



## PRESIDÊNCIA DO CONSELHO DE MINISTROS

### Decreto n.º 3/2021

de 8 de janeiro

*Sumário:* Aprova o Acordo entre a República Portuguesa e a Hungria Relativo à Troca e à Proteção Mútua de Informação Classificada, assinado em Lisboa, em 28 de junho de 2018.

O Acordo entre a República Portuguesa e a Hungria Relativo à Troca e à Proteção Mútua de Informação Classificada foi assinado em Lisboa, em 28 de junho de 2018.

Com o Acordo Relativo à Troca e à Proteção Mútua de Informação Classificada, a República Portuguesa e a Hungria estabelecem as regras para a proteção de informações classificadas trocadas entre as Partes ou entre pessoas singulares ou coletivas sob sua jurisdição, de acordo com o respetivo Direito das Partes.

O referido Acordo representa um contributo para o reforço das relações de amizade e de cooperação entre ambos os Estados.

Assim:

Nos termos da alínea c) do n.º 1 do artigo 197.º da Constituição, o Governo aprova o Acordo entre a República Portuguesa e a Hungria Relativo à Troca e à Proteção Mútua de Informação Classificada, assinado em Lisboa, em 28 de junho de 2018, cujo texto, nas versões autenticadas nas línguas portuguesa, húngara e inglesa, se publica em anexo.

Visto e aprovado em Conselho de Ministros de 10 de dezembro de 2020. — *Pedro Gramaxo de Carvalho Siza Vieira — Augusto Ernesto Santos Silva — Mariana Guimarães Vieira da Silva.*

Assinado em 23 de dezembro de 2020.

Publique-se.

O Presidente da República, MARCELO REBELO DE SOUSA.

Referendado em 29 de dezembro de 2020.

O Primeiro-Ministro, *António Luís Santos da Costa.*

### ACORDO ENTRE A REPÚBLICA PORTUGUESA E A HUNGRIA RELATIVO À TROCA E À PROTEÇÃO MÚTUA DE INFORMAÇÃO CLASSIFICADA

A República Portuguesa e a Hungria (doravante designadas por Partes):

Reconhecendo a importância da cooperação mútua entre as Partes;

Considerando que uma boa cooperação pode implicar a troca de informações classificadas entre as Partes;

Reconhecendo que ambas as Partes asseguram o mesmo tipo de proteção para as informações classificadas;

Pretendendo garantir a proteção das informações classificadas trocadas entre as Partes ou entre as pessoas singulares ou coletivas sob sua jurisdição; e

Tendo em conta o respeito mútuo pelos interesses nacionais e de segurança:

Acordaram no seguinte:

#### Artigo 1.º

#### Âmbito de aplicação

O presente Acordo estabelece as regras para a proteção de informações classificadas trocadas entre as Partes ou entre as pessoas singulares ou coletivas sob sua jurisdição, de acordo com o respetivo Direito das Partes.

**Artigo 2.º****Definições**

Para os efeitos do presente Acordo:

a) «Quebra de segurança» significa um ato ou omissão contrária ao respetivo Direito das Partes, que possa levar à divulgação, perda, destruição, apropriação indevida, acesso ou qualquer outro tipo de comprometimento da informação classificada;

b) «Contrato classificado» designa um acordo que contém ou envolve acesso a informação classificada, estabelecendo e definindo direitos e obrigações legalmente exigíveis;

c) «Informação classificada» designa a informação que, independentemente da sua forma ou natureza, necessita de proteção contra quebras de segurança e que tenha sido designada como tal;

d) «Contratante» significa uma pessoa coletiva ou singular que tem capacidade jurídica para celebrar contratos classificados;

e) «Credenciação de segurança das instalações» significa a decisão, por parte de uma autoridade nacional de segurança, de que uma pessoa coletiva ou singular que possua capacidade jurídica dispõe de condições físicas e organizacionais para manusear e guardar informações classificadas;

f) «Autoridade nacional de segurança» significa a autoridade estatal responsável pela segurança e salvaguarda de informações classificadas, bem como para a aplicação deste Acordo;

g) «Necessidade de conhecer» significa o princípio de acordo com o qual o acesso a informações classificadas só pode ser concedido a uma pessoa que tenha uma necessidade justificada de acesso a informações classificadas em virtude do exercício das suas funções ou para a realização de uma missão específica;

h) «Parte transmissora» designa a Parte, incluindo as pessoas coletivas ou singulares sob sua jurisdição, que transmite informação classificada à outra Parte;

i) «Credenciação de segurança de pessoa singular» significa a decisão, por uma autoridade nacional de segurança, de que um indivíduo é elegível para ter acesso a informações classificadas;

j) «Parte destinatária» designa a Parte, incluindo as pessoas coletivas ou singulares sob sua jurisdição, que recebe a informação classificada da Parte transmissora;

k) «Subcontrato» significa um contrato entre um contratante e outro contratante (subcontratante) criando e definindo direitos e obrigações legalmente exigíveis;

l) «Subcontratante» significa uma pessoa coletiva ou singular que possui capacidade jurídica para celebrar contratos classificados, e com quem um contratante celebra um subcontrato;

m) «Terceira parte» designa qualquer organização internacional ou Estado que não é Parte no presente Acordo.

**Artigo 3.º****Autoridades nacionais de segurança**

1 — As autoridades nacionais de segurança das Partes são:

a) Pela República Portuguesa:

Autoridade Nacional de Segurança, Presidência do Conselho de Ministros (National Security Authority, Presidency of the Council of Ministers);

b) Pela Hungria:

Nemzeti Biztonsági Felügyelet (National Security Authority).

2 — Cada uma das Partes deve informar a outra Parte, por escrito, por via diplomática, de qualquer alteração relacionada com a designação das autoridades de segurança nacional.



3 — As autoridades nacionais de segurança devem indicar os seus contactos oficiais e informar-se mutuamente sobre quaisquer alterações subsequentes.

4 — Qualquer alteração relativa às autoridades nacionais de segurança não constitui uma emenda ao presente Acordo.

