécanismes liés aux systèmes de communication et d'information utilisés pour traiter les Informations classifiées de l'autre Partie. Si nécessaire, la liste mise à jour des équipements et mécanismes approuvés est échangée entre les Autorités compétentes en matière de sécurité.

7. La coopération dans le cadre du présent Accord est menée en anglais.

Article 13
Incident de sécurité

1. Si l'Entité destinataire soupçonne ou constate un Incident de sécurité concernant les Informations classifiées de la Partie d'origine, elle en informe immédiatement par écrit son Autorité compétente en matière de sécurité. La notification contient suffisamment de détails pour que la Partie d'origine puisse évaluer les conséquences et les circonstances de la violation présumée ou avérée.

2. Les Autorités compétentes en matière de sécurité s'informent immédiatement par écrit de tout Incident de sécurité réel ou potentiel impliquant des Informations classifiées.

3. L'Entité destinataire doit immédiatement enquêter sur tout Incident de sécurité réel ou potentiel. L'Autorité compétente en matière de sécurité de la Partie d'origine coopère, si nécessaire, à l'enquête.

4. L'Autorité compétente en matière de sécurité de l'Entité destinataire prend les mesures appropriées, conformément à ses lois et réglementations nationales, afin de limiter les conséquences et d'empêcher que l'Incident de sécurité ne se reproduise. L'Autorité compétente en matière de sécurité de la Partie d'origine est informée du résultat de l'enquête et, le cas échéant, des mesures prises.

Article 14
Coûts

Chaque Partie prend en charge ses propres frais encourus dans le cadre de la mise en œuvre et de l'exécution de ses obligations en vertu du présent Accord.

Article 15
Règlement des litiges

Tout litige découlant de l'interprétation, de la mise en œuvre ou de l'application du présent Accord sera réglé exclusivement par consultation ou négociation entre les Parties par la voie diplomatique.

Article 16
Articulation avec d'autres accords

Le présent Accord ne prévaut sur aucun accord international qui a déjà été conclu ou qui pourrait être conclu et qui régit spécifiquement l'échange et la protection mutuelle des Informations classifiées.

Article 17
Modalités d'application

Les Autorités compétentes en matière de sécurité des Parties ou toute autre autorité compétente en matière de sécurité des Parties peuvent se consulter sur les aspects techniques détaillés liés à l'application du présent Accord et peuvent convenir, au cas par cas, de modalités d'application appropriées conformément au présent Accord.

Article 18
Dispositions finales

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

2. Chaque Partie notifie à l'autre Partie, par voie diplomatique, l'achèvement des procédures nationales nécessaires à l'entrée en vigueur du présent Accord. Le présent Accord entrera en vigueur le premier jour du deuxième mois suivant la réception de cette dernière notification.

3. En ce qui concerne le Royaume des Pays-Bas, le présent Accord s'applique à la partie européenne des Pays-Bas et à la partie caribéenne des Pays-Bas (les îles de Bonaire, Saint-Eustache et Saba).

4. Le présent Accord, y compris son annexe, peut être modifié d'un commun accord des Parties. Chacune des Parties peut proposer à tout moment des amendements au présent Accord par voie diplomatique. Ces amendements entrent en vigueur dans les conditions prévues au paragraphe 2 du présent article, à l'exception d'un amendement concernant les Autorités compétentes en matière de sécurité énumérées à l'annexe, qui entre en vigueur à une date à convenir entre les Parties.

5. Chacune des Parties peut résilier le présent Accord à tout moment par écrit et par voie diplomatique. Dans ce cas, l'Accord prendra fin six mois après réception de cette notification.

6. En cas de résiliation du présent Accord, les Informations classifiées échangées, communiquées ou produites dans le cadre du présent Accord resteront protégées conformément aux dispositions de ce dernier avant sa résiliation, tant que les Informations classifiées resteront classifiées.

EN FOI DE QUOI, les représentants des Parties, dûment mandatés à cet effet, ont signé le présent Accord.

FAIT à Luxembourg, le 21 avril 2026, en deux exemplaires originaux, en langues française, néerlandaise et anglaise, les trois textes faisant également foi.
En cas de divergence d'interprétation, le texte anglais prévaut.

