

No. 57173*

**Belgium
and
Hungary**

Agreement between the Kingdom of Belgium and Hungary on the exchange and mutual protection of classified information. Budapest, 21 September 2015

Entry into force: *1 February 2022, in accordance with article 15(1)*

Authentic texts: *Dutch, English, French and Hungarian*

Registration with the Secretariat of the United Nations: *Belgium, 17 May 2022*

**No UNTS volume number has yet been determined for this record. The Text(s) reproduced below, if attached, are the authentic texts of the agreement /action attachment as submitted for registration and publication to the Secretariat. For ease of reference they were sequentially paginated. Translations, if attached, are not final and are provided for information only.*

**Belgique
et
Hongrie**

Accord entre le Royaume de Belgique et la Hongrie sur l'échange et la protection mutuelle des informations classifiées. Budapest, 21 septembre 2015

Entrée en vigueur : *1^{er} février 2022, conformément au paragraphe 1 de l'article 15*

Textes authentiques : *néerlandais, anglais, français et hongrois*

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : *Belgique, 17 mai 2022*

**Aucun numéro de volume n'a encore été attribué à ce dossier. Les textes disponibles qui sont reproduits ci-dessous sont les textes originaux de l'accord ou de l'action tels que soumis pour enregistrement. Par souci de clarté, leurs pages ont été numérotées. Les traductions qui accompagnent ces textes ne sont pas définitives et sont fournies uniquement à titre d'information.*

[DUTCH TEXT – TEXTE NÉERLANDAIS]

OVEREENKOMST
TUSSEN
HET KONINKRIJK BELGIË
EN
HONGARIJE
INZAKE
DE UITWISSELING EN WEDERZIJDE BESCHERMING
VAN GECLASSIFICEERDE INFORMATIE

**OVEREENKOMST
TUSSEN
HET KONINKRIJK BELGIË
EN
HONGARIJE
INZAKE
DE UITWISSELING EN WEDERZIJDSE BESCHERMING
VAN GECLASSIFICEERDE INFORMATIE**

HET KONINKRIJK BELGIË

EN

HONGARIJE,

hierna te noemen “de Partijen”,

WENSEN de bescherming te verzekeren van Geclassificeerde Informatie die tussen de Partijen of tussen rechtspersonen of natuurlijke personen onder hun bevoegdheid overeenkomstig hun wetgeving wordt uitgewisseld of gezamenlijk door hen wordt opgesteld, en zijn, met wederzijds respect voor de nationale belangen en de veiligheid, het volgende overeengekomen:

ARTIKEL 1 DOEL VAN DEZE OVEREENKOMST

1. Deze Overeenkomst heeft als doel de bescherming te verzekeren van Geclassificeerde Informatie die wordt uitgewisseld of door samenwerking tussen de Partijen of tussen rechtspersonen of natuurlijke personen onder hun bevoegdheid wordt opgesteld.
2. Deze Overeenkomst is van toepassing op alle contracten of overeenkomsten en op elke andere vorm van samenwerking tussen de Partijen of tussen rechtspersonen of natuurlijke personen onder hun bevoegdheid die betrekking hebben op Geclassificeerde Informatie.

ARTIKEL 2 BEGRIPOMSCHRIJVINGEN

Voor de toepassing van deze Overeenkomst, dient te worden verstaan onder:

“Inbreuk op de beschermingsmaatregelen”: een handeling of een nalatigheid door een persoon, die strijdig is met deze Overeenkomst of met de nationale wet- en regelgeving van de Partijen en die aanleiding geeft tot ongeoorloofde openbaarmaking of tot elke andere ongeoorloofde manipulatie van Geclassificeerde Informatie.

“Geclassificeerde Informatie”: alle informatie die, ongeacht de vorm, overeenkomstig de nationale wet- en regelgeving van elke Partij, moet worden beschermd tegen ongeoorloofde openbaarmaking of tegen elke andere ongeoorloofde manipulatie, en die als dusdanig werd aangeduid overeenkomstig het bepaalde in Artikel 4 en Artikel 6 van deze Overeenkomst.

“Geclassificeerd Contract”: een overeenkomst die Geclassificeerde Informatie bevat of die voorziet in de toegang tot Geclassificeerde Informatie.

“Contractant”: een natuurlijke persoon of een rechtspersoon die de rechtsbevoegdheid heeft om overeenkomsten te sluiten.

“Veiligheidsmachtiging voor een vestiging”: een gunstige beslissing van de Nationale Veiligheidsoverheid waardoor, in overeenstemming met de respectieve nationale wet- en regelgevingen, een vestiging uit veiligheidsoogpunt de vereiste fysieke en organisatorische capaciteit heeft om Geclassificeerde Informatie te verwerken.

“Need-to-know”: de beslissing, in overeenstemming met de nationale wet- en regelgeving van de Partijen, dat voor een natuurlijke persoon of een rechtspersoon de toegang vereist is tot Geclassificeerde Informatie met het oog op het uitvoeren van officiële taken of diensten.

“Verstreckende Partij”: de Partij, met inbegrip van natuurlijke personen of rechtspersonen onder haar bevoegdheid, die Geclassificeerde Informatie verstrekt.

“Persoonlijke Veiligheidsmachtiging”: een gunstige beslissing van de Nationale Veiligheidsoverheid die volgt op een veiligheidsonderzoek waardoor, in overeenstemming met de respectieve nationale wet- en regelgevingen, een natuurlijke persoon toegang kan worden verleend tot Geclassificeerde Informatie.

“Ontvangende Partij”: de Partij, met inbegrip van natuurlijke personen of rechtspersonen onder haar bevoegdheid, die Geclassificeerde Informatie ontvangt.

“Derde Partij”: elke staat, met inbegrip van natuurlijke personen of rechtspersonen onder zijn bevoegdheid, of elke internationale organisatie die geen partij is bij deze Overeenkomst.

ARTIKEL 3 NATIONALE VEILIGHEIDSOVERHEDEN

1. De Nationale Veiligheidsoverheden die bevoegd zijn voor de bescherming van Geclassificeerde Informatie en voor de tenuitvoerlegging van en het toezicht op deze Overeenkomst, zijn:

In het Koninkrijk België:

Nationale Veiligheidsoverheid – Autorité nationale de Sécurité

In Hongarije:

Nemzeti Biztonsági Felügyelet

2. De Nationale Veiligheidsoverheden stellen elkaar in kennis van hun officiële contactgegevens en van elke verdere wijziging met betrekking tot deze contactgegevens.
3. Met het oog op de effectieve toepassing van deze Overeenkomst en binnen hun bevoegdheden overeenkomstig hun nationale wet- en regelgeving, kunnen de Nationale Veiligheidsoverheden, zo nodig, schriftelijk meer gedetailleerde administratieve regelingen overeenkomen.

ARTIKEL 4 CLASSIFICATIEGRADEN

1. De volgende classificatiegraden zijn gelijkwaardig:

Voor het Koninkrijk België		Voor Hongarije
IN HET NEDERLANDS	IN HET FRANS	
ZEER GEHEIM (Wet van 11/12/1998)	TRES SECRET (Loi du 11/12/1998)	„Szigorúan titkos!”
GEHEIM (Wet van 11/12/1998)	SECRET (Loi du 11/12/1998)	„Titkos!”
VERTROUWELIJK (Wet van 11/12/1998)	CONFIDENTIEL (Loi du 11/12/1998)	„Bizalmas!”
(zie hieronder)	(zie hieronder)	„Korlátozott terjesztésű!”

2. Het Koninkrijk België zal in overeenstemming met zijn nationale wet- en regelgeving inzake beschermde maar niet-geclassificeerde informatie, alle passende maatregelen nemen om de informatie met vermelding „Korlátozott terjesztésű!” die door Hongarije werd verstrekt, te behandelen en te beschermen, zoals geldt voor informatie gemarkeerd met “BEPERKTE VERSPREIDING/DIFFUSION RESTREINTE”.
3. Hongarije zal alle passende maatregelen nemen om de informatie met markering “BEPERKTE VERSPREIDING/DIFFUSION RESTREINTE” door het Koninkrijk België verstrekt, te behandelen en te beschermen in overeenstemming met zijn nationale wetten en regels die gelden voor de bescherming van informatie met vermelding „Korlátozott terjesztésű!”.

ARTIKEL 5

TOEGANG TOT GECLASSIFICEERDE INFORMATIE

1. De toegang tot informatie met vermelding “BEPERKTE VERSPREIDING/DIFFUSION RESTREINTE” en tot Geclassificeerde Informatie met vermelding “Korlátozott terjesztésű!” wordt uitsluitend verleend aan personen op basis van een Need-to-know, die de passende machtiging hebben verkregen in overeenstemming met de nationale wet- en regelgeving van de Ontvangende Partij.
2. De toegang tot Geclassificeerde Informatie met classificatiegraad VERTROUWELIJK (Wet van 11/12/1998) / CONFIDENTIEL (Loi du 11/12/1998) / „Bizalmas!” of hoger wordt uitsluitend verleend aan personen op basis van een Need-to-know en een geldige Persoonlijke Veiligheidsmachtiging of aan personen die anderszins naar behoren zijn gemachtigd, in overeenstemming met de nationale wet- en regelgeving van de Ontvangende Partij.
3. Elke Partij zorgt ervoor dat alle personen, die toegang hebben verkregen tot Geclassificeerde Informatie volgens lid 1 en 2 van dit Artikel, in kennis worden gesteld van hun verantwoordelijkheden inzake de bescherming van Geclassificeerde Informatie in overeenstemming met de geldende nationale wet- en regelgeving.