#### Artigo 4.º

##### Graus de classificação de segurança

A equivalência entre os respetivos graus de classificação de segurança é a seguinte:

| Para a República Portuguesa | Para a Hungria                       | Termos em língua inglesa |
|-----------------------------|--------------------------------------|--------------------------|
| Muito Secreto . . . . .     | „Szigorúan titkos!” . . . . .        | Top Secret.              |
| Secreto . . . . .           | „Titkos!” . . . . .                  | Secret.                  |
| Confidencial . . . . .      | „Bizalmas!” . . . . .                | Confidential.            |
| Reservado . . . . .         | „Korlátozott terjesztésű!” . . . . . | Restricted.              |

#### Artigo 5.º

##### Acesso à informação classificada

O acesso a informações classificadas ao abrigo deste Acordo deve ser limitado aos indivíduos que tenham necessidade de conhecer, que estão devidamente credenciados e informados sobre suas obrigações para proteger essas informações.

#### Artigo 6.º

##### Princípios de segurança

1 — A Parte transmissora deve:

- Assegurar que a informação classificada é marcada com os graus de classificação de segurança apropriados;
- Informar a Parte destinatária de quaisquer limitações ao uso de informação classificada;
- Informar por escrito e sem atrasos indevidos a Parte destinatária de quaisquer alterações posteriores na classificação de segurança ou na duração dessa classificação.

2 — A Parte destinatária deve:

- Assegurar que as informações classificadas sejam classificadas com a classificação equivalente em conformidade com o artigo 4.º deste Acordo;
- Oferecer o mesmo grau de proteção para informações classificadas, tal como oferecidas às suas próprias informações classificadas de nível de classificação equivalente;
- Assegurar a proteção da informação classificada equivalente ao seu nível de classificação até a notificação por escrito da parte transmissora sobre a desclassificação ou a alteração do nível de classificação ou da validade das informações classificadas;
- Assegurar que as informações classificadas não sejam divulgadas a terceiros sem o consentimento prévio por escrito da parte transmissora;
- Usar informações classificadas apenas para a finalidade para a qual foram transmitidas e de acordo com as condições de transmissão da parte transmissora.

#### Artigo 7.º

##### Cooperação em matéria de segurança

1 — A fim de manter normas de segurança equivalentes, as autoridades de segurança nacional devem, sempre que solicitado, informar-se mutuamente sobre o respetivo Direito aplicável à troca e proteção de informações classificadas.



2 — Sempre que solicitado, as autoridades de segurança nacional devem prestar assistência mútua relativamente aos procedimentos de credenciação de segurança de pessoas singulares ou de credenciação de segurança das instalações.

3 — Sempre que solicitado, as Partes devem reconhecer as credenciações de segurança de pessoas singulares ou as credenciações de segurança das instalações emitidas pela outra Parte.

4 — As autoridades nacionais de segurança devem notificar-se prontamente sobre as alterações nas credenciações de segurança reconhecidas das pessoas singulares ou das instalações, especialmente no caso do seu cancelamento.

5 — A cooperação no âmbito do presente Acordo será efetuada em língua inglesa.

## Artigo 8.º

### Contratos classificados

1 — No caso de contratos classificados com grau de Confidencial/„Bizalmas!“/ Confidential ou superior, executados no território de uma das Partes, a autoridade nacional de segurança da outra Parte deve entregar uma garantia prévia, por escrito, de que o contratante proposto detém uma credenciação de segurança das instalações de grau de classificação de segurança apropriado.

2 — O contratante ou subcontratante deve assegurar que todas as pessoas com acesso à informação classificada estão informadas da sua responsabilidade para com a proteção da informação classificada.

3 — Qualquer das autoridades nacionais de segurança pode solicitar à outra para efetuar uma inspeção de segurança numa instalação situada no território da outra Parte, de forma a assegurar o contínuo cumprimento dos padrões de segurança.

4 — Representantes das autoridades nacionais de segurança podem fazer visitas recíprocas para análise da eficácia das medidas adotadas por um contratante para proteção da informação classificada constante de um contrato classificado.

5 — O contrato classificado celebrado entre contratantes das Partes nos termos das disposições do presente Acordo deve incluir instruções de segurança do projeto apropriadas, identificando pelo menos os seguintes aspetos:

a) Lista de informação classificada envolvida no contrato classificado e a sua classificação de segurança;

b) Procedimento para a comunicação de alteração na classificação de segurança da informação;

c) Canais de comunicação e meios para transmissão eletromagnética;

d) Procedimento para o transporte de informação classificada;

e) Obrigação de notificação de qualquer divulgação não autorizada, acesso indevido ou perda da informação classificada, sejam estes reais ou suspeitas.

6 — Uma cópia das instruções de segurança do projeto deve ser remetida à autoridade de segurança competente da Parte em cujo território o contrato classificado será executado, de forma a garantir a adequada supervisão de segurança e controlo.

## Artigo 9.º

### Transmissão da informação classificada

1 — A informação classificada deve ser transmitida através dos canais diplomáticos, salvo no caso de ter sido determinado outro meio por acordo escrito entre as autoridades nacionais de segurança.

2 — A autoridade nacional de segurança da Parte destinatária deve confirmar, por escrito, a receção da informação classificada.



Artigo 10.º

**Reprodução, tradução e destruição da informação classificada**

1 — As reproduções e traduções de informações classificadas divulgadas ao abrigo do presente Acordo devem conter as classificações apropriadas e devem ser protegidas como originais. O número de reproduções deve ser limitado ao exigido para fins oficiais.

2 — As traduções de informações classificadas divulgadas ao abrigo do presente Acordo devem conter uma nota na língua de tradução que indique que contêm informações classificadas da parte transmissora.

3 — A informação classificada divulgada ao abrigo do presente Acordo marcada Muito Secreto/„Szigorúan titkos!”/Top Secret deve ser reproduzida ou traduzida apenas mediante consentimento prévio e por escrito da parte transmissora.

4 — A informação classificada divulgada ao abrigo do presente Acordo marcada Muito Secreto/„Szigorúan titkos!”/Top Secret não deve ser destruída e deve ser devolvida à parte transmissora.

5 — No caso de uma situação em que é impossível proteger ou devolver a informação classificada à parte transmissora, ela deve ser destruída sem atrasos indevidos. A autoridade nacional de segurança da Parte destinatária deve notificar por escrito a autoridade nacional de segurança da parte transmissora sobre a destruição das informações classificadas.