POUR LE GRAND-DUCHÉ DE LUXEMBOURG



Xavier Bettel

Ministre des Affaires étrangères et du Commerce extérieur

POUR LE ROYAUME DES PAYS-BAS



Tom Berend Willem Berendsen

Ministre des Affaires étrangères

ANNEXE

L'Autorité compétente en matière de sécurité pour le Royaume des Pays-Bas est :

Autorité nationale de sécurité civile
Service général de renseignement et de sécurité
Ministère de l'Intérieur et des Relations du Royaume

Autorité déléguée compétente en matière de sécurité :
Autorité nationale de sécurité militaire
Autorité de sécurité en matière de défense
Direction générale de la politique
Ministère de la Défense.

L'autorité compétente en matière de sécurité pour le Grand-Duché de Luxembourg est :
Ministère d'État
Service de renseignement de l'État
Autorité nationale de sécurité.

AGREEMENT

BETWEEN

THE GRAND DUCHY OF LUXEMBOURG

AND

THE KINGDOM OF THE NETHERLANDS

CONCERNING THE EXCHANGE AND MUTUAL PROTECTION OF CLASSIFIED INFORMATION

The Grand Duchy of Luxembourg

and

the Kingdom of the Netherlands,

Hereinafter jointly referred to as “the Parties”, and each individually as a “Party”,

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

Wishing to ensure the mutual protection of Classified Information have, in the interests of national security, agreed upon the following:

Article 1
Purpose and scope

1. The purpose of this Agreement is to ensure the protection of Classified Information either exchanged between the Parties, between a Party and a Contractor under the jurisdiction of the other Party or between Contractors under the respective Parties' jurisdictions, or generated under this Agreement. This Agreement sets out the security procedures and arrangements for such protection.

2. The Parties shall take all appropriate measures under their national laws and regulations to ensure the protection of Classified Information in accordance with this Agreement.

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

4. This Agreement does not constitute a basis to compel the provision or exchange of Classified Information by the Parties.

Article 2
Definitions

For the purpose of this Agreement, the following definitions mean:

a) **"Agreement"** means this document including its Annex.

b) **"Classified Contract"** means any legally enforceable agreement to provide goods or services to be entered into by one of the Parties or a Contractor under its jurisdiction with a Contractor under the jurisdiction of the other Party, which contains Classified Information or the performance of which requires access to Classified Information. This term includes a sub-contract or any pre-contractual activity.

c) **"Classified Information"** means any information, material or object, regardless of its form or nature, or any parts thereof, marked with a security classification by one of the Parties, the unauthorised disclosure, alteration, compromise or loss of which could cause varying degrees of damage or harm to the interests of one or both of the Parties.

d) **"Competent Security Authority"** means the government authority in a Party, or any delegated competent security authority in a military domain, responsible for supervising the implementation of this Agreement in accordance with the national laws and regulations.

e) **"Contractor**" means any individual other than those engaged by a Party under a contract of employment or any legal entity under the jurisdiction of a Party, entering into or bound by a Classified Contract, including a Sub-contractor.

f) **"Facility Security Clearance"** means a positive determination, confirmed by the Competent Security Authority, that a facility has in place appropriate security measures to access and handle Classified Information up to and including a specified security classification level, in accordance with its national laws and regulations.

g) **"Need to Know"** means the requirement for an individual or legal entity to access, have knowledge of or possess Classified Information in order to be able to perform their official tasks or services.

h) **"Originating Party"** means the Party under whose authority Classified Information has been created.

i) **"Personnel Security Clearance"** means a positive determination, confirmed by the Competent Security Authority, that an individual has been security cleared to access and handle Classified Information up to and including a specified classification level, in accordance with its national laws and regulations.

j) **"Providing Entity"** means the Party or Contractor, under its jurisdiction, which releases Classified Information to the Receiving Entity under this Agreement.

k) **"Receiving Entity"** means the Party or Contractor under its jurisdiction, which receives Classified Information from the Providing Entity under this Agreement.

l) **"Security Classification Guide"** means a document associated with a Classified Contract specifying the applicable security classification levels of each part of that Classified Contract.

m) **"Security Incident"** means any unauthorised disclosure, alteration, compromise, loss, access, handling, storage or destruction of Classified Information, contrary to national laws and regulations of the Receiving Entity or this Agreement.

n) **"Sub-contractor**" means a Contractor to whom a prime Contractor grants a sub-contract.

o) **"Third Party"** means any State, including any public or private entity under its jurisdiction, or any international organisation, which is not a Party to this Agreement.