ARTIKEL 6

BEGINSELEN VOOR DE BEVEILIGING VAN GECLASSIFICEERDE INFORMATIE

1. De Verstreckende Partij:
 - a) zorgt ervoor dat Geclassificeerde Informatie voorzien is van de passende classificatiegraad, in overeenstemming met haar nationale wet- en regelgeving;
 - b) informeert de Ontvangende Partij over de voorwaarden voor het gebruik van Geclassificeerde Informatie;
 - c) stelt de Ontvangende Partij onverwijld in kennis van wijzigingen aangaande het classificeren of declassificeren van informatie.

2. De Ontvangende Partij:

- a) zorgt ervoor dat Geclassificeerde Informatie voorzien is van de overeenkomstige classificatiegraad, in overeenstemming met Artikel 4;
- b) biedt dezelfde mate van bescherming aan Geclassificeerde Informatie zoals geboden wordt aan haar nationaal Geclassificeerde Informatie van het overeenkomstige classificatieniveau;
- c) zorgt ervoor dat Geclassificeerde Informatie niet gedeclassificeerd wordt en dat de classificatie niet gewijzigd wordt zonder de voorafgaande schriftelijke toestemming van de Verstreckende Partij;
- d) zorgt ervoor dat Geclassificeerde Informatie niet aan een Derde Partij wordt vrijgegeven zonder de voorafgaande schriftelijke toestemming van de Verstreckende Partij;
- e) gebruikt Geclassificeerde Informatie uitsluitend voor het doel waarvoor deze bestemd is, in overeenstemming met de gebruiksvoorwaarden van de Verstreckende Partij.

ARTIKEL 7

SAMENWERKING INZAKE BEVEILIGING

- 1. Teneinde vergelijkbare beveiligingsniveaus te behouden, verstrekken de Nationale Veiligheidsoverheden elkaar op verzoek, de informatie over de nationale wet- en regelgeving inzake de bescherming van Geclassificeerde Informatie en over de praktijken die uit de tenuitvoerlegging ervan voortvloeien. De Nationale Veiligheidsoverheden stellen elkaar in kennis van elke substantiële wijziging van hun nationale wet- en regelgeving inzake de bescherming van Geclassificeerde Informatie.
- 2. De Nationale Veiligheidsoverheden verlenen elkaar, op verzoek ervan en overeenkomstig met hun nationale wet- en regelgeving, bijstand tijdens de procedures inzake de Persoonlijke Veiligheidsmachtiging of inzake de Veiligheidsmachtiging voor een Vestiging.
- 3. De Partijen erkennen op verzoek, de Persoonlijke Veiligheidsmachtigingen en de Veiligheidsmachtigingen voor een Vestiging overeenkomstig de nationale wet- en regelgeving volgens de toepassing van Artikel 4 van deze Overeenkomst.
- 4. Binnen het toepassingsgebied van deze Overeenkomst brengen de Nationale Veiligheidsoverheden elkaar onverwijld op de hoogte van wijzigingen in erkende Persoonlijke Veiligheidsmachtigingen en Veiligheidsmachtigingen voor een Vestiging, in het bijzonder bij de intrekking of de beëindiging ervan.

ARTIKEL 8
INDUSTRIËLE BEVEILIGINGSMATREGELEN

1. Geclassificeerde Contracten worden gepubliceerd, afgesloten en uitgevoerd overeenkomstig de respectieve nationale wet- en regelgevingen. Op verzoek bevestigen de Nationale Veiligheidsoverheden dat de voorgestelde contractant die deelneemt aan de precontractuele onderhandelingen of aan de uitvoering van Geclassificeerde Contracten houder is van de vereiste Veiligheidsmachtiging.
2. De Contractant moet, overeenkomstig de geldende wet- en regelgeving:
 - a) beschikken over de vereiste Veiligheidsmachtiging voor een Vestiging, zoals bepaald in Artikel 4;
 - b) ervoor zorgen dat personen die wensen toegang te verkrijgen tot Geclassificeerde Informatie over de vereiste Persoonlijke Veiligheidsmachtiging beschikken, zoals bepaald in de Artikelen 4 en 5;
 - c) ervoor zorgen dat alle personen die toegang hebben tot Geclassificeerde Informatie in kennis worden gesteld van hun verantwoordelijkheden inzake de bescherming van Geclassificeerde Informatie.
3. Alle onderaannemers zijn gebonden door dezelfde veiligheidsvoorschriften als de Contractant.
4. De Nationale Veiligheidsoverheden brengen elkaar op de hoogte van de classificatiegraad die tijdens de precontractuele onderhandelingen werd verstrekt met het oog op het sluiten van een Geclassificeerd Contract.
5. Alle Geclassificeerde Contracten die onder deze Overeenkomst worden gesloten, bevatten een geldige veiligheidsclausule met:
 - a) een programmabeveiligingsinstructie en classificatiegids;
 - b) een procedure voor het meedelen van wijzigingen in de classificatiegraad van de informatie;
 - c) communicatiekanalen;
 - d) procedures voor de overdracht van Geclassificeerde Informatie;
 - e) contactgegevens van de Nationale Veiligheidsoverheid die belast is met de coördinatie van de bescherming van Geclassificeerde Informatie;
 - f) de verplichting om elke werkelijke of vermoedelijke inbreuk op de beschermingsmaatregelen bekend te maken. Elke inbreuk moet worden gemeld aan de Nationale Veiligheidsoverheid van de betreffende Partij.
6. Een kopie van de veiligheidsclausule van alle Geclassificeerde Contracten wordt gestuurd naar de Nationale Veiligheidsoverheid van de Partij waar het Geclassificeerd Contract zal worden uitgevoerd, om voldoende controle en toezicht te garanderen op de beveiligingsnormen, de procedures en de werkwijzen die de Contractanten hebben vastgelegd met het oog op de bescherming van Geclassificeerde Informatie.

7. De Nationale Veiligheidsoverheden kunnen elkaar verzoeken een analyse te maken van de doeltreffendheid van de maatregelen die door de Contractant werden goedgekeurd met het oog op de bescherming van de Geclassificeerde Informatie verbonden aan een Geclassificeerd Contract.

ARTIKEL 9

VERZENDING VAN GECLASSIFICEERDE INFORMATIE

1. Geclassificeerde Informatie wordt overeenkomstig de nationale wet- en regelgeving van de Verstreckende Partij langs diplomatieke weg of via andere middelen verzonden, zoals bepaald door de Nationale Veiligheidsoverheden.
2. De Partijen kunnen Geclassificeerde Informatie via elektronische weg verzenden overeenkomstig de beveiligingsprocedures die door de Nationale Veiligheidsoverheden werden goedgekeurd.

ARTIKEL 10

KOPIËREN, VERTALEN EN VERNIETIGEN VAN GECLASSIFICEERDE INFORMATIE

1. Op alle reproducties en vertalingen van Geclassificeerde Informatie wordt de passende classificatiegraad vermeld. Ze worden op dezelfde manier beschermd als de originele Geclassificeerde Informatie. Het aantal reproducties wordt tot een minimum beperkt.
2. Vertalingen zijn in de taal van de vertaling voorzien van de vermelding dat ze Geclassificeerde Informatie van de Verstreckende Partij bevatten.
3. Geclassificeerde Informatie met de vermelding ZEER GEHEIM (WET VAN 11/12/1998) / TRES SECRET (LOI DU 11/12/1998) / „Szigorúan titkos!” wordt uitsluitend met de voorafgaande schriftelijke toestemming van de Verstreckende Partij vertaald of gereproduceerd.
4. Geclassificeerde Informatie met de vermelding ZEER GEHEIM (WET VAN 11/12/1998) / TRES SECRET (LOI DU 11/12/1998) / „Szigorúan titkos!” wordt niet vernietigd en wordt teruggestuurd naar de Verstreckende Partij.
5. In geval van een crisissituatie, wanneer het onmogelijk is Geclassificeerde Informatie die overeenkomstig deze Overeenkomst werd opgesteld of vrijgegeven, in overeenstemming met haar classificatiegraad te beschermen, of wanneer het onmogelijk is deze terug te sturen, wordt de Geclassificeerde Informatie onmiddellijk vernietigd. De Nationale Veiligheidsoverheid van de Ontvangende Partij stelt de Nationale Veiligheidsoverheid van de Verstreckende Partij onverwijld in kennis van de vernietiging van de Geclassificeerde Informatie.

ARTIKEL 11 BEZOEKEN

1. Bezoeken met toegang tot Geclassificeerde Informatie vereisen de voorafgaande schriftelijke goedkeuring van de betreffende Nationale Veiligheidsoverheid, tenzij anders overeengekomen tussen de Nationale Veiligheidsoverheden.
2. De bezoeker dient zijn bezoekaanvraag minstens twintig dagen vóór het geplande bezoek in bij zijn Nationale Veiligheidsoverheid, die deze doorstuurt naar de Nationale Veiligheidsoverheid van de andere Partij. In dringende gevallen kan de bezoekaanvraag op kortere termijn worden ingediend, mits er vooraf coördinatie plaatsvindt tussen de Nationale Veiligheidsoverheden.
3. De bezoekaanvraag vermeldt:
 - a) voornaam en familienaam van de bezoeker, geboortedatum en geboorteplaats, nationaliteit en nummer van het paspoort/de identiteitskaart;
 - b) functie van de bezoeker en naam van de organisatie die hij vertegenwoordigt;
 - c) niveau van de veiligheidsmachtiging van de bezoeker en geldigheid;
 - d) datum en duur van het bezoek en, in geval van meerdere bezoeken, de totale tijdsduur;
 - e) doel van het bezoek en de hoogste classificatiegraad waarop het bezoek betrekking heeft;
 - f) naam en adres van de te bezoeken vestiging en naam, telefoon-/faxnummer en e-mailadres van de contactpersoon;
 - g) datum, handtekening en officiële stempel van de Nationale Veiligheidsoverheid.
4. De Nationale Veiligheidsoverheden kunnen overeenkomen een lijst op te maken van de bezoekers die gemachtigd zijn om meerdere bezoeken af te leggen. Ze leggen in onderling overleg de voorwaarden voor de volgende bezoeken vast.
5. Geclassificeerde Informatie die door een bezoeker wordt verworven, wordt beschouwd als Geclassificeerde Informatie die in het kader van deze Overeenkomst wordt verstrekt.