Artigo 11.º

**Visitas**

1 — Com exceção das visitas que envolvam acesso a informação classificada marcada como Reservado/„Korlátozott terjesztésű!”/Restricted, que podem ser acordadas diretamente entre os encarregados de segurança das respetivas entidades, as visitas que envolvam acesso a informação classificada estão sujeitas a autorização prévia, por escrito, conferida pela autoridade de segurança competente da Parte anfitriã.

2 — A autoridade nacional de segurança da Parte visitante deve notificar a autoridade de segurança competente da Parte anfitriã mediante um pedido de visita com uma antecedência mínima de 20 dias.

3 — Em caso de urgência, o pedido de visita deve ser submetido com uma antecedência mínima de sete dias.

4 — O pedido de visita deve incluir a informação seguinte:

- a) O nome do visitante, o local e a data de nascimento, a nacionalidade, o número do passaporte ou bilhete de identidade;
- b) O cargo do visitante e o nome da entidade que o visitante representa;
- c) O grau de credenciação de segurança do visitante e respetiva validade;
- d) Data e duração da visita e, em caso de visitas recorrentes, o período total abrangido pelas visitas;
- e) Propósito da visita, incluindo o grau mais elevado de informação classificada envolvida;
- f) O nome e a morada das instalações a visitar, bem como o nome, o número de telefone ou fax e o endereço de correio eletrónico do respetivo ponto de contacto;
- g) A data, a assinatura e a aposição do selo oficial da autoridade de segurança competente.

5 — A autoridade de segurança competente da Parte anfitriã deve informar, oportunamente, a autoridade de segurança competente da Parte visitante sobre a sua decisão.

6 — As visitas de indivíduos de uma terceira parte que envolvam acesso a informação classificada da Parte transmissora apenas devem ser autorizadas mediante consentimento, por escrito, da autoridade de segurança competente da Parte transmissora.

7 — A autoridade de segurança competente da Parte anfitriã deve fornecer uma cópia da aprovação do pedido de visita aos encarregados de segurança da entidade a ser visitada.

8 — A validade da autorização de visita não deve exceder os 12 meses.

9 — As Partes podem acordar estabelecer uma lista de pessoas autorizadas a efetuar visitas recorrentes, que será válida por um período inicial de 12 meses.



10 — Após as Partes terem aprovado as listas para visitas recorrentes, os termos das visitas específicas devem ser diretamente acordados com os encarregados de segurança das entidades a serem visitadas.

11 — Toda a informação classificada obtida por um visitante deve ser considerada como informação classificada transmitida ao abrigo do presente Acordo.

#### **Artigo 12.º**

##### **Quebra de segurança**

1 — As autoridades de segurança nacionais devem, sem atrasos indevidos, informar por escrito a outra parte de qualquer suspeita ou quebra de segurança.

2 — A autoridade nacional de segurança da Parte em cujo território a quebra da segurança ocorreu deve investigar o incidente sem atrasos indevidos. A autoridade nacional de segurança da outra Parte deve, se necessário, cooperar no inquérito.

3 — Em qualquer caso, a autoridade nacional de segurança da parte destinatária deve informar por escrito a autoridade nacional de segurança da Parte transmissora sobre as circunstâncias em que ocorreu a quebra de segurança, a extensão do dano, as medidas adotadas para mitigação e o resultado da investigação.

#### **Artigo 13.º**

##### **Encargos**

Cada Parte deve assumir os encargos que para si advenham da aplicação do presente Acordo.

#### **Artigo 14.º**

##### **Outras obrigações internacionais**

As disposições deste Acordo não afetam os direitos e obrigações decorrentes de outras convenções internacionais às quais as Partes pertençam.

#### **Artigo 15.º**

##### **Solução de controvérsias**

Qualquer controvérsia sobre a interpretação ou aplicação do presente Acordo deve ser resolvida mediante negociação entre as Partes, por via diplomática.

#### **Artigo 16.º**

##### **Entrada em vigor**

O presente Acordo entrará em vigor no trigésimo dia após a receção da última das notificações escritas, por via diplomática, informando que foram cumpridos todos os procedimentos internos necessários para esse efeito.

#### **Artigo 17.º**

##### **Revisão**

1 — As Partes podem rever o presente Acordo com base no consentimento mútuo, por escrito.

2 — As emendas entrarão em vigor nos termos previstos no artigo 16.º do presente Acordo.

#### **Artigo 18.º**

##### **Vigência e denúncia**

1 — O presente Acordo permanecerá em vigor por um período de tempo indeterminado.

2 — Qualquer das Partes pode, a qualquer momento, denunciar o presente Acordo.

3 — A denúncia deve ser notificada, por escrito e por via diplomática, produzindo efeitos seis meses após a data da receção da respetiva notificação.

4 — Não obstante a denúncia, toda a informação classificada transmitida ao abrigo do presente Acordo continuará a ser protegida em conformidade com as disposições do mesmo até que a Parte transmissora dispense a Parte destinatária dessa obrigação, por escrito e por via diplomática.

#### Artigo 19.º

##### Registo

Após a entrada em vigor do presente Acordo, a Parte em cujo território este seja assinado submetê-lo-á para registo junto do Secretariado das Nações Unidas, nos termos do artigo 102.º da Carta das Nações Unidas, e notificará a outra Parte da conclusão deste procedimento, indicando-lhe o número de registo atribuído.

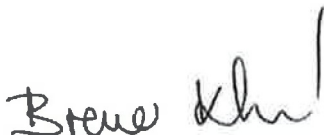
Em fé do que os abaixo assinados, devidamente autorizados para o efeito, assinaram o presente Acordo.

Feito em Lisboa, aos 28 de junho de 2018, em dois originais, cada um nas línguas portuguesa, húngara e inglesa, fazendo todos os textos igualmente fé. Em caso de divergência de interpretação, prevalecerá o texto na língua inglesa.