Article 3
Competent Security Authorities

1. The Competent Security Authorities of the Parties are listed in the Annex of this Agreement.

2. The Competent Security Authorities shall provide each other with official contact details and changes thereof.

Article 4
Security classification levels

1. The Parties undertake to protect Classified Information exchanged between them and agree that the following security classification levels shall be equivalent. The informal translation in English of the Parties' respective security classification levels, is not part of the national laws and regulations of the Parties and shall not be used to mark Classified Information.

For the Kingdom of the Netherlands	**For the Grand Duchy of Luxembourg**	**In the English language**
Stg. ZEER GEHEIM	TRES SECRET LUX	TOP SECRET
Stg. GEHEIM	SECRET LUX	SECRET
Stg. CONFIDENTIEEL	CONFIDENTIEL LUX	CONFIDENTIAL
DEPARTEMENTAAL VERTROUWELIJK	RESTREINT LUX	RESTRICTED

Article 5
Security measures

1. In accordance with their national laws and regulations, the Parties shall ensure the implementation of appropriate measures to protect Classified Information, which is generated or exchanged under this Agreement. Each Party shall afford to such Classified Information at least the same level of protection as afforded to their own Classified Information of the equivalent security classification levels as set forth in Article 4 of this Agreement.

2. When such Classified Information is processed, stored or transmitted via communication and information systems, these measures shall guarantee the confidentiality, integrity, availability, non-repudiation, authenticity and traceability of access to Classified Information. The Parties shall ensure that such Classified Information is stored and handled in accordance with their national laws and regulations.

3. Any Classified Information released under this Agreement shall be marked with the appropriate security classification level in accordance with the national laws and regulations of the Originating Party.

4. The Receiving Entity shall apply its own security classification to all Classified Information received from the Providing Entity under this Agreement, at the equivalent security classification level in accordance with the scheme contained in article 4, in such a way that it is always clear who the Originating Party is.

5. Where the form or nature of the Classified Information does not allow such marking by the Receiving Entity to apply its own corresponding security classification level, the Competent Security Authorities shall decide whether the marking by the Originating Party suffices.

6. The Receiving Entity shall not modify or revoke the security classification of received Classified Information under this Agreement without the written approval of the Originating Party.

7. The Originating Party shall ensure that the Receiving Entity will be informed of any change in the security classification level of the Classified Information provided, in order to apply the appropriate protection measures.

8. The Originating Party may add handling requirements, in English, on the Classified Information, to specify any limitations on its use, disclosure, release and access by the Receiving Entity.

9. The Parties shall take all appropriate measures to ensure that the Receiving Entity:

   a) ensures that Classified Information is not disclosed or released to a Third Party without the prior written consent of the Originating Party;

   b) uses Classified Information solely for the purpose it has been released for and within the limitations stated by the Originating Party.

Article 6
Access to Classified Information

1. Access to Classified Information shall be granted only to those individuals who have a Need to Know, are briefed on their responsibilities for the protection of Classified Information, and have acknowledged their responsibilities to protect Classified Information in accordance with the national laws and regulations of the Receiving Entity.

2. In addition to the requirements in paragraph 1 of this article, access to Classified Information marked as CONFIDENTIEL LUX/Stg. CONFIDENTIEEL and above, shall be granted only to those individuals who hold a Personnel Security Clearance at least at the corresponding level or who are otherwise duly authorized to access Classified Information by virtue of their function in accordance with the national laws and regulations of the Receiving Entity.

Article 7
Classified contracts

1. Upon request of the Originating Party, the Competent Security Authority of the Receiving Entity shall inform the Competent Security Authority of the Originating Party whether a Contractor, under its jurisdiction and participating in a Classified Contract or precontractual negotiations regarding a Classified Contract and requiring access to Classified Information, has been issued a Facility Security Clearance at the required security classification level. If the Contractor does not, at that point, hold a Facility Security Clearance, or the Facility Security Clearance is at a lower level than that required, the requesting Competent Security Authority shall be informed thereof.