ARTIKEL 12 INBREUK OP DE BESCHERMINGSMAATREGELEN

1. De Nationale Veiligheidsoverheden brengen elkaar onverwijld schriftelijk op de hoogte van een inbreuk op de beschermingsmaatregelen dan wel van een vermoeden van inbreuk, die zou kunnen leiden tot ongeoorloofde openbaarmaking of tot een andere ongeoorloofde manipulatie van Geclassificeerde Informatie.

2. De bevoegde overheden van de Ontvangende Partij stellen onverwijld het nodige onderzoek in. Indien nodig werken de bevoegde overheden van de Verstreckende Partij mee aan het onderzoek.
3. De Ontvangende Partij stelt de Verstreckende Partij in elk geval schriftelijk in kennis van de omstandigheden van de inbreuk op de beschermingsmaatregelen, van de omvang van de veroorzaakte schade, van de genomen maatregelen ter beperking van de schade, en van de resultaten van het onderzoek.

ARTIKEL 13

KOSTEN

De Partijen dragen zelf de kosten die ze hebben gemaakt met het oog op de tenuitvoerlegging van deze Overeenkomst.

ARTIKEL 14

INTERPRETATIE EN GESCHILLEN

Elk geschil betreffende de toepassing van deze Overeenkomst wordt buitengerechtelijk beslecht via overleg tussen de Partijen.

ARTIKEL 15

SLOTBEPALINGEN

1. Deze Overeenkomst wordt voor onbepaalde tijd gesloten. Deze Overeenkomst treedt in werking op de eerste dag van de tweede maand na datum van ontvangst van de laatste kennisgeving langs diplomatieke weg waarbij de Partijen aan elkaar mededelen dat aan alle interne wettelijke voorwaarden voor haar inwerkingtreding is voldaan.
2. Deze Overeenkomst kan met onderlinge schriftelijke toestemming van de Partijen worden gewijzigd. De wijzigingen treden in werking zoals bepaald in lid 1 van dit Artikel.
3. Elke Partij kan deze Overeenkomst te allen tijde schriftelijk opzeggen. In dat geval vervalt de geldigheid van de Overeenkomst zes maand na de datum waarop de andere Partij de schriftelijke kennisgeving van opzegging heeft ontvangen.

4. Niettegenstaande de opzegging van deze Overeenkomst blijven de Partijen verplicht de Geclassificeerde Informatie die binnen het bestek van deze Overeenkomst werd vrijgegeven of opgesteld, overeenkomstig de bepalingen van deze Overeenkomst te beschermen, tot wanneer de Verstreckende Partij beslist deze verplichting op te heven.

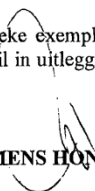
TEN BLIJKE WAARVAN, de vertegenwoordigers van beide Partijen, daartoe naar behoren gemachtigd, deze Overeenkomst hebben ondertekend.

GEDAAN te Boedapest op 21 september 2015, in twee authentieke exemplaren in de Franse, de Nederlandse, de Hongaarse en de Engelse taal. In geval van verschil in uitlegging is de Engelse tekst doorslaggevend.

NAMENS HET KONINKRIJK BELGIË:



NAMENS HONGARIJE:





[ENGLISH TEXT – TEXTE ANGLAIS]

AGREEMENT
BETWEEN
THE KINGDOM OF BELGIUM
AND
HUNGARY
ON
THE EXCHANGE AND MUTUAL PROTECTION
OF CLASSIFIED INFORMATION

**AGREEMENT
BETWEEN
THE KINGDOM OF BELGIUM
AND
HUNGARY
ON
THE EXCHANGE AND MUTUAL PROTECTION
OF CLASSIFIED INFORMATION**

THE KINGDOM OF BELGIUM

AND

HUNGARY,

hereinafter referred to as “the Parties”,

WISHING to ensure the protection of Classified Information exchanged or generated between them or between legal entities or individuals under their jurisdiction have, in mutual respect for national interests and security, agreed upon the following:

ARTICLE 1
SCOPE OF THE AGREEMENT

1. The objective of this Agreement is to ensure the protection of Classified Information exchanged or generated in the course of co-operation between the Parties or between legal entities or individuals under their jurisdiction.
2. This Agreement shall be applied to any contract or agreement as well as any other co-operation between the Parties or between legal entities or individuals under their jurisdiction involving Classified Information.

ARTICLE 2
DEFINITIONS

For the purpose of this Agreement:

“Breach of Security” means an act or an omission by an individual which is contrary to this Agreement or the respective national laws and regulations of the Parties and which results in unauthorised disclosure or any other unauthorised manipulation of Classified Information.

“Classified Information” means any information that, regardless of its form, under the national laws and regulations of either Party, requires protection against unauthorised disclosure, or any other unauthorised manipulation, and has been designated as such in accordance with the provisions of Article 4 and 6 of this Agreement.

“Classified Contract” means a contract that contains or involves access to Classified Information.

“Contractor” means an individual or a legal entity possessing the legal capacity to conclude contracts.

“Facility Security Clearance” means the positive determination by the National Security Authority that, from a security point of view, a facility has the physical and organisational capability to handle Classified Information, in accordance with the respective national laws and regulations.

“Need-to-know” means a determination, in respect with the national laws and regulations of the Parties, that an individual or a legal entity has a requirement to access Classified Information in order to perform official tasks or services.

“Originating Party” means the Party including legal entities or individuals under its jurisdiction, which releases Classified Information.

“Personnel Security Clearance” means the positive determination, stemming from a vetting procedure, by the National Security Authority that an individual is eligible to have access to Classified Information, in accordance with the respective national laws and regulations.

“Recipient Party” means the Party including legal entities or individuals under its jurisdiction, which receives Classified Information.

“Third Party” means any state including legal entities or individuals under its jurisdiction or international organisation not being a party to this Agreement.

ARTICLE 3 NATIONAL SECURITY AUTHORITIES

1. The National Security Authorities responsible for the protection of Classified Information as well as the implementation and supervision of this Agreement are:

In the Kingdom of Belgium:

Nationale Veiligheidszoverheid – Autorité nationale de Sécurité (National Security Authority)

In Hungary:

Nemzeti Biztonsági Felügyelet (National Security Authority)

2. The National Security Authorities shall provide each other with official contact details and shall inform each other of any subsequent changes thereof.
3. In order to ensure the effective implementation of this Agreement, the National Security Authorities may, in the scope of their competences according to their national laws and regulations, conclude, if necessary, written detailed administrative arrangements.

ARTICLE 4 SECURITY CLASSIFICATION LEVELS

1. The equivalence of security classification levels is as follows:

In the Kingdom of Belgium		In Hungary
IN DUTCH LANGUAGE	IN FRENCH LANGUAGE	
ZEER GEHEIM (Wet van 11/12/1998)	TRES SECRET (Loi du 11/12/1998)	„Szigorúan titkos!”
GEHEIM (Wet van 11/12/1998)	SECRET (Loi du 11/12/1998)	„Titkos!”
VERTROUWELIJK (Wet van 11/12/1998)	CONFIDENTIEL (Loi du 11/12/1998)	„Bizalmas!”
(see note hereunder)	(see note hereunder)	„Korlátozott terjesztésű!”

2. The Kingdom of Belgium shall process and protect information marked „Korlátozott terjesztésű!” transferred by Hungary according to its respective national laws and regulations relating to protected but non-classified information, such as “BEPERKTE VERSPREIDING/DIFFUSION RESTREINTE”.
3. Hungary shall process and protect non-classified information but marked as being protected, such as “BEPERKTE VERSPREIDING/DIFFUSION RESTREINTE” transferred by the Kingdom of Belgium according to its respective national laws and regulations relating to the protection of „Korlátozott terjesztésű!”.

ARTICLE 5 ACCESS TO CLASSIFIED INFORMATION

1. Access to information marked “BEPERKTE VERSPREIDING/DIFFUSION RESTREINTE” and Classified Information marked “Korlátozott terjesztésű!” is restricted to individuals who have a Need-to-know and have been properly authorised in accordance with the national laws and regulations of the Recipient Party.
2. Access to Classified Information VERTROUWELIJK (Wet van 11/12/1998) / CONFIDENTIEL (Loi du 11/12/1998) / „Bizalmas!” or above is restricted to individuals who have a Need-to-know and hold a Personnel Security Clearance to the appropriate level or are otherwise duly authorised in accordance with the national laws and regulations of the Recipient Party.
3. Each Party shall ensure that all individuals, granted access to information according to paragraph 1 and 2 of this Article, are informed of their responsibilities to protect such information in accordance with the appropriate national laws and regulations.

ARTICLE 6 PRINCIPLES FOR THE PROTECTION OF CLASSIFIED INFORMATION

1. The Originating Party shall:
 - a) ensure that Classified Information is marked with appropriate security classification markings in accordance with its national laws and regulations;
 - b) inform the Recipient Party of any use conditions of Classified Information;
 - c) inform the Recipient Party without undue delay of any subsequent changes in classification or declassification.
2. The Recipient Party shall:
 - a) ensure that Classified Information is marked with equivalent security classification level in accordance with Article 4;
 - b) afford the same degree of protection to Classified Information as afforded to its national Classified Information of equivalent security classification level;

- c) ensure that Classified Information is not declassified nor its classification changed without the prior written consent of the Originating Party;
- d) ensure that Classified Information is not released to a Third Party without the prior written consent of the Originating Party;
- e) use Classified Information only for the purpose it has been released for and in accordance with use conditions of the Originating Party.