Pela República Portuguesa:



Pela Hungria:



#### EGYEZMÉNY A PORTUGÁL KÖZTÁRSASÁG ÉS MAGYARORSZÁG KÖZÖTT

#### A MINŐSÍTETT ADATOK CSERÉJÉRŐL ÉS KÖLCSÖNÖS VÉDELMEÉRŐL

A Portugal Köztársaság és Magyarország (a továbbiakban: Felek)

elismerve a Felek közötti kölcsönös együttműködés jelentőségét,

**felismerve**, hogy a Felek közötti jó együttműködés során szükség lehet minősített adatok cseréjére,

**elismerve**, hogy azonos szintű védelmet biztosítanak a minősített adatok számára,

**kíváncosnak tartva**, hogy a közöttük vagy joghatóságuk alá tartozó jogi személyek vagy természetes személyek között kicserélt minősített adatok megfelelő védelemben részesüljenek,

tiszteletben tartva egymás nemzeti érdekeiket és biztonságát, az alábbiakban állapodtak meg:

## 1. CIKK AZ EGYEZMÉNY HATÁLYA

Jelen Egyezmény a Felek között vagy a joghatóságuk alá tartozó jogi személyek vagy természetes személyek között kicserélt minősített adatok védelmével kapcsolatos szabályokat határozza meg a Felek vonatkozó jogszabályaival összhangban.

## 2. CIKK FOGALOMMEGHATÁROZÁSOK

Jelen Egyezmény alkalmazásában:

- a) **a minősített adat biztonságának megsértése**: olyan, a Felek vonatkozó jogszabályaival ellentétes tevékenység vagy mulasztás, ami a minősített adat jogosulatlan nyilvánosságra hozatalához, elvesztéséhez, megsemmisüléséhez, jogosulatlan felhasználáshoz, megszerzéséhez vagy egyéb módon történő megsértéséhez vezethet;
- b) **minősített szerződés**: olyan szerződés, amely minősített adatot tartalmaz, vagy amely alapján minősített adathoz való hozzáférés szükséges kikényszeríthető jogokat és kötelezettségeket létrehozva és meghatározva;
- c) **minősített adat**: megjelenési formájától, természetétől függetlenül minden olyan adat, amelyet védelemben kell részesíteni a minősített adat biztonságának megsértésével szemben, és amelyet ennek megfelelően minősítettek;
- d) **szerződő**: olyan jogi személy vagy természetes személy, aki rendelkezik a minősített szerződések megkötésére irányuló képességgel;
- e) **telephely biztonsági tanúsítvány**: a nemzeti biztonsági hatóság azon döntése, amely megállapítja, hogy a jogi személy vagy természetes személy rendelkezik a minősített adatok kezelésére és tárolására vonatkozó fizikai és szervezeti képességekkel;
- f) **nemzeti biztonsági hatóság**: az az állami szerv, amely a minősített adatok biztonságáért és védelméért, valamint jelen Egyezmény alkalmazásáért felelős;
- g) **szükséges ismeret**: az az elv, amely alapján a minősített adathoz való hozzáférés csak annak a személynek biztosítható, akinek az adott minősített adathoz való hozzáférés hivatali kötelessége vagy meghatározott feladata ellátásához igazoltan szükséges;
- h) **átadó Fél**: az a Fél – beleértve a joghatósága alá tartozó jogi személyeket vagy természetes személyeket –, amelyik a minősített adatot a másik Félnek átadja;
- i) **személyi biztonsági tanúsítvány**: a nemzeti biztonsági hatóság azon döntése, amely megállapítja, hogy egy természetes személy alkalmas arra, hogy minősített adatokhoz hozzáférhessen;



- j) **átvevő Fél:** az a Fél – beleértve a joghatósága alá tartozó jogi személyeket vagy természetes személyeket –, amelyik a nemzeti minősített adatot a másik Féltől átveszi;
- k) **alvállalkozói szerződés:** a szerződő által, egy másik szerződővel (alvállalkozóval) kötött szerződés, amely kikényszeríthető jogokat és kötelezettségeket hoz létre és határoz meg;
- l) **alvállalkozó:** olyan, a minősített szerződések megkötésére irányuló képességgel rendelkező jogi személy vagy természetes személy, akivel a szerződő alvállalkozói szerződést köt;
- m) **harmadik Fél:** bármely olyan nemzetközi szervezet vagy állam, amely nem részese jelen Egyezménynek.

### 3. CIKK NEMZETI BIZTONSÁGI HATÓSÁGOK

(1) A Felek nemzeti biztonsági hatóságai:

a) a Portugál Köztársaságban:  
Autoridade Nacional de Segurança,  
Presidência do Conselho de Ministros  
(Nemzeti Biztonsági Felügyelet, A Minisztertanács Elnöksége)

b) Magyarországon:  
Nemzeti Biztonsági Felügyelet

(2) A nemzeti biztonsági hatóságok kötelesek egymást írásban, diplomáciai úton tájékoztatni a nemzeti biztonsági hatósággal kapcsolatos valamennyi változásról.

(3) A nemzeti biztonsági hatóságok kötelesek egymást tájékoztatni hivatalos elérhetőségi adataikról és az azokban bekövetkező valamennyi későbbi változásról.

(4) A nemzeti biztonsági hatósággal kapcsolatos változások nem minősülnek jelen Egyezmény módosításának.

### 4. CIKK MINŐSÍTÉSI SZINTEK

Az egyes minősítési szintek az alábbiak szerint feleltethetők meg egymásnak:

| A Portugál<br>Köztársaságban | Magyarországon             | Angol nyelvű<br>megfelelőjük |
|------------------------------|----------------------------|------------------------------|
| MUITO SECRETO                | „Szigorúan titkos!”        | TOP SECRET                   |
| SECRETO                      | „Titkos!”                  | SECRET                       |
| CONFIDENCIAL                 | „Bizalmas!”                | CONFIDENTIAL                 |
| RESERVADO                    | „Korlátozott terjesztésű!” | RESTRICTED                   |



## **5. CIKK**

### **MINŐSÍTETT ADATHOZ VALÓ HOZZÁFÉRÉS**

Jelen Egyezmény alapján minősített adathoz kizárólag olyan természetes személyek kaphatnak hozzáférést, akik a szükséges ismeret elvének megfelelnek, akik erre megfelelő felhatalmazást kaptak és ezen adatok védelmével kapcsolatos kötelezettségeikről tájékoztatást kaptak.