2. If a Party or a Contractor under its jurisdiction proposes to award a Classified Contract involving access to Classified Information marked as CONFIDENTIEL LUX/Stg. CONFIDENTIEEL or above, to a Contractor under the jurisdiction of the other Party, it shall first obtain written confirmation from the Competent Security Authority of the other Party that the Contractor has been granted a Facility Security Clearance at the appropriate security classification level. For Classified Contracts at the security classification level equivalent to RESTREINT LUX/DEPARTEMENTAAL VERTROUWELIJK, a Facility Security Clearance may be required, in accordance with national laws and regulations of the Party under whose jurisdiction the Contractor operates.

3. The Competent Security Authority of the Party having jurisdiction over the Contractor shall ensure that the Contractor:

   a) ensures that all individuals granted access to Classified Information are informed of their responsibilities to protect Classified Information in accordance with their national laws and regulations as well as with this Agreement;

   b) monitors the security conduct within its facilities;

   c) notifies promptly its Competent Security Authority of any Security Incident relating to the Classified Contract.

4. In addition to the requirements in paragraph 3 of this article, for Classified Contracts involving access to Classified Information marked as CONFIDENTIEL LUX/Stg. CONFIDENTIEEL or above, the Competent Security Authority shall ensure that the Contractor holds a Facility Security Clearance at the corresponding security classification level in order to protect the Classified Information and that the individuals requiring access to Classified Information hold a Personnel Security Clearance at the corresponding security classification level.

5. Every Classified Contract shall include security requirements which identify the following aspects:

   a) a Security Classification Guide;

   b) a procedure for notification of changes in the security classification level, taking into account article 5, paragraph 7 of this Agreement;

   c) the channels and procedures to be used for the transport and/or transmission of Classified Information;

   d) instructions for the handling, storage, destruction and returning of Classified Information;

   e) contact details of the Competent Security Authorities responsible for overseeing the protection of Classified Information related to the Classified Contract;

   f) the obligation to notify any Security Incidents to the Competent Security Authority of the Contractor and the obligation for Contractors to take all reasonable steps to assist in mitigating the effect of such a security violation, in consultation with the Competent Security Authority;

   g) in case a Classified Contract is sub-contracted, in whole or in part, to a sub-Contractor, the obligation to impose all the stipulations concerning Contractors in this Agreement to the sub-Contractor;

h) a reference to this Agreement;

i) a statement that Classified Information exchanged or generated pursuant to the Classified Contract shall be protected by the Contractor in accordance with the applicable national laws and regulations as well as with this Agreement.

6. If a Classified Contract is awarded, the Party or a Contractor under its jurisdiction shall, via its Competent Security Authority, forward a copy of the security requirements referred to in paragraph 5 of this Article to the Competent Security Authority of the Receiving Entity, to facilitate the security oversight of the Classified Contract.

7. The procedures for the approval of visits associated with Classified Contract activities by personnel of one Party to the other Party, shall be in accordance with article 8 of this Agreement.

Article 8
Visits

1. Visits requiring access to Classified Information marked as CONFIDENTIEL LUX/Stg. CONFIDENTIEEL or above are subject to the prior written consent of the Competent Security Authority of the host Party, unless otherwise agreed between the Competent Security Authorities. Such consent shall be given only to individuals referred to in article 6 of this Agreement. With respect to visits requiring access to Classified Information marked as RESTREINT LUX/DEPARTEMENTAAL VERTROUWELIJK, the prior written consent of the Competent Security Authority of the host Party may be required, in accordance with the national laws and regulations of the Party under whose jurisdiction the visit occurs.

2. The visitor shall submit the request for a visit at least ten calendar days in advance of the proposed date of the visit to his Competent Security Authority, which shall forward it to the Competent Security Authority of the other Party. In urgent cases, the Competent Security Authorities may agree on a shorter period.

3. The request for a visit shall include:

a) full name of the visitor, date and place of birth, nationality and passport/ID card number;

b) official title and present position of the visitor and name of the organization the visitor represents or to which the visitor belongs;

c) confirmation of the visitor's Personnel Security Clearance and its level and validity;

d) date and duration of the visit. In the case of recurring visits, the total period covered by the visits shall be stated;

e) purpose of the visit and the anticipated highest security classification level of Classified Information to be discussed or accessed;

f) name, address, phone number, e-mail address of the point of contact of the facility to be visited;

g) dated and stamped signature of a representative of the visitor's Competent Security Authority.