ARTICLE 7 SECURITY CO-OPERATION

1. In order to maintain comparable standards of security, the National Security Authorities shall, on request, inform each other of the national laws and regulations concerning protection of Classified Information and the practices stemming from their implementation. The National Security Authorities shall inform each other of any substantive change of their national laws and regulations concerning the protection of Classified Information.
2. On request, the National Security Authorities shall, in accordance with the national laws and regulations, assist each other during the Personnel Security Clearance procedures and Facility Security Clearance procedures.
3. The Parties shall recognise, on request, their Personnel Security Clearances and Facility Security Clearances in accordance with the national laws and regulations. Article 4 of this Agreement shall apply accordingly.
4. Within the scope of this Agreement, the National Security Authorities shall promptly notify each other about changes in recognised Personnel Security Clearances and Facility Security Clearances, especially in cases of their revocation or termination.

ARTICLE 8 INDUSTRIAL SECURITY MEASURES

1. Classified Contracts shall be published, concluded and implemented in accordance with the respective national laws and regulations. On request, the National Security Authorities shall confirm that the proposed Contractor participating in the pre-contractual negotiations or in the implementation of Classified Contracts holds an appropriate Security Clearance.
2. The Contractor shall, in accordance with its respective laws and regulations, be obliged to:
 - a) Hold an appropriate Facility Security Clearance in accordance with Article 4;
 - b) Ensure that the individuals requiring access to Classified Information hold the appropriate Personnel Security Clearance in accordance with Article 4 and 5;
 - c) Ensure that all individuals granted access to Classified Information are informed of their responsibilities to protect Classified Information.

3. All subcontractors shall fulfill the same security obligations as the Contractor.
4. The National Security Authorities shall inform each other of the classification level provided to the pre-contractual negotiations in order to conclude Classified Contract.
5. Every Classified Contract concluded in accordance with this Agreement shall include an appropriate security section identifying the following aspects:
 - a) A program security instruction and classification guide;
 - b) A procedure for notifying the changes in the classification level of the information;
 - c) Communication channels;
 - d) Procedures for the transportation of Classified Information;
 - e) Contact details of the National Security Authorities responsible for the co-ordination of the protection of Classified Information related to the Contract;
 - f) An obligation to notify any actual or suspected Breach of Security to the appropriate authorities of the respective Parties. The National Security Authority of the respective Party shall always be informed of any Breach of Security.
6. A copy of the security section of all Classified Contracts shall be forwarded to the National Security Authority of the Party where the Classified Contract is to be performed, to allow an adequate supervision and control of the security standards, procedures and practices established by the Contractors for the protection of Classified Information.
7. The National Security Authorities may request each other to analyse the efficiency of the measures adopted by a Contractor for the protection of the Classified Information involved in a Classified Contract.

ARTICLE 9

TRANSMISSION OF CLASSIFIED INFORMATION

1. Classified Information shall be transmitted in accordance with the national laws and regulations of the Originating Party through diplomatic channels or as otherwise agreed between the National Security Authorities.
2. The Parties may transmit Classified Information by electronic means in accordance with the security procedures approved by the National Security Authorities.

ARTICLE 10
REPRODUCTION, TRANSLATION AND DESTRUCTION
OF CLASSIFIED INFORMATION

1. Reproductions and translations of Classified Information shall bear appropriate security classification markings and shall be protected in the same way as the original Classified Information. Number of reproductions shall be limited to the minimum needed.
2. Translations shall bear a note in the language of translation indicating that they contain Classified Information of the Originating Party.
3. Classified Information marked as ZEER GEHEIM (WET VAN 11/12/1998) / TRES SECRET (LOI DU 11/12/1998) / „Szigorúan titkos!” shall be translated or reproduced only upon the prior written consent of the Originating Party.
4. Classified Information marked as ZEER GEHEIM (WET VAN 11/12/1998) / TRES SECRET (LOI DU 11/12/1998) / „Szigorúan titkos!” shall not be destroyed and shall be returned to the Originating Party.
5. In case of any crisis situation, which makes it impossible to protect the Classified Information, generated or released in accordance with this Agreement, according to its classification, or if it is impossible to return, the Classified Information shall be destroyed immediately. The National Security Authority of the Recipient Party shall notify the National Security Authority of the Originating Party about the destruction of the Classified Information as soon as possible.

ARTICLE 11
VISITS

1. Visits requiring access to Classified Information are subject to the prior written consent of the respective National Security Authority, unless otherwise agreed between the National Security Authorities.
2. The visitor shall submit the request for visit at least twenty days in advance of the starting date of the visit to his National Security Authority, which shall forward it to the National Security Authority of the other Party. In urgent cases, the request for visit may be submitted at a shorter notice, subject to prior co-ordination between the National Security Authorities.
3. Request for visit shall include
 - a) first and last name of the visitor, date and place of birth, nationality and passport/ID card number;
 - b) position of the visitor and specification of the facility, which the visitor represents;
 - c) visitor's Personnel Security Clearance status and its validity;
 - d) date and duration of the visit, in case of recurring visit the total period of time covered by the visits shall be stated;

- e) purpose of the visit including the highest level of Classified Information to be involved;
 - f) name, address of the facility to be visited, as well as the name, phone/fax number and e-mail of its point of contact;
 - g) date, signature and stamping of the official seal of the National Security Authority.
- 4. The National Security Authorities may agree on a list of visitors entitled to recurring visit. The National Security Authorities shall agree on the further details of the recurring visit.
 - 5. Classified Information acquired by a visitor shall be considered as Classified Information released under this Agreement.

ARTICLE 12 BREACHES OF SECURITY

- 1. The National Security Authorities shall immediately inform each other in writing of a Breach of Security or suspicion of such a breach which could result in an unauthorized disclosure or any unauthorized manipulation of Classified Information.
- 2. The competent authorities of the Recipient Party shall investigate the incident without undue delay. The competent authorities of the Originating Party shall, if required, co-operate in the investigation.
- 3. In any case, the Recipient Party shall inform the Originating Party in writing about the circumstances of the Breach of Security, the extent of the damage, the measures adopted for its mitigation and the outcome of the investigation.

ARTICLE 13 EXPENSES

The Parties shall bear their own expenses incurred in the course of the implementation of this Agreement.

ARTICLE 14 INTERPRETATION AND DISPUTES

Any dispute regarding the interpretation or application of this Agreement shall be settled by negotiation between the Parties, without recourse to outside jurisdiction.

**ARTICLE 15
FINAL PROVISIONS**

1. This Agreement is concluded for an indefinite period of time. This Agreement shall enter into force on the first day of the second month following the date of receipt of the last of notifications between the Parties, through diplomatic channels, stating that the internal legal procedures for this Agreement to enter into force have been fulfilled.
2. This Agreement may be amended on the basis of the mutual consent of the Parties. Such amendments shall enter into force in accordance with paragraph 1 of this Article.
3. Each Party is entitled to terminate this Agreement in writing at any time. In such a case, the validity of this Agreement shall expire after six months following the day on which the other Party receives the written notice of the termination.
4. Regardless of the termination of this Agreement, all Classified Information released or generated under this Agreement shall be protected in accordance with the provisions set forth herein until the Originating Party dispenses the Recipient Party from this obligation.

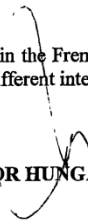
IN WITNESS OF WHICH, the undersigned, duly authorised to this effect, have signed this Agreement.

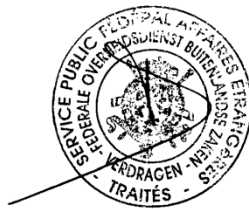
DONE at Budapest on the 21st of September 2015, in two originals, in the French, Dutch, Hungarian and English languages, each text being equally authentic. In case of different interpretation the English text shall prevail.

FOR THE KINGDOM OF BELGIUM:



FOR HUNGARY:





[FRENCH TEXT – TEXTE FRANÇAIS]

ACCORD
ENTRE
LE ROYAUME DE BELGIQUE
ET
LA HONGRIE
SUR
L'ÉCHANGE ET LA PROTECTION MUTUELLE
DES INFORMATIONS CLASSIFIÉES

**ACCORD
ENTRE
LE ROYAUME DE BELGIQUE
ET
LA HONGRIE
SUR
L'ECHANGE ET LA PROTECTION MUTUELLE
DES INFORMATIONS CLASSIFIEES**

LE ROYAUME DE BELGIQUE

ET

LA HONGRIE,

ci-après dénommés “les Parties”,

DÉSIREUX de garantir la protection des Informations Classifiées échangées entre les Parties ou entre des personnes morales ou des personnes physiques qui relèvent de leur juridiction, ou produites par elles, sont convenus de ce qui suit, dans le respect mutuel de la sécurité et des intérêts nationaux:

ARTICLE 1 CHAMP D'APPLICATION DE L'ACCORD

1. Le présent Accord a pour objectif de garantir la protection des Informations Classifiées échangées entre les Parties ou entre des personnes morales ou des personnes physiques qui relèvent de leur juridiction, ou produites par elles dans le cadre de leur coopération.
2. Le présent Accord s'applique à tout contrat ou accord ainsi qu'à tout autre type de coopération entre les Parties ou entre des personnes morales ou des personnes physiques qui relèvent de leur juridiction dès lors qu'ils concernent des Informations Classifiées.

ARTICLE 2 DÉFINITIONS

Pour l'application du présent Accord:

Le terme « **Infraction à la Sécurité** » désigne une action ou une omission par une personne physique, contraire au présent Accord ou aux lois et réglementations nationales respectives des Parties et qui entraîne la divulgation non autorisée ou toute autre manipulation non autorisée d'Informations Classifiées.