## **6. CIKK**

### **BIZTONSÁGI ALAPELVEK**

(1) Az átadó Fél:

- a) biztosítja, hogy a minősített adaton a megfelelő minősítési szint feltüntetésre kerüljön;
- b) tájékoztatja az átvevő Felet a minősített adat felhasználásával kapcsolatos esetleges feltételekről;
- c) késedelem nélkül, írásban tájékoztatja az átvevő Felet az adat minősítésében vagy a minősítés érvényességi idejében bekövetkezett későbbi változásokról.

(2) Az átvevő Fél:

- a) biztosítja, hogy a minősített adaton feltüntetésre kerüljön a jelen Egyezmény 4. cikkének megfelelő egyenértékű minősítési szint;
- b) ugyanolyan szintű védelemben köteles részesíteni a minősített adatot, mint amelyet a saját, azonos minősítési szintű minősített adata számára biztosít;
- c) mindaddig biztosítja a minősített adat minősítési szintjének megfelelő védelmet, amíg az átadó Féltől a minősített adat minősítésének megszüntetéséről vagy minősítési szintjének vagy érvényességi idejének megváltoztatásáról írásban tájékoztatást nem kap;
- d) biztosítja, hogy az átadó Fél előzetes írásbeli hozzájárulása nélkül a minősített adatot harmadik Fél részére nem adja át;
- e) a minősített adatot kizárólag az átadás során megjelölt célra használja fel, betartva az átadó Fél által meghatározott átadási feltételeket.

## **7. CIKK**

### **BIZTONSÁGI EGYÜTTMŰKÖDÉS**

(1) Az összeegyeztethető szintű biztonsági követelmények fenntartása érdekében a nemzeti biztonsági hatóságok megkeresés esetén tájékoztatják egymást a minősített adat cseréjével és védelmével kapcsolatos jogszabályaikról.

(2) Megkeresés esetén a nemzeti biztonsági hatóságok kölcsönösen segítséget nyújtanak egymásnak a személyi biztonsági tanúsítványokkal és a telephely biztonsági tanúsítványokkal kapcsolatos eljárások során.

(3) Megkeresés esetén a Felek elismerik a másik Fél által kibocsátott személyi biztonsági tanúsítványokat és telephely biztonsági tanúsítványokat.

(4) A nemzeti biztonsági hatóságok haladéktalanul értesítik egymást az elismert személyi biztonsági tanúsítványokkal és telephely biztonsági tanúsítványokkal kapcsolatos változásokról, különösen azok visszavonásáról.

(5) A jelen Egyezmény alapján megvalósuló együttműködés angol nyelven történik.

## **8. CIKK**

### **MINŐSÍTETT SZERZŐDÉSEK**

(1) Olyan CONFIDENCIAL/ „Bizalmas!”/ CONFIDENTIAL és magasabb szintű minősített szerződések esetén, melyek teljesítése az egyik Fél területén belül valósul meg, a másik Fél nemzeti biztonsági hatósága előzetesen, írásban megerősíti, hogy a lehetséges szerződő rendelkezik a megfelelő szintű telephely biztonsági tanúsítvánnyal.

(2) A szerződő vagy alvállalkozó biztosítja, hogy azon személyek, akik a minősített adatokhoz hozzáférhetnek, tájékoztatást kaptak a minősített adat védelmével kapcsolatos kötelezettségeikről.

(3) A nemzeti biztonsági hatóság kérheti biztonsági ellenőrzés lefolytatását a másik Fél területén működő létesítményben a biztonsági előírások folyamatos betartásának biztosítása céljából.

(4) A nemzeti biztonsági hatóságok képviselői látogatást tehetnek a másik Fél nemzeti biztonsági hatóságánál a minősített szerződéssel kapcsolatban érintett minősített adatok védelmére vonatkozó, a szerződő által meghozott intézkedések hatékonyságának elemzése céljából.

(5) A Felek szerződői által kötött minősített szerződések jelen Egyezmény rendelkezései alapján megfelelő projekt biztonsági utasítást is tartalmaznak, amelyek legalább az alábbi adatokra kitérnek;

a) a minősített szerződéssel kapcsolatban érintett minősített adatok listája és minősítési szintjük;

b) az adat minősítési szintjében bekövetkezett változásról való tájékoztatás folyamata;

c) az elektromágneses továbbítás kommunikációs csatornái és eszközei;

d) a minősített adat szállításának folyamata;

e) tájékoztatási kötelezettség a minősített adat tényleges vagy feltételezett nyilvánosságra hozataláról, jogosulatlan felhasználásáról vagy elvesztéséről.

(6) Megfelelő biztonsági felügyelet és ellenőrzés biztosítása céljából a minősített szerződés projekt biztonsági utasításának másolata megküldésre kerül azon Fél nemzeti biztonsági hatósága számára, ahol a minősített szerződés teljesítése történik.

## **9. CIKK**

### **A MINŐSÍTETT ADAT TOVÁBBÍTÁSA**

(1) A minősített adat továbbítása diplomáciai úton történik kivéve, ha a nemzeti biztonsági hatóságok írásban ettől eltérően állapodnak meg.

(2) Az átvevő Fél nemzeti biztonsági hatósága a minősített adat átvételét írásban megerősíti.

## **10. CIKK**

### **A MINŐSÍTETT ADAT SOKSZOROSÍTÁSA, FORDÍTÁSA ÉS MEGSEMISÍTÉSE**

(1) Jelen Egyezmény alapján átadott minősített adatról készült másolatokon és fordításokon fel kell tüntetni az eredeti minősítési jelölést, és az így készült adatot ugyanolyan védelemben kell részesíteni, mint az eredeti minősített adatot. A sokszorosított példányok számát a hivatalos célból szükséges mértékre kell korlátozni.

(2) Jelen Egyezmény alapján átadott minősített adat fordítása során keletkező példányokon fel kell tüntetni a fordítás nyelvén azt, hogy az átadó Fél minősített adatát tartalmazza.

(3) Jelen Egyezmény alapján átadott MUITO SECRETO/ „Szigorúan titkos!”/ TOP SECRET minősítésű adat csak az átadó Fél előzetes írásbeli engedélyével sokszorosítható vagy fordítható.