4. The Competent Security Authorities may agree on a list of visitors entitled to recurring visits for a period not exceeding twelve months. The Competent Security Authorities shall agree on the further details of the recurring visits.

5. The Competent Security Authority of the host Party shall inform the security officials of the facility to be visited, of the details of those individuals whose visit request has been approved. Once approval has been given, visit arrangements for individuals who have been given approval for recurring visits may be made directly with the facility concerned.

6. Classified Information provided to or acquired by a visitor shall be handled in accordance with the provisions of this Agreement.

Article 9
Transfer of classified information

1. Classified Information marked as CONFIDENTIEL LUX/Stg. CONFIDENTIEEL or above shall be transferred by means of diplomatic, government or military couriers, or by any other means agreed upon in advance by the Competent Security Authorities, in accordance with their national laws and regulations.

2. Classified Information marked as RESTREINT LUX/DEPARTEMENTAAL VERTROUWELIJK may be transferred by postal services in accordance with the national laws and regulations.

3. Electronic transmission of Classified Information may take place only by using cryptographic means in accordance with procedures to be agreed upon by the Competent Security Authorities.

4. Classified Information marked as CONFIDENTIEL LUX/Stg. CONFIDENTIEEL or above shall be registered.

Article 10
Reproduction and translation of classified information

1. Classified Information marked as TRES SECRET LUX/Stg. ZEER GEHEIM, both the original and the translation, shall not be reproduced or translated without the prior written consent of the Originating Party.

2. Reproductions and translations of Classified Information shall be marked with the original markings and protected in the same way as the original Classified Information.

3. Reproductions and translations shall be limited to the minimum amount required for use under this Agreement.

4. Translations shall contain a suitable annotation in the language of translation, indicating that they contain Classified Information received from the Originating Party.

Article 11
Destruction of classified information

1. Classified Information marked as TRES SECRET LUX/Stg. ZEER GEHEIM shall be destroyed only with the prior written consent of the Originating Party. By default, it shall be returned to the Originating Party after it is no longer considered necessary by the Receiving Entity.

2. Classified Information marked as SECRET LUX/Stg. GEHEIM or below, shall be destroyed after it is no longer considered necessary by the Receiving Entity, insofar as to prevent its reconstruction in whole or in part.

3. If a crisis situation makes it impossible for a Receiving Entity to protect Classified Information provided under this Agreement, the Classified Information shall be destroyed immediately. The Receiving Entity shall, via its Competent Security Authority, notify the Competent Security Authority of the Originating Party as soon as possible and in writing of the destruction of this Classified Information.

Article 12
Security cooperation

1. The Competent Security Authorities shall, on request, inform each other about changes in their national laws and regulations, policies and practices for the protection of Classified Information.

2. On request of the Competent Security Authority of one Party, the Competent Security Authority of the other Party shall issue a written confirmation that an individual has been issued a Personnel Security Clearance or a legal entity has been issued a Facility Security Clearance.

3. Within the scope of this Agreement, each Party shall recognize the Personnel Security Clearances and Facility Security Clearances issued by the other Party.

4. The Competent Security Authorities shall assist each other in carrying out Personnel Security Clearance and Facility Security Clearance investigations on request and in accordance with their national laws and regulations.

5. The Competent Security Authorities shall promptly notify each other in writing about changes in Personnel Security Clearances and Facility Security Clearances for which a confirmation has been provided.

6. Within the scope of this Agreement and notwithstanding Article 9, each Party shall recognise a formal act of approval issued by the other Party referring to equipment and mechanisms related to and including communication and information systems which are used to process the other Party's Classified Information. When necessary, the updated list of approved equipment and mechanisms shall be exchanged between the Competent Security Authorities.

7. The cooperation under this Agreement is conducted in English.

Article 13
Security Incident

1. In case a Security Incident of the Classified Information of the Originating Party is suspected or ascertained by the Receiving Entity, it shall inform its Competent Security Authority in writing as soon as possible. The notice must contain sufficient details for the Originating Party to assess the consequences and circumstances of the suspected or actual violation.

2. The Competent Security Authorities shall immediately inform each other in writing of any actual or potential Security Incident involving Classified Information.

3. The Receiving Entity shall immediately investigate any actual or potential Security Incident. The Competent Security Authority of the Originating Party shall, if required, cooperate in the investigation.