Le terme « **Informations Classifiées** » désigne toute information, quelle qu'en soit la forme, qui, conformément aux lois et réglementations nationales de chacune des Parties, requiert une protection contre la divulgation non autorisée ou toute autre manipulation non autorisée, et a été qualifiée comme telle en vertu des dispositions des Articles 4 et 6 du présent Accord.

Le terme « **Contrat Classifié** » désigne un contrat qui contient ou implique l'accès à des Informations Classifiées.

Le terme « **Contractant** » désigne une personne physique ou une personne morale disposant de la capacité juridique de conclure des contrats.

Le terme « **Habilitation de Sécurité d'établissement** » désigne la décision favorable prise par l'Autorité Nationale de Sécurité selon lequel, du point de vue de la sécurité, un établissement a la capacité physique et organisationnelle de traiter des Informations Classifiées, conformément aux lois et réglementations nationales respectives des Parties.

Le terme « **Besoin d'en Connaître** » désigne une décision, conformément aux lois et réglementations nationales des Parties, qui reconnaît qu'une personne physique ou une personne morale a la nécessité d'accéder à des Informations Classifiées afin d'exercer des fonctions ou de fournir des services à caractère officiel.

Le terme « **Partie d'Origine** » désigne la Partie, en ce compris les personnes physiques ou les personnes morales qui relèvent de sa juridiction, qui communique des informations classifiées.

Le terme « **Habilitation de Sécurité d'une personne** » désigne la décision favorable prise par l'Autorité Nationale de Sécurité après enquête de sécurité, qui permet à une personne physique d'avoir accès aux Informations Classifiées, conformément aux lois et réglementations nationales respectives des Parties.

Le terme “**Partie Destinataire**” désigne la Partie, en ce compris les personnes physiques ou les personnes morales qui relèvent de sa juridiction, qui reçoit les Informations Classifiées.

Le terme “**Tierce Partie**” désigne tout État, en ce compris les personnes physiques ou les personnes morales qui relèvent de sa juridiction, ou toute organisation internationale n’étant pas partie au présent Accord.

ARTICLE 3 AUTORITES NATIONALES DE SECURITE

1. Les Autorités Nationales de Sécurité chargées de la protection des Informations Classifiées ainsi que de la mise en œuvre et de la supervision du présent Accord sont:

Pour le Royaume de Belgique:

Autorité Nationale de Sécurité – Nationale Veiligheidsoverheid

Pour la Hongrie:

Nemzeti Biztonsági Felügyelet

2. Les Autorités Nationales de Sécurité se communiquent leurs informations de contact officielles et se notifient toute modification ultérieure.
3. Dans leur champ de compétence, conformément à leurs lois et réglementations nationales, les Autorités Nationales de Sécurité peuvent, si besoin est, arrêter par écrit des dispositions administratives détaillées afin de garantir la mise en œuvre effective du présent Accord.

ARTICLE 4 NIVEAUX DE CLASSIFICATION DE SECURITE

1. Les niveaux de classification de sécurité des deux Parties présentent les équivalences suivantes:

Pour le Royaume de Belgique		Pour la Hongrie
EN LANGUE FRANÇAISE	EN LANGE NEERLANDAISE	
TRES SECRET (Loi du 11/12/1998)	ZEER GEHEIM (Wet van 11/12/1998)	„Szigorúan titkos!”
SECRET (Loi du 11/12/1998)	GEHEIM (Wet van 11/12/1998)	„Titkos!”
CONFIDENTIEL (Loi du 11/12/1998)	VERTROUWELIJK (Wet van 11/12/1998)	„Bizalmas!”
(voir note infra)	(voir note infra)	„Korlátozott terjesztésű!”

2. Le Royaume de Belgique traite et protège les informations portant le marquage „Korlátozott terjesztésű!” transférées par la Hongrie comme il le fait pour les informations portant le marquage “DIFFUSION RESTREINTE/BEPERKTE VERSPREIDING”, conformément à ses lois et réglementations nationales relatives aux informations protégées mais non classifiées.
3. Les informations non classifiées mais portant le marquage “DIFFUSION RESTREINTE/BEPERKTE VERSPREIDING” indiquant qu’elles sont protégées, transférées par le Royaume de Belgique, sont traitées et protégées par la Hongrie conformément à ses lois et réglementations nationales relatives à la protection des informations portant le marquage „Korlátozott terjesztésű!”.

ARTICLE 5

ACCES AUX INFORMATIONS CLASSIFIEES

1. L'accès aux informations portant le marquage “DIFFUSION RESTREINTE/BEPERKTE VERSPREIDING” et aux Informations Classifiées portant le marquage „Korlátozott terjesztésű!” est limité aux personnes physiques qui ont le besoin d'en connaître et qui ont été dûment autorisées conformément aux lois et réglementations nationales de la Partie Destinataire.
2. L'accès aux Informations Classifiées du niveau CONFIDENTIEL (Loi du 11/12/1998) / VERTROUWELIJK (Wet van 11/12/1998) / „Bizalmas!” ou d'un niveau supérieur est limité aux personnes physiques qui ont le besoin d'en connaître et détiennent une Habilitation de Sécurité personnelle du niveau approprié ou qui ont été dûment autorisées de toute autre manière conformément aux lois et réglementations nationales de la Partie Destinataire.
3. Chaque Partie veille à ce que toutes les personnes physiques auxquelles est accordé l'accès aux informations en vertu des paragraphes 1 et 2 du présent Article soient informées de la responsabilité qui leur incombe de protéger ces informations conformément aux lois et réglementations nationales appropriées.

ARTICLE 6

PRINCIPES POUR LA PROTECTION DES INFORMATIONS CLASSIFIEES

1. La Partie d'Origine:
 - a) veille à ce que les Informations Classifiées portent les marquages de classification de sécurité appropriés conformément à ses lois et réglementations nationales;
 - b) informe la Partie Destinataire de toutes les conditions d'utilisation des Informations Classifiées;
 - c) informe la Partie Destinataire, sans retard injustifié, de toute modification ultérieure au niveau de la classification ou de la déclassification.

2. La Partie Destinataire:

- a) veille à ce que les Informations Classifiées portent un marquage de classification de sécurité équivalent, conformément aux dispositions de l'Article 4;
- b) accorde aux Informations Classifiées qui lui ont été communiquées le niveau de protection attribué à ses propres informations nationales classifiées ou un niveau de classification de sécurité équivalent;
- c) veille à ce que les Informations Classifiées ne soient pas déclassifiées ni leur classification modifiée sans le consentement préalable écrit de la Partie d'Origine;
- d) veille à ce que les Informations Classifiées ne soient pas divulguées à une Tierce Partie sans le consentement préalable écrit de la Partie d'Origine;
- e) utilise les Informations Classifiées uniquement aux fins pour lesquelles elles ont été communiquées et conformément aux conditions d'utilisation de la Partie d'Origine.

**ARTICLE 7
COOPERATION EN MATIERE DE SECURITE**

1. Afin de conserver des normes de sécurité comparables, les Autorités Nationales de Sécurité se tiennent, sur demande, mutuellement informées des lois et réglementations nationales en matière de protection des Informations Classifiées et des pratiques découlant de leur mise en œuvre. Les Autorités Nationales de Sécurité se tiennent mutuellement informées de toute modification fondamentale de leurs lois et réglementations nationales relatives à la protection des Informations Classifiées.
2. Sur demande, les Autorités Nationales de Sécurité se prêtent assistance, conformément à leurs lois et réglementations nationales, durant les procédures d'Habilitation de Sécurité individuelle et d'Habilitation de Sécurité d'installation.
3. Sur demande, les Parties reconnaissent mutuellement leurs Habilitations de Sécurité personnelles et d'installation délivrées conformément aux lois et réglementations nationales. L'Article 4 du présent Accord s'applique en conséquence.
4. Dans le cadre du présent Accord, les Autorités Nationales de Sécurité se notifient immédiatement tout changement relatif à une Habilitation de Sécurité personnelle ou d'installation reconnue, particulièrement en cas de révocation ou de dénonciation.

**ARTICLE 8
MESURES DE SECURITE INDUSTRIELLE**

1. Les Contrats Classifiés sont publiés, conclus et mis en œuvre conformément aux lois et réglementations nationales respectives des Parties. Sur demande, les Autorités Nationales de Sécurité confirment que le Contractant proposé qui participe aux négociations précontractuelles ou à la mise en œuvre des Contrats Classifiés possède une Habilitation de Sécurité du niveau approprié.

2. Conformément aux lois et réglementations applicables, le Contractant est tenu:
 - a) de posséder l'Habilitation de Sécurité d'installation appropriée conformément à l'article 4;
 - b) de garantir que les personnes physiques demandant l'accès à des Informations Classifiées possèdent le niveau d'Habilitation de Sécurité personnelle approprié conformément aux articles 4 et 5;
 - c) de garantir que toutes les personnes physiques ayant obtenu l'accès à des Informations Classifiées sont informées de leurs responsabilités en ce qui concerne la protection des Informations Classifiées.
3. Tous les sous-traitants doivent satisfaire aux mêmes obligations de sécurité que le Contractant.
4. Les Autorités Nationales de Sécurité se communiquent le niveau de classification de sécurité attribué aux négociations précontractuelles visant la conclusion d'un Contrat Classifié.
5. Tout Contrat Classifié conclu conformément aux dispositions du présent Accord comporte un chapitre approprié consacré à la sécurité couvrant les aspects suivants:
 - a) une instruction de sécurité relative au programme et un guide de classification de sécurité;
 - b) une procédure de communication des changements intervenus dans le niveau de classification des informations;
 - c) les canaux de communication;
 - d) les procédures de transport des Informations Classifiées;
 - e) les informations de contact des Autorités Nationales de Sécurité chargées de la coordination de la protection des Informations Classifiées liées au contrat;
 - f) une obligation de notifier toute infraction à la sécurité avérée ou présumée aux autorités appropriées des Parties respectives. L'Autorité Nationale de Sécurité de la Partie concernée est systématiquement informée de toute Infraction à la -Sécurité.
6. Une copie du chapitre consacré à la sécurité de tous les Contrats Classifiés est transmise à l'Autorité Nationale de Sécurité de la Partie sur le territoire de laquelle le Contrat Classifié doit être exécuté, afin de permettre la supervision et le contrôle corrects des normes, procédures et pratiques de sécurité fixées par les Contractants en vue de la protection des Informations Classifiées.
7. Les Autorités Nationales de Sécurité peuvent se demander de procéder à la vérification de l'efficacité des mesures adoptées par un contractant en vue de la protection des Informations Classifiées liées à un Contrat Classifié.