(4) Jelen Egyezmény alapján átadott MUITO SECRETO/ „Szigorúan titkos!”/ TOP SECRET minősítésű adat nem semmisíthető meg és az átadó Fél részére kell visszaküldeni.

(5) A minősített adatot olyan válsághelyzet esetén, amely lehetetlenné teszi annak védelmét, vagy ha annak az átadó Félhez való visszajuttatása nem lehetséges, késedelem nélkül meg kell semmisíteni. A minősített adat megsemmisítéséről az átvevő Fél nemzeti biztonsági hatósága az átadó Fél nemzeti biztonsági hatóságát írásban értesíti.

## 11. CIKK LÁTOGATÁSOK

(1) A minősített adathoz való hozzáféréssel járó látogatásokhoz a fogadó Fél nemzeti biztonsági hatóságának előzetes írásbeli beleegyezése szükséges, kivéve a RESERVADO/ „Korlátozott terjesztésű!”/ RESTRICTED minősítésű minősített adathoz való hozzáféréssel járó látogatásokat, amelyeket közvetlenül az érintett létesítmények biztonsági vezetői is lebonyolíthatnak.

(2) A látogatást kezdeményező Fél nemzeti biztonsági hatósága legalább húsz nappal a látogatás kezdő időpontja előtt értesíti a fogadó Fél nemzeti biztonsági hatóságát a tervezett látogatásról.

(3) Sürgős esetben a látogatási kérelem legalább hét nappal megelőzően benyújtható.

(4) A látogatási kérelem az alábbiakat tartalmazza:

- a) a látogató neve, születési helye és ideje, állampolgársága, útlevelének vagy más személyazonosító igazolványának száma;
- b) a látogató beosztása és a látogató által képviselt szervezet 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, beleértve a látogatással érintett legmagasabb minősítési szintű minősített adat minősítési szintjének megjelölését;
- f) a meglátogatandó létesítmény neve és címe, valamint a kapcsolattartójának neve, telefonszáma, fax száma, e-mail címe;
- g) dátum, aláírás és a nemzeti biztonsági hatóság hivatalos pecsétjének lenyomata.

(5) A fogadó Fél nemzeti biztonsági hatósága a látogató Fél nemzeti biztonsági hatóságát kellő időben tájékoztatja a döntésről.

(6) Harmadik országbeli személyek olyan látogatása, amely az átadó Fél minősített adatához való hozzáféréssel jár, kizárólag az átadó Fél nemzeti biztonsági hatóságának írásbeli engedélye esetén bonyolítható le.

(7) A fogadó Fél nemzeti biztonsági hatósága a jóváhagyott látogatási kérelem másolatát megküldi a meglátogatandó létesítmények biztonsági vezetőinek.

(8) A látogatási engedély érvényessége nem lehet több mint tizenkét hónap.

(9) A Felek közösen meghatározhatják a visszatérő látogatásra jogosult személyek listáját, melynek kezdő érvényességi ideje tizenkét hónap

(10) A visszatérő látogatók listájának a Felek által való elfogadása után az egyes látogatások részleteiről a meglátogatandó létesítmények biztonsági vezetői közvetlenül állapodnak meg.

(11) A látogató által megismert minősített adatot úgy kell tekinteni, mint a jelen Egyezmény alapján átadott minősített adatot.



## **12. CIKK A MINŐSÍTETT ADAT BIZTONSÁGÁNAK MEGSÉRTÉSE**

- (1) A nemzeti biztonsági hatóságok késedelem nélkül írásban tájékoztatják egymást a minősített adat biztonságának megsértéséről vagy annak gyanújáról.
- (2) Azon Fél nemzeti biztonsági hatósága, ahol a minősített adat biztonságának megsértésére sor került, késedelem nélkül kivizsgálja az esetet. Ha szükséges, a másik Fél nemzeti biztonsági hatósága együttműködik a vizsgálatban.
- (3) Az átvevő Fél nemzeti biztonsági hatósága minden esetben írásban tájékoztatja az átadó Fél nemzeti biztonsági hatóságát 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 EGYÉB NEMZETKÖZI KÖTELEZETTSÉGEK**

Jelen Egyezmény rendelkezései nem érintik a Felek egyéb nemzetközi egyezményből eredő jogait és kötelezettségeit.

## **15. CIKK VITÁK RENDEZÉSE**

Felek a jelen Egyezmény értelmezéséből vagy végrehajtásából fakadó vitákat tárgyalás útján, diplomáciai úton kötelesek rendezni.

## **16. CIKK HATÁLYBALÉPÉS**

Jelen Egyezmény az Egyezmény hatálybalépéséhez szükséges belső eljárások teljesítéséről diplomáciai úton küldött utolsó írásbeli értesítés kézhezvételét követő harmincadik napon lép hatályba.

## **17. CIKK MÓDOSÍTÁS**

- (1) Jelen Egyezmény a Felek kölcsönös egyetértésével írásban módosítható.
- (2) A módosítások hatálybalépésével kapcsolatban a jelen Egyezmény 16. cikkében foglaltak az irányadók.

## 18. CIKK TARTAM ÉS FELMONDÁS

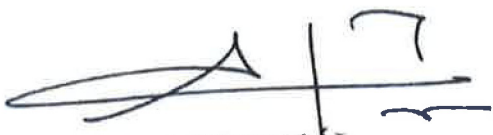
- (1) Jelen Egyezmény határozatlan ideig hatályban marad.
- (2) Bármelyik Fél jogosult a jelen Egyezményt bármikor felmondani.
- (3) Felmondás esetén az Egyezmény a felmondásról szóló írásbeli, diplomáciai úton küldött értesítés kézhezvételétől számított hat hónap elteltével veszti hatályát.
- (4) Az Egyezmény megszűnésétől függetlenül az annak alapján átadott valamennyi minősített adatot az Egyezményben meghatározott rendelkezések szerint kell védelemben részesíteni mindaddig, amíg az átadó Fél írásban, diplomáciai úton felmentést nem ad az átvevő Fél részére e kötelezettség alól.