4. The Competent Security Authority of the Receiving Entity shall take appropriate measures in accordance with its national laws and regulations to limit the consequences and to prevent a recurrence of the Security Incident. The Competent Security Authority of the Originating Party shall be informed of the outcome of the investigation and, if any, of the measures taken.

Article 14
Costs

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

Article 15
Dispute resolution

Any dispute arising from the interpretation, implementation or application of this Agreement shall be settled exclusively by consultation or negotiations between the Parties through diplomatic channels.

Article 16
Relation to other agreements

This Agreement does not prevail over any international agreement that has already been or may be entered into and that specifically governs the exchange and mutual protection of Classified Information.

Article 17
Implementing arrangements

The Competent Security Authorities of the Parties or any other competent security authorities of the Parties may consult each other on detailed technical aspects relating to the application of this Agreement and may conclude, on a case-by-case basis, appropriate implementing arrangements pursuant to this Agreement.

Article 18
Final provisions

1. This Agreement is concluded for an indefinite period of time.

2. Each Party shall notify the other Party through diplomatic channels once the national procedures necessary for the 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 latter notification.

3. With regard to the Kingdom of the Netherlands, this Agreement shall apply to the European part of the Netherlands and the Caribbean part of the Netherlands (the islands of Bonaire, Sint Eustatius and Saba).

4. This Agreement including its Annex may be amended with the mutual consent of the Parties. Either Party may propose amendments to this Agreement at any time through diplomatic channels. Such amendments shall enter into force under the conditions laid down in paragraph 2 of this article, with the exception of an amendment of the Competent Security Authorities listed in the Annex, which amendment shall enter into force on a date to be agreed upon by the Parties.

5. Either Party may terminate this Agreement in writing at any time through diplomatic channels. In this case, the Agreement shall expire six months after receipt of such notification.

6. In case of termination of this Agreement, all Classified Information exchanged, released or generated under this Agreement shall remain protected in accordance with the terms of this Agreement before it was terminated, for as long as the Classified Information remains classified.

IN WITNESS whereof the representatives of the Parties, duly authorised thereto, have signed this Agreement.

DONE in Luxembourg, on the 21st day of April 2026, in two original copies, in French, Dutch and English languages, the three texts being equally authentic.
In case of divergence of interpretation, the English text shall prevail.

FOR THE GRAND DUCHY OF LUXEMBOURG

Xavier Bettel

Minister for Foreign Affairs and Foreign Trade

FOR THE KINGDOM OF THE NETHERLANDS

Tom Berend Willem Berendsen

Minister of Foreign Affairs

ANNEX

The Competent Security Authority for the Kingdom of the Netherlands is:

Civil National Security Authority
General Intelligence and Security Service
Ministry of the Interior and Kingdom Relations

The delegated competent security authority:
Military National Security Authority
Defence Security Authority
Directorate-General of Policy
Ministry of Defence.

The Competent Security Authority for the Grand Duchy of Luxembourg is:
Ministère d'Etat
Service de renseignement de l'Etat
Autorité nationale de sécurité.

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère des Affaires étrangères
et européennes, de la Défense, de la
Coopération et du Commerce extérieur

Commentaire de l'article unique

L'article unique du projet de loi vise à approuver l'Accord entre le Grand-Duché de Luxembourg et le Royaume des Pays-Bas relatif à l'échange et la protection mutuelle des informations classifiées, fait à Luxembourg, le 21 avril 2026.

Remarque concernant l'article 18, paragraphe 4, de l'Accord :

L'Accord entrera en vigueur lorsque chacune des deux Parties aura rempli les conditions juridiques nécessaires à son entrée en vigueur conformément à leur droit national, tel que prévu par l'article 18, paragraphe 2, de l'Accord. Au Grand-Duché de Luxembourg il s'agira de l'adoption et de la publication d'une loi d'approbation de l'Accord, ainsi que de la ratification de l'Accord. Il convient toutefois de relever que l'article 18, paragraphe 4, de l'Accord prévoit une exception pour ce qui est de la modification des Autorités compétentes en matière de sécurité, énumérées à l'Annexe de l'Accord. En effet, une telle modification entrera en vigueur, tel que prévu par cet article, à une date à convenir entre les Parties. Elle ne nécessitera par conséquent pas d'approbation législative au Grand-Duché de Luxembourg, s'agissant de la modification d'un élément purement technique et se limitant à ce seul aspect, à savoir la modification des Autorités compétentes en matière de sécurité, telles qu'énumérées à l'Annexe.