ARTICLE 9
TRANSMISSION DES INFORMATIONS CLASSIFIEES

1. Les informations classifiées sont transmises conformément aux lois et réglementations nationales de la Partie d'origine par la voie diplomatique ou de toute autre manière convenue entre les Autorités Nationales de Sécurité.
2. Les Parties peuvent transmettre des Informations Classifiées par voie électronique conformément aux procédures de sécurité approuvées par les Autorités Nationales de Sécurité.

ARTICLE 10
REPRODUCTION, TRADUCTION ET DESTRUCTION
DES INFORMATIONS CLASSIFIEES

1. Les reproductions et les traductions des informations classifiées portent les marquages de classification de sécurité appropriés et bénéficient du niveau de protection accordé aux informations classifiées originales. Le nombre de reproductions est limité au minimum requis.
2. Les traductions sont accompagnées d'une note dans la langue de traduction indiquant qu'elles contiennent des Informations Classifiées reçues de la Partie d'Origine.
3. La traduction et la reproduction des Informations Classifiées portant le marquage TRÈS SECRET (Loi du 11/12/1998) / ZEER GEHEIM (Wet van 11/12/1998) / „Szigorúan titkos!” sont autorisées moyennant le consentement écrit préalable de la Partie d'Origine.
4. Les Informations Classifiées portant le marquage TRÈS SECRET (Loi du 11/12/1998) / ZEER GEHEIM (Wet van 11/12/1998) / „Szigorúan titkos!” ne sont pas détruites. Elles sont renvoyées à la Partie d'Origine.
5. Dans toute situation de crise rendant impossible la protection, dans le respect de leur classification, des Informations Classifiées produites ou communiquées conformément au présent Accord, ou lorsque leur renvoi est impossible, les Informations Classifiées sont détruites immédiatement. L'Autorité Nationale de Sécurité de la Partie Destinataire informe dès que possible l'Autorité Nationale de Sécurité de la Partie d'Origine de la destruction des Informations Classifiées.

ARTICLE 11
VISITES

1. Les visites nécessitant l'accès à des Informations Classifiées sont soumises au consentement écrit préalable de l'Autorité Nationale de Sécurité concernée, sauf s'il en a été convenu autrement entre les Autorités Nationales de Sécurité.
2. Les visiteurs adressent toute demande de visite au moins vingt jours avant la visite à leur propre Autorité Nationale de Sécurité, qui la transmet à l'Autorité Nationale de Sécurité de l'autre Partie. Dans les cas d'urgence, le préavis peut être plus court, sous réserve d'une coordination préalable entre les Autorités Nationales de Sécurité.

3. Toute demande de visite contient les renseignements suivants:
 - a) nom et prénom du visiteur, date et lieu de naissance, nationalité et numéro de passeport ou de carte d'identité;
 - b) qualité du visiteur et nom de l'établissement représenté;
 - c) statut de l'Habilitation de Sécurité individuelle du visiteur et sa validité;
 - d) date et durée de la visite; en cas de visites multiples, il convient d'indiquer la période totale couverte par les visites;
 - e) objet de la visite, avec mention du niveau de protection le plus élevé requis par les Informations Classifiées concernées;
 - f) nom et adresse de l'établissement qui fait l'objet de la visite, ainsi que le nom du point de contact, ses numéros de téléphone et de fax et son adresse de courriel;
 - g) date, signature et sceau officiel de l'Autorité Nationale de Sécurité.
4. Les Autorités Nationales de Sécurité peuvent convenir d'une liste de visiteurs autorisés à effectuer des visites multiples. Les modalités détaillées sont convenues entre les Autorités Nationales de Sécurité.
5. Les Informations Classifiées acquises par un visiteur sont considérées au même titre que des Informations Classifiées communiquées en vertu du présent Accord.

ARTICLE 12

INFRACTIONS A LA SECURITE

1. Les Autorités Nationales de Sécurité se notifient toute Infraction à la Sécurité avérée ou présumée susceptible d'entraîner la divulgation non autorisée ou toute autre manipulation non autorisée d'Informations Classifiées.
2. Les autorités compétentes de la Partie Destinataire mènent sans retard injustifié une enquête sur l'incident. Sur demande, les autorités compétentes de la Partie d'Origine participent à l'enquête.
3. Dans tous les cas, la Partie Destinataire informe par écrit la Partie d'Origine des circonstances de l'Infraction à la Sécurité, de l'étendue des dommages, des mesures prises en vue d'atténuer les effets et du résultat de l'enquête.

ARTICLE 13

FRAIS

Chaque Partie supporte les frais encourus dans le cadre de la mise en œuvre du présent Accord.

ARTICLE 14
INTERPRETATION ET LITIGES

Tout litige relatif à l'interprétation ou à l'application du présent Accord est réglé par voie de négociations entre les Parties, sans recours à une juridiction extérieure.

ARTICLE 15
DISPOSITIONS FINALES

1. Le présent Accord est conclu pour une durée indéterminée. Le présent Accord entre en vigueur le premier jour du deuxième mois suivant la date de réception de la dernière notification entre les Parties, par la voie diplomatique, établissant qu'il a été satisfait aux procédures juridiques internes de mise en œuvre du présent Accord.
2. Le présent Accord peut être modifié sur la base du consentement mutuel des Parties. Ces modifications entrent en vigueur conformément aux dispositions du paragraphe 1 du présent Article.
3. Chaque Partie peut à tout moment dénoncer par écrit le présent Accord. L'Accord prend fin, dans ce cas, six mois après la date de la réception par l'autre Partie de la notification de dénonciation.
4. Même en cas de dénonciation du présent Accord, toutes les Informations Classifiées communiquées ou produites en exécution du présent Accord sont protégées conformément aux dispositions stipulées dans le présent Accord, jusqu'à ce que la Partie d'Origine libère la Partie Destinataire de cette obligation.

EN FOI DE QUOI, les soussignés, dûment autorisés à cet effet, ont signé le présent Accord.

FAIT à Budapest le 21 septembre 2015, en deux exemplaires originaux, en langues française, néerlandaise, hongroise et anglaise, tous les textes faisant également foi. En cas de divergence d'interprétation, le texte anglais prévaudra.

POUR LE ROYAUME DE BELGIQUE:



POUR LA HONGRIE:



[HUNGARIAN TEXT – TEXTE HONGROIS]

EGYEZMÉNY
A BELGA KIRÁLYSÁG
ÉS
MAGYARORSZÁG
KÖZÖTT A MINÓSÍTETT ADATOK CSERÉJÉRŐL
ÉS KÖLCSÖNÖS VÉDELMEÉRŐL

**EGYEZMÉNY
A BELGA KIRÁLYSÁG ÉS
MAGYARORSZÁG
KÖZÖTT A MINŐSÍTETT ADATOK CSERÉJÉRŐL
ÉS KÖLCŐSÖNÖS VÉDELMÉRŐL**

A BELGA KIRÁLYSÁG

ÉS

MAGYARORSZÁG,

a továbbiakban együtt: „a Felek”,

BIZTOSÍTANI kívánva a közöttük vagy joghatóságuk alá tartozó jogi személyek vagy természetes személyek között kicserélt vagy keletkezett minősített adatok védelmét egymás nemzeti érdekeinek és biztonságának kölcsönös tiszteletben tartásával az alábbiakban állapodtak meg:

1. CIKK

AZ EGYEZMÉNY TÁRGYA

1. Jelen Egyezmény célja, hogy biztosítsa a Felek, vagy a joghatóságuk alá tartozó jogi személyek és természetes személyek közötti együttműködés során kicserélt vagy keletkezett minősített adatok védelmét.
2. Jelen Egyezményt kell alkalmazni a Felek vagy joghatóságuk alá tartozó jogi személyek és természetes személyek között létrejött valamennyi, minősített adattal kapcsolatos szerződésnél vagy megállapodásnál, és egyéb együttműködésnél.

2 CIKK

FOGALOMMEGHATÁROZÁSOK

Jelen Egyezmény alkalmazásában:

„Minősített adat biztonságának megsértése” olyan, valamely személy által elkövetett tett vagy mulasztás, amely jelen Egyezménnyel vagy a Felek vonatkozó nemzeti jogszabályainak és egyéb szabályainak rendelkezéseivel ellentétes, és amely a minősített adat jogosulatlan felhasználását vagy egyéb jogosulatlan befolyásolását eredményezi.

„Minősített adat” megjelenési formájától függetlenül minden olyan adat, amelyet bármelyik Fél nemzeti jogszabályai és egyéb szabályai szerint védelemben kell részesíteni a jogosulatlan hozzáféréssel vagy bármely más jogosulatlan megváltoztatással szemben, s amelyet a jelen Egyezmény 4. és 6. Cikk rendelkezései szerint ilyennek minősítettek.

„Minősített Szerződés” olyan szerződést jelent, amely minősített adatot tartalmaz, vagy amely alapján minősített adathoz történő hozzáférés szükséges.

„Szerződést kötő” az a természetes vagy jogi személy, aki a szerződés megkötésére jogképességgel rendelkezik.