## 19. CIKK REGISZTRÁCIÓ

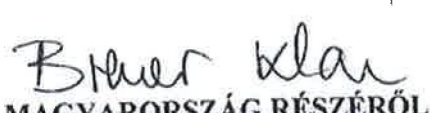
Jelen Egyezmény hatálybalépését követően azon Fél, amelynek területén az Egyezmény aláírása történik, az Egyesült Nemzetek Alapokmánya 102. cikke alapján megküldi az Egyezményt az Egyesült Nemzetek Szervezetének Titkárságára, és tájékoztatja a másik Felet az eljárás befejezéséről, megjelölve a megfelelő regisztrációs számot.

Fentiek tanúbizonyságául, az alulírott és az erre felhatalmazott megbízottak jelen Egyezményt aláírásukkal látták el.

Készült Lisszabon -n, 2018. június 28 -án, két eredeti példányban portugál, magyar és angol nyelven, valamennyi szöveg egyaránt hiteles. Eltérő értelmezés esetén az angol nyelvű szöveg az irányadó.



A PORTUGÁL  
KÖZTÁRSASÁG  
RÉSZÉRŐL



MAGYARORSZÁG RÉSZÉRŐL

### AGREEMENT BETWEEN THE PORTUGUESE REPUBLIC AND HUNGARY ON EXCHANGE AND MUTUAL PROTECTION OF CLASSIFIED INFORMATION

The Portuguese Republic and the Hungary (hereinafter referred to as "Parties"):

Recognising the importance of mutual co-operation between the Parties;

Realising that good co-operation may require exchange of classified information between the Parties;

Recognising that both Parties ensure equivalent protection for classified information;

Wishing to ensure the protection of classified information exchanged between them or between the legal entities or individuals under their jurisdiction:

Have, in mutual respect for their national interests and security, agreed upon the following:

#### Article 1

##### Scope of application

This Agreement sets out rules for the protection of classified information exchanged between the Parties or between the legal entities or individuals under their jurisdiction, in accordance with the respective Law of the Parties.

## Article 2

## Definitions

For the purpose of this Agreement:

- a) “Breach of security” means an act or an omission contrary to the respective Law of the Parties, which may lead to unauthorised disclosure, loss, destruction, misappropriation, access or any other type of compromise of classified information;
- b) “Classified contract” means an arrangement that contains or requires access to classified information, creating and defining enforceable rights and obligations;
- c) “Classified information” means any information that, regardless of its form or nature, requires protection against breach of security and has been duly designated;
- d) “Contractor” means a legal entity or an individual possessing the legal capacity to conclude classified contracts;
- e) “Facility security clearance” means the determination by a national security authority that a legal entity or an individual, possessing legal capacity, has the physical and organizational capability to handle and store classified information;
- f) “National security authority” means the state authority responsible for security and safeguarding of classified information as well as for the application of this Agreement;
- g) “Need-to-know” means the principle, according to which access to classified information may only be granted to a person who has a verified need to access classified information in connection with his/her official duties or for the performance of a specific task;
- h) “Originating party” means the Party, including the legal entities or individuals under its jurisdiction, which releases classified information to the other Party;
- i) “Personnel security clearance” means the determination by a national security authority that an individual is eligible to have access to classified information;
- j) “Receiving party” means the Party, including the legal entities or individuals under its jurisdiction, which receives classified information from the originating party;
- k) “Sub-contract” means a contract between a contractor and another contractor (sub-contractor) creating and defining enforceable rights and obligations;
- l) “Sub-contractor” means a legal entity or an individual possessing the legal capacity to conclude classified contracts, to whom a contractor gives a sub-contract;
- m) “Third party” means any international organisation or State that is not a Party to this Agreement.

## Article 3

## National security authorities

1 — The national security authorities of the Parties are:

a) For the Portuguese Republic:

Autoridade Nacional de Segurança, Presidência do Conselho de Ministros (National Security Authority, Presidency of the Council of Ministers);

b) For Hungary:

Nemzeti Biztonsági Felügyelet (National Security Authority).

2 — The Parties shall inform each other, in writing through diplomatic channels of any change regarding to the designation of the national security authorities.

3 — The national security authorities shall provide each other with official contact details and shall inform each other of any subsequent changes.

4 — Any change regarding to the national security authorities shall not constitute an amendment to this Agreement.

**Article 4****Security classification levels**

The equivalence of the respective security classification levels is as follows:

| For Hungary                | For the Portuguese Republic | Terms in the English language |
|----------------------------|-----------------------------|-------------------------------|
| „Szigorúan titkos!”        | Muito Secreto               | Top Secret.                   |
| „Titkos!”                  | Secreto                     | Secret.                       |
| „Bizalmas!”                | Confidencial                | Confidential.                 |
| „Korlátozott terjesztésű!” | Reservado                   | Restricted.                   |

**Article 5****Access to classified information**

Access to classified information under this Agreement shall be limited to individuals with a need-to-know, who are duly authorised and briefed of their responsibilities to protect such information.

**Article 6****Security principles**

1 — The originating party shall:

- a) Ensure that classified information is marked with appropriate classification markings;
- b) Inform the receiving party of any conditions for the use of classified information;
- c) Inform the receiving party in writing without undue delay of any subsequent changes in the classification level or duration of classification.

2 — The receiving party shall:

- a) Ensure that classified information is marked with the equivalent classification marking in accordance with article 4 of this Agreement;
- b) Afford the same degree of protection to classified information as afforded to its own classified information of equivalent classification level;
- c) Ensure protection of the classified information equivalent to its classification level until the written notification from the originating party about the declassification or the change of the classification level or the validity of the classified information;
- 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 conditions for release 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 their respective Law concerning the exchange and protection of classified information.

2 — On request, the national security authorities shall assist each other during the personnel security clearance procedures and facility security clearance procedures.

3 — On request, the Parties shall recognise the personnel security clearances and facility security clearances issued by the other Party.

4 — The national security authorities shall promptly notify each other about changes in the recognised personnel security clearances and facility security clearances, especially in case of their withdrawal.

5 — The co-operation under this Agreement shall be effected in the English language.

## **Article 8**

### **Classified contracts**

1 — In case of classified contracts marked „Bizalmas!”/Confidencial/Confidential and above, implemented in the territory of one of the Parties, the national security authority of the other Party shall deliver prior written assurance that the proposed contractor holds a facility security clearance of an appropriate security classification level.

2 — The contractor or subcontractor shall ensure that all persons with access to classified information are informed of their responsibility towards the protection of classified information.