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère des Affaires étrangères
et européennes, de la Défense, de la
Coopération et du Commerce extérieur

Fiche financière

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

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

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

CHECK DE DURABILITÉ - NOHALTEGKEETSCHECK

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

Ministre responsable :	Le Ministre des Affaires étrangères et européennes
Projet de loi ou amendement :	Projet de loi portant approbation de l'accord entre le Grand-Duché de Luxembourg et le Royaume des Pays-Bas relatif à l'échange et la protection mutuelle des informations classifiées, fait à Luxembourg, le 21 avril 2026

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

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

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

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

Points d'orientation
Documentation
☐ Oui ☒ Non

Le présent accord bilatéral qui prévoit l'échange d'information classifiées entre les gouvernements des deux pays n'est pas concerné par cette question.

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

Points d'orientation
Documentation
☐ Oui ☒ Non

Le présent accord bilatéral qui prévoit l'échange d'information classifiées entre les gouvernements des deux pays n'est pas concerné par cette question.

3. Promouvoir une consommation et une production durables.

Points d'orientation
Documentation
☐ Oui ☒ Non

Le présent accord bilatéral qui prévoit l'échange d'information classifiées entre les gouvernements des deux pays n'est pas

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

Le présent accord bilatéral qui prévoit l'échange d'information classifiées entre les gouvernements des deux pays n'est pas concerné par cette question.

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

Le présent accord bilatéral qui prévoit l'échange d'information classifiées entre les gouvernements des deux pays n'est pas concerné par cette question.

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

Le présent accord bilatéral qui prévoit l'échange d'information classifiées entre les gouvernements des deux pays n'est pas concerné par cette question.

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

Le présent accord bilatéral qui prévoit l'échange d'information classifiées entre les gouvernements des deux pays n'est pas concerné par cette question.

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

Le présent accord bilatéral qui prévoit l'échange d'information classifiées entre les gouvernements des deux pays n'est pas concerné par cette question.

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

Le présent accord bilatéral qui prévoit l'échange d'information classifiées entre les gouvernements des deux pays n'est pas concerné par cette question.

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

Le présent accord bilatéral qui prévoit l'échange d'information classifiées entre les gouvernements des deux pays n'est pas concerné par cette question.

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

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

Continuer avec l'évaluation ? ☐ Oui ☒ Non

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

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

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

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

1. Coordonnées du projet

Intitulé du projet :	Projet de loi portant approbation de l'accord entre le Grand-Duché de Luxembourg et le Royaume des Pays-Bas relatif à l'échange et la protection mutuelle des informations classifiées, fait à Luxembourg, le 21 avril 2026
Ministre initiateur :	Le Ministre des Affaires étrangères et du Commerce extérieur
Auteur(s) :	Daniela HOLDERER
Téléphone :	247 72489
Courriel :	daniela.holderer@mae.etat.lu
Objectif du projet :	Approbation de l'accord bilatéral susmentionné
Autre(s) Ministère(s) / Organisme(s) / Commune(s) impliqué(e)(s) :	Ministère d'Etat (Autorité nationale de sécurité)
Date :	30/06/2026

2. Objectifs à valeur constitutionnelle

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

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

- ☐ Garantir le droit au travail et veiller à assurer l'exercice de ce droit
- ☐ Promouvoir le dialogue social
- ☐ Veiller à ce que toute personne puisse vivre dignement et dispose d'un logement approprié
- ☐ Garantir la protection de l'environnement humain et naturel en œuvrant à l'établissement d'un équilibre durable entre la conservation de la nature, en particulier sa capacité de renouvellement, ainsi que la sauvegarde de la biodiversité, et satisfaction des besoins des générations présentes et futures
- ☐ S'engager à lutter contre le dérèglement climatique et œuvrer en faveur de la neutralité climatique
- ☐ Protéger le bien-être des animaux
- ☐ Garantir l'accès à la culture et le droit à l'épanouissement culturel
- ☐ Promouvoir la protection du patrimoine culturel
- ☐ Promouvoir la liberté de la recherche scientifique dans le respect des valeurs d'une société démocratique fondée sur les droits fondamentaux et les libertés publiques

Remarques :

3. Mieux légiférer

1) Chambre(s) professionnelle(s) à saisir / saisi(e)s pour avis [1] :

- [x] Chambre des fonctionnaires et employés publics
- [x] Chambre des salariés
- [x] Chambre des métiers
- [x] Chambre de commerce
- [x] Chambre d'agriculture

[1] Veuillez indiquer la/les Chambre(s) professionnelle(s) saisie(s) du projet sous rubrique suite à son approbation par le Conseil de gouvernement.