„Telephely Biztonsági Tanúsítvány” a Nemzeti Biztonsági Felügyelet azon pozitív döntése, amely szerint a létesítmény biztonsági szempontból nézve rendelkezik a minősített adatok kezeléséhez szükséges és a vonatkozó nemzeti jogszabályok és egyéb szabályok rendelkezéseinek megfelelő fizikai és szervezeti feltételekkel.

„Szükséges ismeret” a nemzeti jogszabályok és egyéb szabályok rendelkezéseinek tiszteletben tartásával annak megállapítása, hogy a természetes személy vagy jogi személy számára hivatali feladata vagy kötelezettségének ellátása céljából szükséges a minősített adatokhoz való hozzáférés.

„Átadó Fél” azt a Felet, valamint a joghatósága alá tartozó jogi vagy természetes személyeket jelenti, amelyek a minősített adatot átadják.

„Személyi Biztonsági Tanúsítvány” a Nemzeti Biztonsági Felügyelet azon, átvilágítás alapján hozott pozitív döntése, amely szerint a természetes személy a nemzeti jogszabályok és egyéb szabályok rendelkezéseinek tiszteletben tartásával jogosult hozzáférni minősített adatokhoz.

„Átvevő Fél” azt a Felet, valamint a joghatósága alá tartozó jogi személyeket vagy természetes személyeket jelenti, amelyek a minősített adatot átveszi.

„Harmadik Fél” bármely olyan államot, valamint a joghatósága alá tartozó jogi személyeket vagy természetes személyeket, továbbá nemzetközi szervezetet jelenti, amely nem részese jelen Egyezménynek.

3. CIKK NEMZETI BIZTONSÁGI FELÜGYELETEK

1. A minősített adatok védelméért, valamint jelen Egyezmény végrehajtásáért és felügyeletéért felelős Nemzeti Biztonsági Felügyelet a következők:

A Belga Királyságban:

National Veiligheidsverheid – Autorité nationale de Sécurité (Nemzeti Biztonsági Felügyelet)

Magyarországon:

Nemzeti Biztonsági Felügyelet

2. A Nemzeti Biztonsági Felügyelet kötelesek egymás rendelkezésére bocsátani hivatalos elérhetőségeiket és tájékoztatni egymást az ezekkel kapcsolatos valamennyi későbbi változásról.
3. Jelen Egyezmény hatékony végrehajtása érdekében a Nemzeti Biztonsági Felügyelet, a nemzeti jogszabályok és egyéb szabályok szerinti hatáskörükben eljárva, szükség esetén írásban részletes adminisztratív intézkedéseket is hozhatnak.

4. CIKK MINŐSÍTÉSI SZINTEK MEGFELELTETÉSE

1. Az egyes biztonsági minősítési szintek az alábbiak szerint feleltethetők meg egymásnak:

A Belga Királyságban		Magyarországon
Holland nyelven	Francia nyelven	
ZEER GEHEIM (Wet van 11/12/1998)	TRES SECRET (Loi du 11/12/1998)	„Szigorúan titkos!”
GEHEIM (Wet van 11/12/1998)	SECRET (Loi du 11/12/1998)	„Titkos!”
VERTROUWELIJK (Wet van 11/12/1998)	CONFIDENTIEL (Loi du 11/12/1998)	„Bizalmas!”
(lásd megjegyzés lent)	(lásd megjegyzés lent)”	„Korlátozott terjesztésű!”

2. A Belga Királyság a Magyarország által továbbított, „Korlátozott terjesztésű!” minősítéssel ellátott adatot a védett, de nem minősített adatra, mint a „BEPERKTE VERSPREIDING/DIFFUSION RESTREINTE” jelöléssel ellátott adatra vonatkozó nemzeti jogszabályainak és egyéb szabályainak megfelelően köteles kezelni és védeni.
3. Magyarország a Belga Királyság által továbbított, védett, de nem minősített adatot, mint a „BEPERKTE VERSPREIDING/DIFFUSION RESTREINTE” jelöléssel ellátott adatot köteles a „Korlátozott terjesztésű!” jelöléssel ellátott adatra vonatkozó nemzeti jogszabályainak és egyéb szabályainak megfelelően kezelni és védeni.

5. CIKK

MINŐSÍTETT ADATHOZ VALÓ HOZZÁFÉRÉS

1. A "BEPERKTE VERSPREIDING/DIFFUSION RESTREINTE" jelöléssel ellátott adathoz és a „Korlátozott terjesztésű!” jelöléssel ellátott minősített adathoz való hozzáférésre kizárólag az a személy jogosult, aki eleget tesz a szükséges ismeret elvének, és aki ezen adatokhoz való hozzáférésre az Átvevő Fél nemzeti jogszabályainak és egyéb szabályainak megfelelő felhatalmazást kapott.
2. A VERTROUWELIJK (Wet van 11/12/1998) / CONFIDENTIEL (Loi du 11/12/1998)/ „Bizalmas!” vagy magasabb szintű jelöléssel ellátott minősített adathoz való hozzáférésre kizárólag az a személy jogosult, aki eleget tesz a szükséges ismeret elvének, és megfelelő szintű Személyi Biztonsági Tanúsítvánnyal vagy az Átvevő Fél nemzeti jogszabályainak és egyéb szabályainak megfelelő felhatalmazással rendelkezik.
3. A Felek kötelesek biztosítani, hogy minden személy, aki jelen Cikk 1. és 2. bekezdése alapján férhet hozzá adatokhoz az adatok védelmével kapcsolatos kötelezettségéről a vonatkozó nemzeti jogszabályok és egyéb szabályok rendelkezéseivel összhangban tájékoztatást kapjon.

6. CIKK

A MINŐSÍTETT ADATOK VÉDELMERE VONATKOZÓ ALAPELVEK

1. Az Átadó Fél:
 - a) köteles biztosítani, hogy a minősített adaton a nemzeti jogszabályai és egyéb szabályai rendelkezéseinek megfelelő minősítési szint feltüntetésre kerüljön;
 - b) köteles tájékoztatni az Átvevő Felet a minősített adat felhasználásával kapcsolatos esetleges feltételekről;
 - c) haladéktalanul köteles tájékoztatni az Átvevő Felet az adat minősítésében bekövetkezett változásokról.
2. Az Átvevő Fél:
 - a) köteles biztosítani, hogy a minősített adaton feltüntetésre kerüljön a 4. Cikk alapján meghatározott egyenértékű minősítési szint;

- b) ugyanolyan szintű védelemben köteles részesíteni a minősített adatot, mint amelyet a saját, azonos minősítési szintű nemzeti minősített adata számára biztosít;
- c) köteles biztosítani, hogy az Átadó Fél előzetes írásbeli hozzájárulása nélkül az átvett minősített adat minősítését nem szünteti meg, illetve minősítési szintjét nem változtatja meg;
- d) köteles biztosítani, hogy az Átadó Fél előzetes írásbeli hozzájárulása nélkül az átvett minősített adatot Harmadik Fél részére nem adja át;
- e) a minősített adatot kizárólag az átadás során megjelölt célra használhatja fel, betartva az Átadó Fél által meghatározott felhasználásával kapcsolatos esetleges feltételeket.

7. CIKK

BIZTONSÁGI EGYÜTTMŰKÖDÉS

1. A hasonló szintű biztonsági követelmények fenntartása érdekében a Nemzeti Biztonsági Felügyelet a másik fél megkeresésére kötelesek egymást tájékoztatni a minősített adatok védelmével kapcsolatos nemzeti jogszabályokról és egyéb szabályokról, valamint mindezek gyakorlati alkalmazásáról. A Nemzeti Biztonsági Felügyelet tájékoztatják egymást minden, a nemzeti jogszabályokat és egyéb szabályokat érintő, a minősített adatok védelmével kapcsolatos lényeges változásról.
2. Megkeresés esetén a Nemzeti Biztonsági Felügyelet, összhangban a nemzeti jogszabályok és egyéb szabályok rendelkezéseivel, kölcsönösen segítséget nyújtanak egymásnak a Személyi Biztonsági Tanúsítványokkal és a Telephely Biztonsági Tanúsítványokkal kapcsolatos eljárások során.
3. A Felek megkeresés esetén nemzeti jogszabályok és egyéb szabályok rendelkezéseivel összhangban elismerik a másik Fél által kibocsátott Személyi Biztonsági Tanúsítványokat és Telephely Biztonsági Tanúsítványokat. Mindezek során a jelen Egyezmény 4. Cikkében foglaltakat kell alkalmazni.
4. Jelen Egyezmény hatálya alatt a Nemzeti Biztonsági Felügyelet haladéktalanul értesítik egymást az elismert Személyi Biztonsági Tanúsítványokkal és a Telephely Biztonsági Tanúsítványokkal kapcsolatos változásokról, különösen azok visszavonásáról vagy érvényességi idejük lejártáról.

8. CIKK

IPARBIZTONSÁGI INTÉZKEDÉSEK

1. A Minősített Szerződéseket a Felek saját nemzeti jogszabályok és egyéb szabályok rendelkezései alapján kell megkötöni, kihirdetni és teljesíteni. A Nemzeti Biztonsági Felügyelet megkeresésre kötelesek megerősíteni, hogy a szerződéskötést megelőző tárgyalásokban részt vevő lehetséges szerződő fél vagy a minősített szerződések teljesítésében részt vevő szerződő fél rendelkezik-e a megfelelő biztonsági tanúsítvánnyal.