3 — The national security authorities may request each other to carry out a security inspection in a facility located in the territory of the other Party in order to ensure continuing compliance with security standards.

4 — Representatives of the national security authorities may visit each other in order to analyse the efficiency of the measures adopted by a contractor for the protection of classified information involved in a classified contract.

5 — Classified contract concluded between contractors of the Parties under the provisions of this Agreement shall include appropriate project security instructions identifying, at least, the following aspects:

- a) List of classified information involved in the classified contract and their security classification;
- b) Procedure for the communication of alteration in the security classification of information;
- c) Communication channels and means for electromagnetic transmission;
- d) Procedure for the transportation of classified information;
- e) Obligation to notify any actual or suspected unauthorized disclosure, misappropriation or loss of classified information.

6 — A copy of the project security instructions of a classified contract shall be forwarded to the national security authority of the Party where the classified contract is to be performed to allow adequate security supervision and control.

## **Article 9**

### **Transmission of classified information**

1 — Classified information shall be transmitted through diplomatic channels unless otherwise agreed in writing between the national security authorities.

2 — The national security authority of the receiving party shall confirm, in writing, the receipt of the classified information.

## **Article 10**

### **Reproduction, translation and destruction of classified information**

1 — Reproductions and translations of classified information released under this Agreement shall bear appropriate classification markings and shall be protected as the originals. The number of reproductions shall be limited to that required for official purposes.

2 — Translations of classified information released under this Agreement shall bear a note in the language of translation indicating that they contain classified information of the originating party.



3 — Classified information released under this Agreement marked „Szigorúan titkos!”/Muito Secreto/Top Secret shall be reproduced or translated only upon prior written consent of the originating party.

4 — Classified information released under this Agreement marked „Szigorúan titkos!”/Muito Secreto/Top Secret shall not be destroyed and shall be returned to the originating party.

5 — In case of a situation in which it is impossible to protect or to return the classified information to the originating party, it shall be destroyed without undue delay. The national security authority of the receiving party shall notify the national security authority of the originating party in writing of the destruction of the classified information.

## Article 11

### Visits

1 — With exception of visits entailing access to classified information marked as „Korlátozott terjesztésű!”/Reservado/Restricted which may be arranged directly between security officers of the entities concerned, visits entailing access to classified information are subject to prior written consent given by the national security authority of the host Party.

2 — The national security authority of the visiting Party shall notify the national security authority of the host Party about the planned visit through a request for visit at least twenty days before the visit takes place.

3 — In urgent cases, the request for visit shall be submitted at least seven days in advance.

4 — The request for visit shall contain the following:

- a) Name of the visitor, date and place of birth, nationality and passport/ID card number;
- b) Position of the visitor and specification of the organisation represented;
- c) Personnel security clearance level of the visitor and its validity;
- d) Date and duration of the visit and in case of recurring visits the total period of time covered by the visits;
- e) Purpose of the visit including the highest classification level of classified information involved;
- f) Name and address of the facility to be visited, as well as the name, phone/fax number, e-mail address of its point of contact;
- g) Date, signature and stamping of the official seal of the national security authority.

5 — The national security authority of the host Party shall inform, in due time, the national security authority of the visiting Party about the decision.

6 — Visit of individuals from a third party entailing access to classified information of the originating party shall only be authorized by a written consent of the national security authority of the originating party.

7 — The national security authority of the host Party shall provide a copy of the approved request for visit to the security officers of the entity to be visited.

8 — The validity of the visit authorization shall not exceed twelve months.

9 — The Parties may agree to establish a list of authorized persons to make recurring visits, which shall be valid for an initial period of twelve months.

10 — Once the Parties have approved the list for recurring visits, the terms of the specific visits shall be directly arranged with the security officers of the entities to be visited.

11 — Any classified information acquired by a visitor shall be considered as classified information released under this Agreement.

## Article 12

### Breach of security

1 — The national security authorities shall, without undue delay, inform each other in writing of any breach of security or suspicion thereof.



2 — The national security authority of the Party where the breach of security has occurred shall investigate the incident without undue delay. The national security authority of the other Party shall, if required, co-operate in the investigation.

3 — In any case, the national security authority of the receiving party shall inform the national security authority of 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**

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

#### **Article 14**

##### **Other international obligations**

The provisions of this Agreement shall not affect the rights and obligations arising from other international conventions, to which they are Party.

#### **Article 15**

##### **Settlement of disputes**

Any dispute regarding the interpretation or implementation of this Agreement shall be settled by negotiations between the Parties, through diplomatic channels.

#### **Article 16**

##### **Entry into force**

This Agreement shall enter into force on the thirtieth day following the receipt of the last written notification through diplomatic channels, stating that all the internal procedures necessary to that effect have been fulfilled.

#### **Article 17**

##### **Amendment**

1 — The Parties may amend this Agreement on the basis of mutual written consent.

2 — The amendments shall enter into force according to the terms specified in article 16 of this Agreement.

#### **Article 18**

##### **Duration and termination**

1 — This Agreement shall remain in force for an indeterminate period of time.

2 — Each Party may, at any time, terminate this Agreement.

3 — The termination shall be notified, in writing and through diplomatic channels, producing its effects six months after the date of the receipt of the respective notification.

4 — Notwithstanding the termination, all classified information released under this Agreement shall continue to be protected according to the provisions set forth herein, until the originating party dispenses the receiving party from this obligation, in writing and through diplomatic channels.

**Article 19****Registration**

Upon the entry into force of this Agreement, the Party in which territory it is signed shall transmit it for registration to the Secretariat of the United Nations, according to article 102 of the Charter of the United Nations, and shall notify the other Party of the conclusion of this proceeding, indicating the respective number of registration.

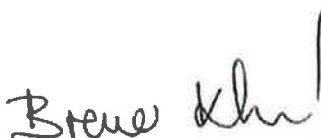
In witness whereof the undersigned, duly authorised to this effect, have signed this Agreement.

Done in Lisbon, on 28<sup>th</sup> of June 2018, in two originals, in hungarian, portuguese and english languages, each text being equally authentic. In case of any divergence of interpretation the english text shall prevail.

For the Portuguese Republic:



For Hungary:



113851157