2) Autre(s) partie(s) prenante(s) (organismes divers, citoyens, ...) à saisir / saisi(e)s pour avis : ☐ Oui ☒ Non

Si oui, laquelle / lesquelles :

Remarques / Observations :

3) En cas de transposition de directives européennes, le principe « la directive, rien que la directive » est-il respecté ? ☐ Oui ☐ Non ☒ N.a. [2]

Si non, pourquoi ?

4) Destinataires du projet :

- Entreprises / Professions libérales : ☐ Oui ☒ Non
- Citoyens : ☐ Oui ☒ Non
- Administrations : ☒ Oui ☐ Non

5) Le principe « Think small first » est-il respecté ? ☐ Oui ☐ Non ☒ N.a. [2]
(c.-à-d. des exemptions ou dérogations sont-elles prévues suivant la taille de l'entreprise et/ou son secteur d'activité ?)

Remarques / Observations :

6) Le projet contribue-t-il à la simplification administrative, notamment en supprimant ou en simplifiant des régimes d'autorisation et de déclaration existants, en réduisant les délais de réponse de l'administration, en réduisant la charge administrative pour les destinataires ou en améliorant la qualité des procédures ou de la règlementation ? ☐ Oui ☒ Non

Remarques / Observations :

7) **Le projet en question contient-il des dispositions spécifiques concernant la protection des personnes à l'égard du traitement des données à caractère personnel ?** ☐ Oui ☐ Non ☒ N.a. [2]

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

8) **Y a-t-il un besoin en formation du personnel de l'administration concernée ?** ☐ Oui ☒ Non ☐ N.a. [2]

Si oui, lequel ?

Remarques / Observations :

[2] N.a. : non applicable.

4. Digitalisation et données

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

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

10) **Le projet tient-il compte du principe « digital by default » (priorisation de la voie numérique) ?** ☐ Oui ☒ Non

11) **Le projet crée-t-il une démarche administrative qui nécessite des informations ou des données à caractère personnel sur les** ☐ Oui ☒ Non

Si oui, ces informations ou données à caractère personnel peuvent-elles être obtenues auprès d'une ou plusieurs administrations conformément au principe «Once only» ?

12) **Le projet envisage-t-il la création ou l'adaptation d'une banque de données ?** ☐ Oui ☒ Non

5. Égalité des chances (à remplir pour les projets de règlements grand-ducaux) [3]

13) **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 : Femmes et hommes peuvent postuler aux postes et sont vivement incités à le faire.

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

Si oui, expliquez de quelle manière :

14) Y a-t-il un impact financier différent sur les femmes et les hommes ? ☐ Oui ☐ Non ☒ N.a. [2]

Si oui, expliquez de quelle manière :

[3] Pour les projets de loi, il convient de se référer au point 1 « Assurer une inclusion sociale et une éducation pour tous. » du Nohaltegkeetscheck.

6. Projets nécessitant une notification auprès de la Commission européenne

15) Directive « services » : Le projet introduit-il une exigence en matière d'établissement ou de prestation de services transfrontalière ? ☐ Oui ☐ Non ☒ N.a. [2]

Si oui, veuillez contacter le Ministère de l'Economie en suivant les démarches suivantes :

https://meco.gouvernement.lu/fr/domaines-activites/politique-europeenne/notifications-directive-services.html

16) Directive « règles techniques » : Le projet introduit-il une exigence ou règlementation technique par rapport à un produit ou à un service de la société de l'information (domaine de la technologie et de l'information)? ☐ Oui ☐ Non ☒ N.a. [2]

Si oui, veuillez contacter l'ILNAS en suivant les démarches suivantes :

https://portail-qualite.public.lu/content/dam/qualite/publications/normalisation/2017/ilnas-notification-infoflyer-web.pdf