2. A szerződő fél vonatkozó nemzeti jogszabályainak és egyéb szabályainak rendelkezéseivel összhangban köteles:
 - a) a 4. cikkben foglaltaknak megfelelően Telephely Biztonsági Tanúsítvánnyal rendelkezni;
 - b) biztosítani, hogy a minősített adathoz való hozzáférést igénylő személy a 4. és 5. cikk rendelkezéseinek megfelelően rendelkezzen Személyi Biztonsági Tanúsítvánnyal;
 - c) biztosítani, hogy a minősített adathoz való hozzáférésre feljogosított valamennyi személy a minősített adat védelmével kapcsolatos kötelezettségeiről tájékoztatást kapjon.
3. Az alvállalkozók kötelesek ugyanazon biztonsági követelményeknek eleget tenni, mint a szerződő fél.
4. A Nemzeti Biztonsági Felügyelet, a minősített szerződések megkötése érdekében kötelesek egymást tájékoztatni a szerződéskötést megelőző tárgyalásokhoz szükséges minősítési szintekről.
5. Jelen Egyezményrel összhangban kötött valamennyi Minősített Szerződésnek tartalmaznia kell egy megfelelő biztonsági fejezetet, amely az alábbiakat foglalja magába:
 - a) program biztonsági utasítás és minősítési jegyzék;
 - b) az adat minősítési szintjében bekövetkezett változások bejelentési eljárása;
 - c) kommunikációs csatornák;
 - d) minősített adat továbbításának eljárása;
 - e) a szerződéssel kapcsolatos minősített adatok védelmének koordinálásáért felelős Nemzeti Biztonsági Felügyelet elérhetősége;
 - f) bejelentési kötelezettség a minősített adat biztonságának tényleges vagy feltételezett megsértése esetén az érintett felek illetékes hatóságai felé. Az érintett fél Nemzeti Biztonsági Felügyeletét minden esetben értesíteni kell a minősített adat biztonságának megsértéséről.
6. Valamennyi Minősített Szerződés biztonsági rendelkezéseket tartalmazó fejezetéről másolatot kell küldeni azon Fél Nemzeti Biztonsági Felügyeletének, amelynek területén a Minősített Szerződés teljesítésére sor kerül azért, hogy biztosított legyen a szerződő felek által a minősített adatok védelme érdekében elfogadott biztonsági előírások, eljárások és gyakorlatok megvalósulásának megfelelő felügyelete és ellenőrzése.
7. A Nemzeti Biztonsági Felügyelet felkérheti a másik Fél Nemzeti Biztonsági Felügyeletét, hogy folytasson vizsgálatot a szerződő felek által a Minősített Szerződésben foglalt minősített adatok védelme érdekében foganatosított intézkedések hatékonyságáról.

9. CIKK

A MINŐSÍTETT ADAT TOVÁBBÍTÁSA

1. A minősített adat továbbítása az Átadó Fél nemzeti jogszabályainak és egyéb szabályainak rendelkezései szerint, diplomáciai úton, vagy a Nemzeti Biztonsági Felügyelet által közösen meghatározott egyéb módon történik.
2. A Felek a Nemzeti Biztonsági Felügyelet által jóváhagyott biztonsági eljárási rend szerint, elektronikus úton is továbbíthatnak minősített adatot.

10. CIKK

A MINŐSÍTETT ADAT SOKSZOROSÍTÁSA, FORDÍTÁSA ÉS MEGSEMMISÍTÉSE

1. A minősített adatról készült másolatokon és fordításokon fel kell tüntetni a megfelelő minősítési jelölést és az így készült adatot ugyanolyan védelemben kell részesíteni, mint az eredeti minősített adatot. A sokszorosított példányok számát a hivatalos célból szükséges minimumra kell korlátozni.
2. A fordításokon a fordítás nyelvén fel kell tüntetni, hogy az Átadó Fél minősített adatát tartalmazza.
3. A ZEER GEHEIM (Wet van 11/12/1998) / TRES SECRET (LOI DU 11/12/1998) / „Szigorúan titkos!” minősítésű adat fordítása vagy sokszorosítása kizárólag az Átadó Fél előzetes írásbeli engedélyével történhet.
4. A ZEER GEHEIM (Wet van 11/12/1998) / TRES SECRET (LOI DU 11/12/1998) / „Szigorúan titkos!” minősítésű adat nem semmisíthető meg, az ezen minősítési szintű adatokat az Átadó Félnek kell visszaszolgáltatni.
5. A jelen Egyezmény alapján keletkezett vagy átadott minősített adatot olyan válsághelyzet esetén, amely lehetetlenné teszi a minősítési szintjének megfelelő védelmét - ha visszajuttatása nem lehetséges - haladéktalanul meg kell semmisíteni. A minősített adat megsemmisítéséről az Átvevő Fél Nemzeti Biztonsági Felügyelete haladéktalanul értesíti az Átadó Fél Nemzeti Biztonsági Felügyeletét.

11. CIKK

LÁTOGATÁSOK

1. Minősített adathoz való hozzáférést igénylő látogatásra a Fogadó Fél Nemzeti Biztonsági Felügyeletének előzetes írásbeli jóváhagyása alapján kerülhet sor, kivéve, ha a Nemzeti Biztonsági Felügyeletek másként állapodtak meg.
2. A látogatásra vonatkozó megkeresést a látogatónak legalább húsz nappal a látogatás kezdő időpontja előtt a Nemzeti Biztonsági Felügyeletéhez kell benyújtani, amely azt továbbítja a másik Fél Nemzeti Biztonsági Felügyeletéhez. Sürgős esetben, a Nemzeti Biztonsági Felügyeletek közötti előzetes egyeztetést követően a látogatásra vonatkozó megkeresés a látogatás kezdetéhez közelebbi időpontban is benyújtható.

3. A látogatásra vonatkozó megkeresésnek az alábbiakat kell tartalmaznia:
- a) a látogató vezeték- és keresztnéve, születési helye és ideje, állampolgársága, útlevelének vagy más személyazonosító igazolványának száma;
 - b) a látogató beosztásának és a látogató által képviselt létesítmény megjelölése;
 - c) a látogató Személyi Biztonsági Tanúsítványának szintje és érvényességi ideje;
 - d) a látogatás időpontja és időtartama, visszatérő látogatások esetén az egyes látogatások összesített időtartama,
 - e) a látogatás célja, valamint a megismerendő legmagasabb minősítési szintű minősített adat minősítési szintjének megjelölése;
 - f) a meglátogatandó létesítmény neve és címe, valamint a kapcsolattartójának neve, telefonszáma/ fax száma, e-mail címe;
 - g) dátum, aláírás és a Nemzeti Biztonsági Felügyelet hivatalos pecsétjének lenyomata.
4. A Nemzeti Biztonsági Felügyeletnek közösen meghatározhatják a visszatérő látogatásra jogosult személyek listáját. A visszatérő látogatások további részleteit a Nemzeti Biztonsági Felügyelet állapítja meg.
5. A látogató által megismert minősített adatot úgy kell tekinteni, mint a jelen Egyezmény alapján átadott minősített adatot.

12. CIKK

ELJÁRÁS A MINŐSÍTETT ADAT BIZTONSÁGÁNAK MEGSÉRTÉSE ESETÉN

1. A Nemzeti Biztonsági Felügyeletnek késedelem nélkül írásban tájékoztatják egymást a minősített adat biztonságának megsértéséről vagy annak gyanúja esetén, ha az a minősített adathoz való jogosulatlan hozzáférést, vagy a minősített adat jogosulatlan megváltoztatását eredményezheti.
2. Az Átvevő Fél hatáskörrel rendelkező hatóságai kötelesek késedelem nélkül kivizsgálni az eseményt. Az Átadó Fél hatáskörrel rendelkező hatóságai szükség esetén részt vesznek a vizsgálatban.
3. Az Átvevő Fél minden esetben írásban tájékoztatja az Átadó Felet a minősített adat biztonságának megsértésével kapcsolatos körülményekről, a kár mértékéről, a kár enyhítése érdekében megtett intézkedésekről, valamint a vizsgálat eredményéről.

13. CIKK

KÖLTSÉGEK VISELÉSE

A Felek maguk viselik a jelen Egyezmény végrehajtásával összefüggésben felmerült költségeiket.

14. CIKK
ÉRTELMEZÉS ÉS VITÁK

Felek a jelen Egyezmény értelmezéséből vagy végrehajtásából fakadó vitákat tárgyalás és egyeztetés útján, külső igazságszolgáltatási fórum igénybevétele nélkül rendezik.

15. CIKK
ZÁRÓ RENDELKEZÉSEK

1. Jelen Egyezmény határozatlan időre jön létre. Jelen Egyezmény a Felek által az Egyezmény hatálybalépéséhez szükséges belső feltételek teljesítésére vonatkozó, diplomáciai úton küldött utolsó értesítés kézhezvételének napját követő második hónap első napján lép hatályba.
2. Jelen Egyezmény a Felek kölcsönös egyetértésével módosítható. A módosítások hatálybalépésével kapcsolatban a jelen Cikk 1. pontjában foglaltak az irányadók.
3. Bármelyik Fél jogosult jelen Egyezményt bármikor írásban felmondani. Felmondás esetén az Egyezmény a felmondásról szóló írásbeli értesítés másik Fél általi kézhezvételétől számított hat hónap elteltével hatályát veszti.
4. Az Egyezmény megszűnésétől függetlenül az annak alapján átadott vagy keletkezett minősített adatokat az Egyezményben meghatározott rendelkezések szerint kell védelemben részesíteni, mindaddig, amíg az Átadó Fél írásban felmentést nem ad az Átvevő Fél részére ezen kötelezettség alól.

FENTIEK TANÚBIZONYSÁGÁUL, az alulírott és az erre felhatalmazott megbízottak jelen Egyezményt aláírásukkal látták el.

KÉSZÜLT Budapesten, 2015. szeptember 21-én, két eredeti példányban, francia, holland, magyar és angol nyelven, valamennyi szöveg egyaránt hiteles. Eltérés esetén az angol nyelvű szöveg az irányadó.

A BELGA KIRÁLYSÁG
RÉSZÉRŐL:



MAGYARORSZÁG
RÉSZÉRŐL:

