PRESIDÊNCIA DO CONSELHO DE MINISTROS

Decreto n.º 11/2023

de 31 de maio

Sumário: Aprova o Acordo entre a República Portuguesa e a República de Chipre sobre a Troca e a Proteção Mútua de Informação Classificada, assinado em Nicósia em 8 de outubro de 2022.

O Acordo entre a República Portuguesa e a República de Chipre sobre a Troca e a Proteção Mútua de Informação Classificada foi assinado em Nicósia em 8 de outubro de 2022.

O presente Acordo tem por objeto estabelecer as regras para garantir a proteção da informação classificada que é gerada ou mutuamente trocada entre as Partes.

O referido Acordo representa um contributo para o reforço da 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 República de Chipre sobre a Troca e a Proteção Mútua de Informação Classificada, assinado em Nicósia em 8 de outubro de 2022, cujo texto, nas versões autênticas, nas línguas portuguesa, grega e inglesa, se publica em anexo.

Visto e aprovado em Conselho de Ministros de 27 de abril de 2023. — *Mariana Guimarães Vieira da Silva — Paulo Alexandre Nascimento Cafôfo.*

Assinado em 11 de maio de 2023.

Publique-se.

O Presidente da República, Marcelo Rebelo de Sousa.

Referendado em 18 de maio de 2023.

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

ACORDO ENTRE A REPÚBLICA PORTUGUESA E A REPÚBLICA DE CHIPRE SOBRE A TROCA E A PROTEÇÃO MÚTUA DE INFORMAÇÃO CLASSIFICADA

A República Portuguesa e a República de Chipre, doravante designadas por «Partes»:

Reconhecendo a necessidade de estabelecer normas para proteção da informação classificada mutuamente trocada no interesse da segurança nacional no âmbito de qualquer forma e área de cooperação, bem como qualquer informação classificada gerada no processo dessa cooperação;

Pretendendo assegurar a proteção mútua da informação classificada, que tenha sido classificada por uma Parte e transferida para a outra Parte no âmbito da cooperação entre as Partes;

Desejando estabelecer um conjunto de regras sobre a proteção mútua da informação classificada trocada entre as Partes;

Considerando o mútuo interesse na proteção da informação classificada de acordo com o Direito nacional das Partes:

acordam no seguinte:

Artigo 1.º

Objetivo

O objetivo do presente Acordo é garantir a proteção da informação classificada que é gerada ou mutuamente trocada entre as Partes.

Artigo 2.º

Definições

Para os efeitos do presente Acordo:

a) «Informação classificada» designa a informação, qualquer que seja a sua forma ou natureza, que necessita de proteção contra acesso não autorizado ou manipulação, à qual tenha sido atribuído um nível de classificação de segurança de acordo com o Direito nacional das Partes;

b) «Autoridade nacional de segurança (ANS)» designa a autoridade estatal de cada Parte, a qual de acordo com o Direito nacional respetivo é responsável pela implementação e supervisão do presente Acordo;

c) «Quebra de segurança» designa uma ação contrária ou omissão ao presente Acordo ou ao respetivo Direito nacional das Partes que possa levar à divulgação não autorizada, perda, destruição, apropriação indevida ou qualquer outro tipo de comprometimento da informação classificada;

d) «Contrato classificado» designa um acordo entre dois ou mais cocontratantes ou subcontratados, que contém ou envolve acesso, ou criação, de informação classificada;

e) «Autoridade de segurança competente» designa a autoridade competente das Partes, que não a ANS, que de acordo com o Direito respetivo das Partes é responsável pela implementação do presente Acordo;

f) «Cocontratante» designa uma pessoa singular ou coletiva que tem capacidade jurídica para celebrar e empreender contratos classificados;

g) «Credenciação de segurança física» designa a decisão positiva pela autoridade nacional de segurança de que uma pessoa singular ou coletiva tem a capacidade física e organizacional para manusear e armazenar informação classificada de acordo com o respetivo Direito nacional de ambas as Partes;

h) «Necessidade de conhecer» designa o princípio segundo o qual o acesso a informação classificada é concedido exclusivamente no âmbito de um determinado cargo oficial e para o desempenho de uma tarefa especifica;

i) «Parte transmissora» designa a Parte que cria ou disponibiliza a informação classificada à Parte destinatária;

j) «Credenciação de segurança pessoal» designa a decisão positiva da autoridade nacional de segurança confirmando, de acordo com o Direito nacional respetivo das Partes, que uma pessoa singular está autorizada a aceder e manusear a informação classificada até um nível de classificação específico;

k) «Parte Destinatária» designa a Parte à qual a informação classificada é transmitida;

l) «Terceira Parte» designa qualquer Estado, organização, pessoa coletiva ou singular que não é Parte no presente Acordo.

Artigo 3.º

Níveis de classificação de segurança

As Partes acordam que os seguintes níveis e marcas de classificações de segurança são equivalentes e correspondem aos níveis de classificação de segurança previstos no Direito nacional respetivo:

Para a República Portuguesa	Para a República de Chipre	Equivalente em inglês
Muito secreto.	Ακρωσ απορρητο.	Top secret.
Secreto.	Απορρητο.	Secret.
Confidencial.	Εμπιστευτικο.	Confidential.
Reservado.	Περιορισμενησ χρησησ.	Restricted.

Artigo 4.º

Autoridades de segurança

1 — As autoridades nacionais de segurança das Partes são:

Pela República Portuguesa:

Autoridade nacional de segurança:

Presidência do Conselho de Ministros;

Pela República de Chipre:

Autoridade nacional de segurança:

Ministério da Defesa da República de Chipre.

2 — As autoridades nacionais de segurança informar-se-ão mutuamente, por escrito e por via diplomática, sobre qualquer alteração de designação das autoridades nacionais de segurança.

3 — As autoridades nacionais de segurança fornecem uma à outra os seus contactos oficiais e informam-se de quaisquer alterações subsequentes.

4 — Quaisquer alterações relativas às autoridades nacionais de segurança não constituirão uma revisão deste Acordo.

5 — As autoridades nacionais de segurança informam-se mutuamente do respetivo Direito nacional sobre informação classificada e sobre quaisquer alterações significativas ao mesmo e devem trocar informações sobre as normas, procedimentos e práticas de segurança para a proteção da informação classificada.

Artigo 5.º

Medidas de proteção e acesso à informação classificada

1 — Em conformidade com o Direito respetivo as Partes adotam as medidas necessárias à proteção da informação classificada criada ou trocada no âmbito do presente Acordo.

2 — As Partes atribuem à informação classificada criada ou disponibilizada no âmbito do presente Acordo o mesmo nível de proteção que atribuem à sua informação classificada com o equivalente nível de classificação de segurança como tal previsto no artigo 3.º do presente Acordo.

3 — A Parte Transmissora informa por escrito:

a) A Parte Destinatária de quaisquer condições de liberação ou limitações ao uso da informação classificada;

b) A Parte Destinatária de alterações ao nível de classificação da informação classificada transmitida.

4 — A informação classificada só é acessível às pessoas singulares ou coletivas que de acordo com o Direito nacional respetivo estão autorizadas a aceder a informação classificada de equivalente nível de segurança e de acordo com a necessidade de conhecer.

5 — No âmbito do presente Acordo, cada Parte reconhece a credenciação de segurança pessoal e a credenciação de segurança física atribuídas pela outra Parte.

6 — As autoridades nacionais de segurança de acordo com o Direito nacional respetivo assistem-se mutuamente, mediante solicitação, na realização dos procedimentos de verificação necessários para a aplicação do presente Acordo.

7 — No âmbito do presente Acordo, as autoridades de segurança das Partes informam-se mutuamente e sem demora sobre qualquer alteração relacionada com as credenciações de segurança física ou pessoal, em particular sobre a sua revogação/caducidade ou abaixamento de nível.

8 — A Parte Destinatária:

a) Libera informação classificada para uma Terceira Parte somente após o recebimento do consentimento prévio por escrito da Parte Transmissora;

b) Marca a informação classificada em conformidade com o artigo 3.º do presente Acordo;
c) Usa a informação classificada apenas com o intuito para que a mesma foi fornecida.

9 — Mediante solicitação da autoridade nacional de segurança da Parte Transmissora, a autoridade nacional de segurança da Parte Destinatária emite uma confirmação por escrito de que determinada pessoa tem o direito de aceder a informação classificada.

10 — As autoridades de segurança competentes das Partes, dentro do espírito de boa vontade de cooperação mútua e compreensão, podem visitar-se mutuamente para discutir e trocar pontos de vista, experiências, lições aprendidas e conhecimentos técnicos nas áreas de segurança física, segurança eletrónica, segurança industrial, procedimentos de verificação e quaisquer outras questões relacionadas com a segurança da informação classificada.

11 — O acesso à informação classificada de ambas as Partes por pessoas singulares de uma Terceira Parte só é autorizado após consentimento por escrito da autoridade nacional de segurança da Parte Transmissora.

Artigo 6.º

Transmissão da informação classificada

1 — A informação classificada é transmitida entre as Partes, de acordo com o Direito nacional da Parte Transmissora, normalmente por via diplomática, ou por qualquer outro meio decidido entre as autoridades de segurança competentes.

2 — A Parte Destinatária confirmará, por escrito, a receção da informação classificada.

3 — A informação classificada com o nível de Akρωσ απορρhto/Muito secreto/Top secret é transmitida pelos Governos através de canais do Governo de acordo com o Direito nacional das Partes.

4 — Como requisito mínimo de segurança, informação classificada com o nível de Akρωσ απορρhto/Muito secreto/Top secret deve ser transportada por, e sob o controlo exclusivo de um correio do Governo que possua uma credenciação de segurança pessoal do mesmo nível.

5 — A Parte Destinatária confirma por escrito a receção da informação classificada de nível Akρωσ απορρhto/Muito secreto/Top secret.

6 — A informação classificada com o nível Απορρhto/Secreto/Secret ou Εμπιστeytiko/Confidencial/Confidential é transmitida pelos Governos através de canais do Governo de acordo com o Direito nacional das Partes, ou através de outros canais seguros mutuamente aprovados pelas autoridades nacionais de segurança de ambas as Partes.

7 — A Parte Destinatária confirma por escrito a receção da informação classificada nível Απορρhto/Secreto/Secret ou Εμπιστeytiko/Confidencial/Confidential.

8 — A informação classificada nível Περιορισμενhσ χρhσhσ/Reservado/Restricted é transmitida através de canais seguros de acordo com o Direito nacional das Partes.

9 — Os procedimentos para o transporte de grandes remessas contendo informação classificada serão acordados e avaliados conjuntamente, caso a caso, pela autoridade nacional de segurança de ambas as Partes.

10 — Se a informação classificada nível Απορρhto/Secreto/Secret, Εμπιστευτικο/Confidencial/Confidential ou Περιορισμενhσ χρhσhσ/Reservado/Restricted for transmitida eletronicamente entre as Partes, não é enviada em texto claro.

11 — A transmissão eletrónica dos níveis específicos de classificação referidos no número anterior deve ser efetuada através de meios criptográficos certificados mutuamente aprovados pelas autoridades nacionais de segurança.

12 — Os principais pontos de entrada e saída da informação classificada trocada nos termos do presente Acordo são:

Para a República Portuguesa:

O Registo Central do Gabinete Nacional de Segurança;

Para a República de Chipre:

Central Top Secret Registry do Ministério dos Negócios Estrangeiros.

13 — Sem prejuízo do disposto no n.º 12 deste artigo, sempre que seja considerado necessário, pelas forças de segurança, forças militares ou pela polícia, o intercâmbio de informação classificada, esse intercâmbio será efetuado de acordo com o respetivo Direito nacional das Partes.

14 — Os principais pontos de entrada e saída para esta categoria de informação classificada serão acordados pelas forças de segurança, forças militares ou pela polícia, mediante prévio consentimento e aprovação por escrito pelas autoridades nacionais de segurança das Partes.

Artigo 7.º

Reprodução e tradução da informação classificada

1 — As traduções e reproduções da informação classificada são efetuadas em conformidade com o Direito nacional da Parte Destinatária e com os seguintes procedimentos:

a) As traduções e as reproduções são marcadas e protegidas da mesma forma que a informação classificada original;

b) As traduções e o número de reproduções são limitados ao necessário para fins oficiais;

c) As traduções têm uma anotação apropriada na língua de tradução indicando que contém informação classificada recebida da Parte Transmissora.

2 — A informação classificada marcada com nível Απορρhto/Secreto/Secret ou Ακρωσ απορρhto/Muito secreto/Top secret só é traduzida ou reproduzida mediante prévia permissão por escrito da Parte Transmissora.

Artigo 8.º

Destruição da informação classificada

1 — A informação classificada é destruída de forma a prevenir a sua reconstrução total ou parcial.

2 — A informação classificada marcada com nível até Απορρhto/Secreto/Secret é destruída de acordo com o Direito nacional das Partes.

3 — A informação classificada com nível Ακρωσ απορρhto/Muito secreto/Top secret não é destruída e será devolvida à autoridade nacional de segurança da Parte Transmissora.

4 — Deve ser elaborado um relatório da destruição da informação classificada sendo a sua tradução em inglês enviada à autoridade nacional de segurança da Parte Transmissora.

5 — Em caso de situação de crise na qual seja impossível proteger ou devolver informação classificada esta é imediatamente destruída sendo a autoridade nacional de segurança da Parte Transmissora informada dessa destruição pela Parte Destinatária com a brevidade possível.

Artigo 9.º

Contratos classificados

1 — A autoridade nacional de segurança duma Parte entregará à autoridade nacional de segurança da outra Parte uma garantia escrita prévia de que o cocontratante ou subcontratado que deseja empreender um contrato classificado de nível Εμπιστευτικο/Confidencial/Confidential e Απορρhto/Secreto/Secret detém ou está em processo de obtenção de uma credenciação de segurança física de nível de classificação de segurança apropriado.

2 — A autoridade nacional de segurança duma Parte pode solicitar à outra uma inspeção de segurança numa instalação situada no território da outra Parte por forma a assegurar o contínuo cumprimento dos padrões de segurança em conformidade com o respetivo Direito nacional.

3 — Cada contrato classificado em conformidade com o presente Acordo tem de incluir:

a) Um compromisso de cumprir as disposições do presente Acordo;

b) Um compromisso do cocontratante ou subcontratado de garantir que as suas instalações têm as condições necessárias para o manuseio e armazenamento de informações classificadas de um determinado nível de classificação de segurança;

c) Um compromisso do cocontratante ou subcontratado garantindo que as pessoas que desempenham funções que requerem acesso a informação classificada estão devidamente autorizadas de acordo com o respetivo Direito nacional para ter acesso a informação classificada do nível de classificação de segurança equivalente e tenham sido regularmente instruídas sobre segurança;

d) Uma lista da informação classificada envolvida e uma lista das áreas onde vai ser manuseada e armazenada;

e) Os procedimentos para o transporte da informação classificada;

f) Os canais de comunicação e meios para transmissão eletrónica;

g) Um compromisso do cocontratante ou subcontratado de notificar a sua autoridade nacional de segurança de qualquer quebra de segurança real ou suspeita;

h) Um compromisso do cocontratante ou subcontratado de encaminhar uma cópia do contrato classificado à autoridade nacional de segurança de ambas as Partes.

4 — A credenciação de segurança física e a credenciação de segurança pessoal não são necessárias para os contratos classificados cuja informação classificada seja limitada ao nível de classificação de Περιορισμενης χρησης/Reservado/Restricted.

5 — Os contratos classificados a que se refere o n.º 4 deste artigo contêm uma cláusula de exigência de segurança adequada definindo o requisito mínimo de segurança a ser aplicado pelo cocontratante à informação classificada que é gerada e/ou fornecida como resultado do contrato.

6 — A cláusula de segurança a que se refere o n.º 5 deste artigo inclui uma disposição relativa à nomeação, pelo cocontratante, de uma pessoa que tem a responsabilidade geral pela proteção da informação classificada marcada com o nível Περιορισμενης χρησης/Reservado/Restricted.

7 — Uma cópia da cláusula de exigência de segurança a que se refere o n.º 6 deste artigo deverá ser fornecida à autoridade nacional de segurança, somente mediante solicitação.

Artigo 10.º

Visitas

1 — As visitas relacionadas com contratos classificados e que envolvam acesso a informação classificada estão sujeitas a autorização prévia por escrito (aprovação) conferida pela autoridade nacional de segurança da Parte visitada.

2 — A autoridade nacional de segurança da Parte visitada tem de receber o pedido de visita com pelo menos 20 dias de antecedência.

3 — Em casos urgentes, o pedido de visita é submetido num prazo mais curto.

4 — O pedido de visita inclui:

a) O nome e o apelido do visitante, o local e a data de nascimento, a nacionalidade, o número do passaporte ou do documento de identificação;

b) O nome da pessoa coletiva que o visitante representa ou a que pertence e o cargo que detém;

c) Nome, morada e informação de contacto da entidade e das instalações que irão ser visitadas;

d) Confirmação da credenciação de segurança pessoal do visitante, da sua validade e do seu nível;

e) Objeto e propósito da visita e qual o mais elevado nível de classificação de segurança da informação classificada envolvido;

f) Data e duração previstas para a visita solicitada e, em caso de visitas recorrentes, o período total abrangido pelas mesmas deverá ser referido;

g) A data, a assinatura e o selo oficial da autoridade nacional de segurança.

5 — Assim que a visita for autorizada, a autoridade nacional de segurança da Parte anfitriã providenciará uma cópia do pedido de visita ao encarregado de segurança da entidade a ser visitada.

6 — A validade da autorização de visita não excederá os 12 meses.

7 — A autoridade nacional de segurança da Parte que recebe o pedido de visita informará, assim que possível, a autoridade nacional de segurança da Parte requerente sobre a sua decisão.

8 — As autoridades nacionais de segurança das Partes podem acordar estabelecer listas de pessoas autorizadas a efetuar visitas recorrentes as quais serão válidas por um período de 12 meses, podendo mediante acordo ser alargadas por um novo período que não exceda mais 12 meses.

9 — Os termos das respetivas visitas são acertados diretamente com os pontos de contacto adequados da entidade a visitar, nos termos e condições acordados.

Artigo 11.º

Quebra de segurança

1 — Em caso de quebra de segurança ou suspeita de tal, a autoridade nacional de segurança da Parte onde ocorreu informa, sem demora e por escrito, a autoridade nacional de segurança da Parte Transmissora e inicia os procedimentos apropriados de acordo com as leis e regulamentos nacionais, a fim de determinar as circunstâncias da quebra de segurança, a extensão dos danos e as medidas adotadas para sua mitigação.

2 — Se uma quebra de segurança ocorrer numa Terceira Parte, a autoridade nacional de segurança da Parte que divulgou a informação à Terceira Parte toma todas as medidas necessárias para garantir que as ações prescritas no n.º 1 deste artigo são iniciadas.

3 — A Parte Transmissora, mediante solicitação, coopera na investigação de acordo com o n.º 1 deste artigo.

4 — A Parte Transmissora é informada dos resultados da investigação e receberá o relatório final sobre as causas e o grau dos danos.

Artigo 12.º

Despesas

Cada Parte assume as despesas que para si advenham da aplicação do presente Acordo e respetiva supervisão.

Artigo 13.º

Solução de controvérsias

Qualquer controvérsia sobre a interpretação ou aplicação do presente Acordo será solucionada através de negociação entre as Partes, por via diplomática.

Artigo 14.º

Revisão

1 — O presente Acordo pode ser objeto de revisão com base no mútuo consentimento escrito das Partes.

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

Artigo 15.º

Vigência e denúncia

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

2 — Qualquer das Partes poderá, a qualquer momento, denunciar o presente Acordo mediante notificação escrita à outra Parte por via diplomática.

3 — O presente Acordo cessa a sua vigência seis meses após a data da receção da notificação acima mencionada.

4 — Não obstante a denúncia do presente Acordo, as Partes asseguram que toda a informação classificada continuará a ser protegida até que a Parte Transmissora dispense a Parte Destinatária desta obrigação.

Artigo 16.º

Entrada em vigor

O presente Acordo entrará em vigor no primeiro dia do segundo mês após a data de recebimento da última notificação escrita pela qual as Partes se notificaram, por via diplomática, de que os requisitos legais nacionais necessários para sua entrada em vigor foram cumpridos.

Artigo 17.º

Registo

Após a entrada em vigor do presente Acordo, a Parte em cujo território o Acordo for 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 respetivo número de registo.

Feito em Nicósia, aos 8 de outubro de 2022, em dois originais, cada um nas línguas portuguesa, grega e inglesa, sendo todos os textos autênticos. Em caso de divergência de interpretação o texto na língua inglesa prevalecerá.

Pela República Portuguesa:

João Gomes Cravinho, Ministro dos Negócios Estrangeiros.

Pela República de Chipre:

Charalambos Petrides, Ministro da Defesa.

ΣΥΜΦΩΝΙΑ
ΜΕΤΑΞΥ
ΤΗΣ ΠΟΡΤΟΓΑΛΙΚΗΣ ΔΗΜΟΚΡΑΤΙΑΣ
ΚΑΙ
ΤΗΣ ΚΥΠΡΙΑΚΗΣ ΔΗΜΟΚΡΑΤΙΑΣ
ΓΙΑ ΤΗΝ ΑΝΤΑΛΛΑΓΗ ΚΑΙ ΑΜΟΙΒΑΙΑ ΠΡΟΣΤΑΣΙΑ
ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ

Η Πορτογαλική Δημοκρατία,
και η **Κυπριακή Δημοκρατία**

εφεξής καλούμενες «τα Μέρη»,

Αναγνωρίζοντας την ανάγκη για τον καθορισμό κανόνων σχετικά με την προστασία Διαβαθμισμένων Πληροφοριών, τις οποίες ανταλλάσσουν προς το συμφέρον της εθνικής ασφάλειας στο πλαίσιο οποιασδήποτε μορφής και τομέα συνεργασίας, καθώς και οποιωνδήποτε Διαβαθμισμένων Πληροφοριών που προκύπτουν από τη διαδικασία της εν λόγω συνεργασίας,

Σκοπεύοντας να διασφαλίσουν την αμοιβαία προστασία των Διαβαθμισμένων Πληροφοριών, οι οποίες διαβαθμίστηκαν από το ένα μέρος και διαβιβάστηκαν στο άλλο μέρος στο πλαίσιο συνεργασίας μεταξύ των Μερών,

Επιθυμώντας να θεσπίσουν κανόνες για την αμοιβαία προστασία των Διαβαθμισμένων Πληροφοριών, τις οποίες ανταλλάσσουν τα Μέρη μεταξύ τους,

Λαμβάνοντας υπόψη το αμοιβαίο συμφέρον της προστασίας των Διαβαθμισμένων Πληροφοριών, σύμφωνα με τη νομοθεσία των Μερών,

Συμφώνησαν ως ακολούθως:

Άρθρο 1
Σκοπός

Σκοπός της παρούσας Συμφωνίας είναι η διασφάλιση της προστασίας Διαβαθμισμένων Πληροφοριών, τις οποίες παράγουν ή ανταλλάσσουν μεταξύ τους τα Μέρη.

Άρθρο 2

Ορισμοί

Για τους σκοπούς της παρούσας Συμφωνίας:

α) **«Διαβαθμισμένες Πληροφορίες»** σημαίνει κάθε πληροφορία, ανεξαρτήτως τύπου ή φύσεως, η οποία χρήζει προστασίας από μη εξουσιοδοτημένη πρόσβαση ή χειρισμό και διαβαθμίστηκε με κάποιο επίπεδο διαβάθμισης ασφαλείας, σύμφωνα με την εθνική νομοθεσία των Μερών,

β) **«Εθνική Αρχή Ασφαλείας»** σημαίνει την αρχή κάθε Μέρους, η οποία σύμφωνα με την εθνική νομοθεσία του είναι υπεύθυνη για τη γενική εφαρμογή και εποπτεία της παρούσας Συμφωνίας,

γ) **«Παραβίαση Ασφαλείας»** σημαίνει πράξη ή παράλειψη, η οποία αντιβαίνει στην παρούσα Συμφωνία ή στην εθνική νομοθεσία των Μερών και το αποτέλεσμα της οποίας ενδέχεται να οδηγήσει σε γνωστοποίηση, απώλεια, καταστροφή, παράνομη χρήση ή οποιαδήποτε άλλη διαρροή Διαβαθμισμένων Πληροφοριών,

δ) **«Διαβαθμισμένη Σύμβαση»** σημαίνει κάθε συμφωνία μεταξύ δύο ή περισσοτέρων εργολάβων ή υπεργολάβων και η οποία περιέχει ή περιλαμβάνει πρόσβαση σε Διαβαθμισμένες Πληροφορίες ή δημιουργία Διαβαθμισμένων Πληροφοριών,

ε) **«Αρμόδια Αρχή Ασφαλείας»** σημαίνει οποιαδήποτε αρμόδια αρχή των Μερών πλην των Εθνικών Αρχών Ασφαλείας, η οποία, σύμφωνα με την εθνική νομοθεσία των Μερών, είναι υπεύθυνη για την εφαρμογή της παρούσας Συμφωνίας,

στ) **«Εργολάβος»** σημαίνει το φυσικό ή νομικό πρόσωπο που έχει τη νομική ικανότητα σύναψης ή ανάληψης διαβαθμισμένων συμβάσεων,

ζ) **«Εξουσιοδότηση Ασφαλείας Φορέα»** σημαίνει τη θετική απόφαση της Εθνικής Αρχής Ασφαλείας, η οποία επιβεβαιώνει ότι κάποιο φυσικό ή νομικό πρόσωπο έχει την τεχνική και οργανωτική ικανότητα να χειρίζεται και να αποθηκεύει Διαβαθμισμένες Πληροφορίες, σύμφωνα με την αντίστοιχη εθνική νομοθεσία και των δύο Μερών,

η) **«Ανάγκη για γνώση»** σημαίνει την αρχή βάσει της οποίας παρέχεται πρόσβαση σε συγκεκριμένες Διαβαθμισμένες Πληροφορίες αποκλειστικά στο πλαίσιο συγκεκριμένης επίσημης θέσης και για την εκτέλεση συγκεκριμένης εργασίας,

θ) **«Μέρος Αποστολέας»** σημαίνει το Μέρος, το οποίο δημιουργεί και παρέχει Διαβαθμισμένες Πληροφορίες στο Μέρος Παραλήπτη,

ι) **«Εξουσιοδότηση Ασφαλείας Προσωπικού»** σημαίνει τη θετική απόφαση της Εθνικής Αρχής Ασφαλείας, η οποία επιβεβαιώνει, σύμφωνα με την αντίστοιχη εθνική νομοθεσία των Μερών, ότι κάποιο φυσικό πρόσωπο εξουσιοδοτείται να έχει πρόσβαση σε και να χειρίζεται Διαβαθμισμένες Πληροφορίες έως κάποιο συγκεκριμένο επίπεδο διαβάθμισης,

ια) **«Μέρος Παραλήπτης»** σημαίνει το Μέρος, στο οποίο διαβιβάζονται Διαβαθμισμένες Πληροφορίες,

ιβ) **«Τρίτο Μέρος»** σημαίνει οποιοδήποτε κράτος, οργανισμό, νομικό ή φυσικό πρόσωπο, το οποίο δεν είναι συμβαλλόμενο μέρος στην παρούσα Συμφωνία.

Άρθρο 3

Επίπεδα Διαβάθμισης Ασφαλείας

Τα Μέρη συμφωνούν ότι, τα ακόλουθα Επίπεδα Διαβάθμισης Ασφαλείας και διαβαθμίσεις ισοδυναμούν και αντιστοιχούν στα Επίπεδα Διαβάθμισης Ασφαλείας, τα οποία ορίζονται από την αντίστοιχη εθνική τους νομοθεσία:

Για την Πορτογαλική Δημοκρατία	Για την Κυπριακή Δημοκρατία	Αντίστοιχη αγγλική ορολογία
MUITO SECRETO	ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	TOP SECRET
SECRETO	ΑΠΟΡΡΗΤΟ	SECRET
CONFIDENCIAL	ΕΜΠΙΣΤΕΥΤΙΚΟ	CONFIDENTIAL
RESERVADO	ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	RESTRICTED

Άρθρο 4

Αρχές Ασφαλείας

1. Οι Εθνικές Αρχές Ασφαλείας των Μερών είναι:

Για την Πορτογαλική Δημοκρατία:

Εθνική Αρχή Ασφαλείας

Προεδρία του Υπουργικού Συμβουλίου

Για την Κυπριακή Δημοκρατία:

Εθνική Αρχή Ασφαλείας

Υπουργείο Άμυνας της Κυπριακής Δημοκρατίας

2. Οι Εθνικές Αρχές Ασφαλείας αλληλοενημερώνονται γραπτώς, μέσω της διπλωματικής οδού, για τυχόν αλλαγές που αφορούν στις Εθνικές Αρχές Ασφαλείας.

3. Οι Εθνικές Αρχές Ασφαλείας ανταλλάσσουν τα επίσημα στοιχεία επικοινωνίας τους και αλληλοενημερώνονται για τυχόν μεταγενέστερες αλλαγές.

4. Τυχόν αλλαγές αναφορικά με τις Εθνικές Αρχές Ασφαλείας δεν αποτελούν τροποποίηση της παρούσας Συμφωνίας.

5. Οι Εθνικές Αρχές Ασφαλείας αλληλοενημερώνονται για την αντίστοιχη εθνική νομοθεσία περί Διαβαθμισμένων Πληροφοριών και για τυχόν σημαντικές τροποποιήσεις σε αυτή και ανταλλάσσουν πληροφορίες σχετικά με τα πρότυπα, τις διαδικασίες και πρακτικές που αφορούν στην προστασία Διαβαθμισμένων Πληροφοριών.

Άρθρο 5

Μέτρα Προστασίας και Πρόσβαση σε Διαβαθμισμένες Πληροφορίες

1. Σύμφωνα με την εθνική τους νομοθεσία, τα Μέρη λαμβάνουν όλα τα κατάλληλα μέτρα για την προστασία Διαβαθμισμένων Πληροφοριών, τις οποίες δημιουργούν ή ανταλλάσσουν βάσει της παρούσας Συμφωνίας.

2. Τα Μέρη θα παρέχουν στις Διαβαθμισμένες Πληροφορίες, οι οποίες παράγονται ή και παρέχονται βάσει της παρούσας Συμφωνίας, το ίδιο επίπεδο ασφαλείας, όπως προβλέπεται για τις εθνικές τους Διαβαθμισμένες Πληροφορίες του αντίστοιχου Επιπέδου Διαβάθμισης Ασφαλείας, σύμφωνα με το Άρθρο 3 της παρούσας Συμφωνίας.

3. Το Μέρος Αποστολέας ενημερώνει γραπτώς:

α) το Μέρος Παραλήπτη για τυχόν προϋποθέσεις κυκλοφορίας ή περιορισμούς στη χρήση των Διαβαθμισμένων Πληροφοριών,

β) το Μέρος Παραλήπτη για τυχόν αλλαγή στο Επίπεδο Διαβάθμισης Ασφαλείας των διαβιβασθέντων Διαβαθμισμένων Πληροφοριών.

4. Η πρόσβαση σε Διαβαθμισμένες Πληροφορίες περιορίζεται μόνο σε φυσικά ή νομικά πρόσωπα που εξουσιοδοτούνται σύμφωνα με την αντίστοιχη εθνική νομοθεσία να έχουν πρόσβαση σε Διαβαθμισμένες Πληροφορίες του αντίστοιχου επιπέδου διαβάθμισης ασφαλείας και βάσει της αρχής της ανάγκης για γνώση.

5. Στο πλαίσιο της παρούσας Συμφωνίας, κάθε Μέρος αναγνωρίζει τις Εξουσιοδοτήσεις Ασφαλείας Προσωπικού και Εξουσιοδοτήσεις Ασφαλείας Φορέα, οι οποίες εκδίδονται από το άλλο Μέρος.

6. Οι Εθνικές Αρχές Ασφαλείας, κατόπιν αιτήματος και σύμφωνα με την αντίστοιχη εθνική τους νομοθεσία, αλληλοβοηθούνται στη διεξαγωγή των διαδικασιών ελέγχου ασφαλείας, οι οποίες απαιτούνται για την εφαρμογή της παρούσας Συμφωνίας.

7. Στο πλαίσιο της παρούσας Συμφωνίας, οι Εθνικές Αρχές Ασφαλείας των Μερών αλληλοενημερώνονται χωρίς καθυστέρηση σχετικά με τυχόν αλλαγές στις Εξουσιοδοτήσεις Ασφαλείας Προσωπικού και Εξουσιοδοτήσεις Ασφαλείας Φορέα, και πιο συγκεκριμένα όταν πρόκειται για την απόσυρση ή την υποβάθμισή του Επιπέδου Διαβάθμισης Ασφαλείας.

8. Το Μέρος Παραλήπτης:

α) Υποβάλλει Διαβαθμισμένες Πληροφορίες σε τυχόν τρίτο μέρος μόνο κατόπιν γραπτής συγκατάθεσης του Μέρους Αποστολέα,

β) Διαβαθμίζει την παραληφθείσα πληροφορία σύμφωνα με το Άρθρο 3 της παρούσας Συμφωνίας,

γ) Χρησιμοποιεί Διαβαθμισμένες Πληροφορίες μόνο για τους σκοπούς για τους οποίους προβλέπονται.

9. Κατόπιν αιτήματος της Εθνικής Αρχής Ασφαλείας του Μέρους Αποστολέα, η Εθνική Αρχή Ασφαλείας του Μέρους Παραλήπτη εκδίδει γραπτή επιβεβαίωση ότι συγκεκριμένο άτομο έχει δικαίωμα πρόσβασης σε Διαβαθμισμένες Πληροφορίες.

10. Οι Αρμόδιες Αρχές Ασφαλείας των Μερών, εντός του πνεύματος καλής θέλησης για αμοιβαία συνεργασία και κατανόηση, δύνανται να ανταλλάζουν επισκέψεις για να συζητούν και να ανταλλάζουν απόψεις, εμπειρίες, διδάγματα και τεχνική γνώση στους τομείς της φυσικής, ηλεκτρονικής και βιομηχανικής ασφάλειας, των διαδικασιών ελέγχου ασφαλείας και οποιαδήποτε άλλα θέματα σχετίζονται με την ασφάλεια Διαβαθμισμένων Πληροφοριών.

11. Η πρόσβαση σε Διαβαθμισμένες Πληροφορίες και των δύο Μερών από φυσικά πρόσωπα Τρίτου Μέρους επιτρέπεται μόνο κατόπιν γραπτής συγκατάθεσης της Εθνικής Αρχής Ασφαλείας του Μέρους Αποστολέα.

Άρθρο 6

Διαβίβαση Διαβαθμισμένων Πληροφοριών

1. Οι Διαβαθμισμένες Πληροφορίες διαβιβάζονται μεταξύ των Μερών, σύμφωνα με την εθνική νομοθεσία του Μέρους Αποστολέα, κανονικά μέσω της διπλωματικής οδού, ή διαφορετικά σύμφωνα με τρόπο που συμφωνούν οι Αρμόδιες Αρχές Ασφαλείας μεταξύ τους.

2. Το Μέρος Παραλήπτης επιβεβαιώνει γραπτώς τη λήψη Διαβαθμισμένων Πληροφοριών.

3. Πληροφορίες με Επίπεδο Διαβάθμισης Ασφαλείας ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / MUITO SECRETO / TOP SECRET διαβιβάζονται μέσω κυβερνητικής οδού σύμφωνα με την εθνική νομοθεσία των Μερών.

4. Ως ελάχιστο επίπεδο ασφαλείας, πληροφορίες με Επίπεδο Διαβάθμισης Ασφαλείας ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / MUITO SECRETO / TOP SECRET μεταφέρονται από και υπό τον αποκλειστικό έλεγχο κυβερνητικού μεταφορέα, ο οποίος κατέχει Εξουσιοδότηση Ασφαλείας Προσωπικού στο ίδιο επίπεδο.

5. Το Μέρος Παραλήπτης επιβεβαιώνει γραπτώς τη λήψη πληροφοριών με Επίπεδο Διαβάθμισης Ασφαλείας ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / MUITO SECRETO / TOP SECRET.

6. Πληροφορίες με Επίπεδο Διαβάθμισης Ασφαλείας ΑΠΟΡΡΗΤΟ / SECRETO / SECRET ή ΕΜΠΙΣΤΕΥΤΙΚΟ / CONFIDENCIAL / CONFIDENTIAL διαβιβάζονται μέσω κυβερνητικής οδού σύμφωνα με την εθνική νομοθεσία των Μερών, ή μέσω άλλης ασφαλούς οδού, την οποία έχουν εγκρίνει αμοιβαία οι Εθνικές Αρχές Ασφαλείας και των δύο Μερών.

7. Το Μέρος Παραλήπτης επιβεβαιώνει γραπτώς τη λήψη πληροφοριών με Επίπεδο Διαβάθμισης Ασφαλείας ΑΠΟΡΡΗΤΟ / SECRETO / SECRET και ΕΜΠΙΣΤΕΥΤΙΚΟ / CONFIDENCIAL / CONFIDENTIAL.

8. Πληροφορίες με Επίπεδο Διαβάθμισης Ασφαλείας ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ / RESERVADO / RESTRICTED διαβιβάζονται μέσω ασφαλούς οδού σύμφωνα με την εθνική νομοθεσία των Μερών.

9. Οι διαδικασίες για τη μεταφορά μεγάλων φορτίων που περιέχουν Διαβαθμισμένες Πληροφορίες αξιολογούνται και συμφωνούνται από κοινού από τις Εθνικές Αρχές Ασφαλείας, για κάθε περίπτωση ξεχωριστά.

10. Εάν πληροφορίες με Επίπεδο Διαβάθμισης Ασφαλείας ΑΠΟΡΡΗΤΟ / SECRETO / SECRET, ΕΜΠΙΣΤΕΥΤΙΚΟ / CONFIDENCIAL / CONFIDENTIAL ή ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ / RESERVADO / RESTRICTED πρόκειται να διαβιβαστούν ηλεκτρονικά μεταξύ των Μερών, δεν αποστέλλονται υπό μορφή απλού κειμένου.

11. Η ηλεκτρονική διαβίβαση τέτοιων συγκεκριμένων Επιπέδων Διαβάθμισης Ασφαλείας γίνεται μέσω πιστοποιημένων κρυπτογραφικών μέσων, τα οποία έχουν εγκριθεί αμοιβαία από τις Εθνικές Αρχές Ασφαλείας.

12. Τα κύρια σημεία εισόδου και εξόδου Διαβαθμισμένων Πληροφοριών τις οποίες ανταλλάσσουν τα Μέρη στο πλαίσιο της παρούσας Συμφωνίας είναι:

Για την Πορτογαλική Δημοκρατία:
Το Κεντρικό Μητρώο της Εθνικής Αρχής Ασφαλείας.

Για την Κυπριακή Δημοκρατία:
Η Κεντρική Γραμματεία ΑΚΡΩΣ ΑΠΟΡΡΗΤΩΝ του Υπουργείου Εξωτερικών.

13. Τηρουμένης της Παραγράφου 12 του παρόντος Άρθρου, όποτε η ανταλλαγή Διαβαθμισμένων Πληροφοριών κρίνεται αναγκαία από τις Δυνάμεις Ασφαλείας, το Στρατό ή την Αστυνομία, η ανταλλαγή αυτή θα γίνεται σύμφωνα με την εθνική νομοθεσία των Μερών.

14. Τα κύρια σημεία εισόδου και εξόδου για αυτή την κατηγορία Διαβαθμισμένων Πληροφοριών θα συμφωνούνται από τις Δυνάμεις Ασφαλείας, το Στρατό ή την Αστυνομία, κατόπιν γραπτής συγκατάθεσης και έγκρισης των Εθνικών Αρχών Ασφαλείας των Μερών.

Άρθρο 7

Αναπαραγωγή και Μετάφραση Διαβαθμισμένων Πληροφοριών

1. Οι μεταφράσεις και οι αναπαραγωγές Διαβαθμισμένων Πληροφοριών θα γίνονται σύμφωνα με την εθνική νομοθεσία του Μέρους Παραλήπτη και με τις ακόλουθες διαδικασίες:

α) Οι μεταφράσεις και οι αναπαραγωγές διαβαθμίζονται και προστατεύονται όπως και οι πρωτότυπες Διαβαθμισμένες Πληροφορίες,

β) Οι μεταφράσεις και ο αριθμός των αντιγράφων περιορίζονται στον αριθμό που απαιτείται για επίσημους σκοπούς,

γ) Οι μεταφράσεις φέρουν κατάλληλη σημείωση στη γλώσσα μετάφρασης υποδεικνύοντας ότι περιέχουν Διαβαθμισμένες Πληροφορίες που λήφθηκαν από το Μέρος Αποστολέα.

2. Πληροφορίες με Επίπεδο Διαβάθμισης Ασφαλείας ΑΠΟΡΡΗΤΟ / SECRETO / SECRET ή ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / MUITO SECRETO / TOP SECRET μεταφράζονται ή αναπαράγονται μόνο κατόπιν γραπτής συγκατάθεσης του Μέρους Αποστολέα.

Άρθρο 8

Καταστροφή Διαβαθμισμένων Πληροφοριών

1. Οι Διαβαθμισμένες Πληροφορίες καταστρέφονται με τέτοιο τρόπο ώστε να αποφεύγεται η μερική ή ολική ανακατασκευή τους.

2. Οι πληροφορίες που έχουν διαβαθμιστεί έως το Επίπεδο Διαβάθμισης Ασφαλείας ΑΠΟΡΡΗΤΟ / SECRETO / SECRET καταστρέφονται σύμφωνα με την εθνική νομοθεσία των Μερών.

3. Οι πληροφορίες με Επίπεδο Διαβάθμισης Ασφαλείας ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / MUITO SECRETO / TOP SECRET δεν καταστρέφονται. Επιστρέφονται στην Εθνική Αρχή Ασφαλείας του Μέρους Αποστολέα.

4. Συντάσσεται έκθεση για την καταστροφή των Διαβαθμισμένων Πληροφοριών και η μετάφρασή της στην αγγλική γλώσσα παραδίδεται στην Εθνική Αρχή Ασφαλείας του Μέρους Αποστολέα.

5. Σε περίπτωση κατάστασης κρίσης κατά την οποία δεν είναι δυνατή η προστασία ή η επιστροφή Διαβαθμισμένων Πληροφοριών, αυτές καταστρέφονται αμέσως. Το Μέρος Παραλήπτης ενημερώνει την Εθνική Αρχή Ασφαλείας του Μέρους Αποστολέα σχετικά με την εν λόγω καταστροφή το συντομότερο δυνατόν.

Άρθρο 9

Διαβαθμισμένες Συμβάσεις

1. Η Εθνική Αρχή Ασφαλείας του ενός Μέρους παρέχει, εκ των προτέρων, στην Εθνική Αρχή Ασφαλείας του άλλου Μέρους γραπτή επιβεβαίωση ότι, ο εργολάβος ή ο υπεργολάβος που επιθυμεί να συνάψει διαβαθμισμένη σύμβαση με Επίπεδο Διαβάθμισης Ασφαλείας ΕΜΠΙΣΤΕΥΤΙΚΟ / CONFIDENCIAL / CONFIDENTIAL και ΑΠΟΡΡΗΤΟ / SECRETO /SECRET, διαθέτει ή έχει κινήσει διαδικασίες για την εξασφάλιση Εξουσιοδότηση Ασφαλείας Φορέα στο κατάλληλο Επίπεδο Διαβάθμισης Ασφαλείας.

2. Κάθε Εθνική Αρχή Ασφαλείας δύναται να ζητήσει από την άλλη να διεξάγει επιθεώρηση ασφαλείας στις εγκαταστάσεις που βρίσκονται στην επικράτεια του κράτους τους για να διασφαλίσει τη συνεχιζόμενη συμμόρφωση με τα πρότυπα ασφαλείας σύμφωνα με την αντίστοιχη εθνική νομοθεσία.

3. Κάθε Διαβαθμισμένη Σύμβαση που συνάπτεται σύμφωνα με την παρούσα Συμφωνία περιλαμβάνει:

α) Δέσμευση συμμόρφωσης με τις πρόνοιες της παρούσας Συμφωνίας,

β) Δέσμευση του εργολάβου ή του υπεργολάβου με την οποία διασφαλίζεται ότι, τα υποστατικά του πληρούν τις απαραίτητες προϋποθέσεις για χειρισμό και αποθήκευση Διαβαθμισμένων Πληροφοριών ενός συγκεκριμένου Επιπέδου Διαβάθμισης Ασφαλείας,

γ) Δέσμευση του εργολάβου ή του υπεργολάβου με την οποία διασφαλίζεται ότι, όλα τα άτομα που εκτελούν καθήκοντα τα οποία απαιτούν πρόσβαση σε Διαβαθμισμένες Πληροφορίες είναι δεόντως εξουσιοδοτημένα, σύμφωνα με την εθνική τους νομοθεσία, να έχουν πρόσβαση σε Διαβαθμισμένες Πληροφορίες με το αντίστοιχο Επίπεδο Διαβάθμισης Ασφαλείας και ότι ενημερώνονται τακτικά σε θέματα ασφαλείας,

δ) Κατάλογο των Διαβαθμισμένων Πληροφοριών και των χώρων χειρισμού και αποθήκευσης Διαβαθμισμένων Πληροφοριών,

ε) Τη διαδικασία μεταφοράς Διαβαθμισμένων Πληροφοριών,

στ) Οδούς επικοινωνίας και μέσα ηλεκτρονικής διαβίβασης,

ζ) Δέσμευση του εργολάβου ή του υπεργολάβου να ενημερώνει τις αντίστοιχες Εθνικές Αρχές Ασφαλείας του για τυχόν πραγματική ή ενδεχόμενη Παραβίαση Ασφαλείας,

η) Δέσμευση του εργολάβου ή του υπεργολάβου να προωθήσει αντίγραφο της Διαβαθμισμένης Σύμβασης στις Εθνικές Αρχές Ασφαλείας και των δύο Μερών.

4. Δεν απαιτείται Εξουσιοδότηση Ασφαλείας Φορέα ούτε και Εξουσιοδότηση Ασφαλείας Προσωπικού για Διαβαθμισμένες Συμβάσεις που περιορίζονται σε πληροφορίες με Επίπεδο Διαβάθμισης Ασφαλείας ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ / RESERVADO / RESTRICTED.

5. Οι Διαβαθμισμένες Συμβάσεις που αναφέρονται στην Παράγραφο 4 του παρόντος Άρθρου περιέχουν κατάλληλη ρήτρα απαίτησης ασφαλείας, η οποία ορίζει την ελάχιστη απαίτηση ασφαλείας που πρέπει να εφαρμοστεί από τον εργολάβο σε Διαβαθμισμένες Πληροφορίες που παράγονται ή και παρέχονται ως αποτέλεσμα της Σύμβασης.

6. Η ρήτρα ασφαλείας που αναφέρεται στην Παράγραφο 5 του παρόντος Άρθρου, περιέχει πρόνοια αναφορικά με τον διορισμό, από τον εργολάβο, προσώπου που έχει τη συνολική ευθύνη για την προστασία διαβαθμισμένων πληροφοριών με Επίπεδο Διαβάθμισης Ασφαλείας ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ / RESERVADO / RESTRICTED.

7. Αντίγραφο της πρόνοιας απαίτησης ασφαλείας, η οποία αναφέρεται στην Παράγραφο 6 του παρόντος Άρθρου, παρέχεται στην Εθνική Αρχή Ασφαλείας, μόνο κατόπιν απαίτησης.

Άρθρο 10

Επισκέψεις

1. Οι επισκέψεις που αφορούν σε Διαβαθμισμένες Συμβάσεις και περιλαμβάνουν πρόσβαση σε Διαβαθμισμένες Πληροφορίες υπόκεινται στην εκ των προτέρων γραπτή εξουσιοδότηση (έγκριση), την οποία παρέχει η Εθνική Αρχή Ασφαλείας του Μέρους υποδοχής.

2. Η Εθνική Αρχή Ασφαλείας του Μέρους υποδοχής θα πρέπει να λάβει αίτηση επίσκεψης τουλάχιστον 20 (είκοσι) ημέρες νωρίτερα.

3. Σε έκτακτες περιπτώσεις η αίτηση επίσκεψης μπορεί να διαβιβαστεί εντός συντομότερης προθεσμίας.

4. Η αίτηση επίσκεψης περιλαμβάνει:

α) Το ονοματεπώνυμο του επισκέπτη, τον τόπο και την ημερομηνία γέννησης, την υπηκοότητα και τον αριθμό διαβατηρίου ή εγγράφου ταυτοποίησης,

β) Την επωνυμία του νομικού προσώπου, το οποίο εκπροσωπεί ο επισκέπτης και τη θέση του επισκέπτη στο νομικό πρόσωπο,

γ) Την επωνυμία, τη διεύθυνση και τα στοιχεία επικοινωνίας του νομικού προσώπου και των εγκαταστάσεων που πρόκειται να δεχθούν την επίσκεψη,

δ) Επιβεβαίωση της Εξουσιοδότησης Ασφαλείας Προσωπικού του επισκέπτη, της εγκυρότητάς και του επιπέδου αυτής,

ε) Τον σκοπό και τους λόγους της επίσκεψης, καθώς και το υψηλότερο Επίπεδο Διαβάθμισης Ασφαλείας των Διαβαθμισμένων Πληροφοριών στις οποίες αφορά η επίσκεψη,

στ) Την αναμενόμενη ημερομηνία και διάρκεια της επίσκεψης. Σε περίπτωση επαναλαμβανόμενων επισκέψεων, αναφέρεται η συνολική διάρκεια των επισκέψεων,

ζ) Την ημερομηνία, την υπογραφή και την επίσημη σφραγίδα της Εθνικής Αρχής Ασφαλείας.

5. Μόλις εγκριθεί η επίσκεψη, η Εθνική Αρχή Ασφαλείας του Μέρους υποδοχής παρέχει αντίγραφο της αίτησης επίσκεψης στον λειτουργό ασφαλείας του νομικού προσώπου που πρόκειται να δεχτεί την επίσκεψη.

6. Η ισχύς της έγκρισης επίσκεψης δεν υπερβαίνει τους δώδεκα (12) μήνες.

7. Η Εθνική Αρχή Ασφαλείας του Μέρους που λαμβάνει την αίτηση για επίσκεψη ενημερώνει, εν ευθέτω χρόνω, την Εθνική Αρχή Ασφαλείας του αιτούντος Μέρους σχετικά με την απόφαση.

8. Οι Εθνικές Αρχές Ασφαλείας των Μερών δύνανται να καταρτίσουν καταλόγους με φυσικά πρόσωπα, τα οποία είναι εξουσιοδοτημένα να κάνουν επαναλαμβανόμενες επισκέψεις. Οι κατάλογοι αυτοί ισχύουν για αρχική περίοδο δώδεκα (12) μηνών και κατόπιν συμφωνίας η περίοδος δύναται να παραταθεί για περίοδο που δεν υπερβαίνει τους δώδεκα (12) μήνες.

9. Οι όροι των αντίστοιχων επισκέψεων θα καθορίζονται απευθείας από τα αρμόδια άτομα του νομικού προσώπου που πρόκειται να δεχτεί την επίσκεψη, σύμφωνα με τους όρους και προϋποθέσεις που θα συμφωνηθούν.

Άρθρο 11

Παραβίαση Ασφαλείας

1. Σε περίπτωση πραγματικής ή εικαζόμενης Παραβίασης Ασφαλείας, η Εθνική Αρχή Ασφαλείας του Μέρους όπου συνέβη ενημερώνει γραπτώς και χωρίς καθυστέρηση την Εθνική Αρχή Ασφαλείας του Μέρους Αποστολέα και κινεί τις κατάλληλες διαδικασίες σύμφωνα με την εθνική νομοθεσία και κανονισμούς, για τη διαπίστωση των περιστάσεων της Παραβίασης Ασφαλείας, της έκτασης της ζημιάς και των μέτρων που υιοθετήθηκαν για τον μετριασμό της.

2. Εάν η Παραβίαση Ασφαλείας επέλθει σε Τρίτο Μέρος, η Εθνική Αρχή Ασφαλείας του Μέρους, το οποίο κοινοποίησε τις πληροφορίες στο Τρίτο Μέρος λαμβάνει όλα τα απαραίτητα μέτρα για να διασφαλίσει ότι, οι δράσεις που περιγράφονται στην Παράγραφο 1 του παρόντος Άρθρου έχουν τεθεί σε εφαρμογή.

3. Το Μέρος Αποστολέας, κατόπιν αιτήματος, συνεργάζεται στην έρευνα σύμφωνα με την Παράγραφο 1 του παρόντος Άρθρου.

4. Το Μέρος Αποστολέας ενημερώνεται για τα αποτελέσματα της έρευνας και λαμβάνει την τελική έκθεση για τα αίτια και τον βαθμό της ζημιάς.

Άρθρο 12

Έξοδα

Κάθε Μέρος αναλαμβάνει τα δικά του έξοδα, τα οποία θα προκύψουν από την εφαρμογή και εποπτεία της παρούσας Συμφωνίας.

Άρθρο 13

Διευθέτηση Διαφορών

Τυχόν διαφορές που προκύπτουν από την ερμηνεία ή εφαρμογή της παρούσας Συμφωνίας, διευθετούνται με διαπραγματεύσεις μεταξύ των Μερών μέσω της διπλωματικής οδού.

Άρθρο 14

Τροποποιήσεις

1. Η παρούσα Συμφωνία δύναται να τροποποιείται με την αμοιβαία γραπτή έγκριση των Μερών.
2. Οι τροποποιήσεις τίθενται σε ισχύ σύμφωνα με τους όρους που αναφέρονται στο Άρθρο 16.

Άρθρο 15

Διάρκεια και Τερματισμός

1. Η παρούσα Συμφωνία συνάπτεται για απεριόριστο χρονικό διάστημα.

2. Κάθε Μέρος δύναται, ανά πάσα στιγμή, να τερματίσει τη Συμφωνία δίδοντας στο άλλο Μέρος γραπτή ειδοποίηση μέσω της διπλωματικής οδού.

3. Η Συμφωνία τερματίζεται έξι (6) μήνες μετά την ημερομηνία παραλαβής της προαναφερθείσας ειδοποίησης.

4. Σε περίπτωση τερματισμού της παρούσας Συμφωνίας, τα Μέρη διασφαλίζουν ότι, όλες οι Διαβαθμισμένες Πληροφορίες θα συνεχίσουν να προστατεύονται έως ότου το Μέρος Αποστολέας απαλλάξει το Μέρος Παραλήπτη από την εν λόγω υποχρέωση.

Άρθρο 16
Έναρξη ισχύος

Η παρούσα Συμφωνία τίθεται σε ισχύ την πρώτη ημέρα του δεύτερου μήνα μετά την ημερομηνία λήψης της τελευταίας γραπτής ειδοποίησης με την οποία τα Μέρη ανακοινώνουν το ένα στο άλλο, μέσω της διπλωματικής οδού, ότι πληρούνται όλες οι αναγκαίες εθνικές νομικές προϋποθέσεις που απαιτούνται για την έναρξη ισχύος της παρούσας Συμφωνίας.

Άρθρο 17
Καταχώρηση

Μετά την έναρξη ισχύος της παρούσας Συμφωνίας, το Μέρος στην επικράτεια του οποίου υπεγράφη η παρούσα Συμφωνία τη διαβιβάζει στη Γραμματεία των Ηνωμένων Εθνών προς καταχώρηση, σύμφωνα με το Άρθρο 102 της Χάρτας των Ηνωμένων Εθνών και ενημερώνει το άλλο Μέρος για την ολοκλήρωση της εν λόγω διαδικασίας, καθώς και για τον αριθμό καταχώρησής της.

Συντάχθηκε στη Λευκωσία, στις 08 Οκτωβρίου 2022, σε δύο πρωτότυπα, στην Ελληνική, Πορτογαλική και Αγγλική γλώσσα, και όλα τα κείμενα είναι εξίσου αυθεντικά. Σε περίπτωση διαφωνίας στην ερμηνεία, το αγγλικό κείμενο υπερισχύει.

Για την
Πορτογαλική Δημοκρατία

João Gomes Cravinho
Υπουργός Εξωτερικών

Για την
Κυπριακή Δημοκρατία

Χαράλαμπος Πετρίδης
Υπουργός Άμυνας

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

The Portuguese Republic and the Republic of Cyprus, hereinafter referred to as "the Parties":

Recognizing the need to set rules on protection of classified information mutually exchanged in the interest of national security within the scope of any form and area of co-operation, as well as any classified information generated in the process of such co-operation;

Intending to ensure the mutual protection of classified information, which has been classified by one Party and transferred to the other Party in the course of co-operation between the Parties;

Desiring to create a set of rules on the mutual protection of classified information exchanged between the Parties;

Considering the mutual interest in the protection of classified information, in accordance with the legislation of the Parties:

have agreed as follows:

Article 1

Objective

The objective of this Agreement is to ensure the protection of classified information that is generated or mutually exchanged between the Parties.

Article 2

Definitions

For the purposes of this Agreement:

a) "Classified information" means any information, regardless of its form or nature, which requires protection against unauthorised access or manipulation and for which a security classification level has been assigned, in accordance with the national legislation of the Parties;

b) "National security authority (NSA)" means the state authority of each Party, which in accordance with its national legislation is responsible for the general implementation and supervision of this Agreement;

c) "Breach of security" means an act which is contrary or an omission to this Agreement or to the national legislation of the Parties, the result of which may lead to disclosure, loss, destruction, misappropriation or any other type of compromise of classified information;

d) "Classified contract" means an agreement between two or more contractors or sub-contractors, which contains or involves access to, or the creation of classified information;

e) "Competent security authority" means any competent authority of the Parties other than the NSA's that according to its national legislation, is responsible for the implementation of this Agreement;

f) "Contractor" means a natural person, or a legal entity possessing the legal capacity to conclude or undertake classified contracts;

g) "Facility security clearance" means the positive decision by the national security authority confirming that a natural person or the legal entity has the physical and organisational capability to handle and store classified information in accordance with the respective national legislation of both Parties;

h) "Need-to-know" means the principle whereby access to specific classified information is granted exclusively in the scope of a given official position and for the performance of a specific task;

i) "Providing Party" means the Party that creates or provides classified information to the Receiving Party;

j) "Personnel security clearance" means the positive decision by the national security authority confirming, in accordance with the respective national legislation of the Parties, that a natural person is authorized to have access to and handle classified information up to a specific classification level;

k) "Receiving Party" means the Party to which classified information is transmitted;

l) "Third Party" means any State, organisation, legal or natural person, which is not a party to this Agreement.

Article 3

Security classification levels

The Parties agree that the following security classification levels and markings are equivalent and correspond to the security classification levels specified in their respective national legislation:

For the Portuguese Republic	For the Republic of Cyprus	Equivalent in English
Muito secreto.	Ακρωσ απορρhto.	Top secret.
Secreto.	Απορρhto.	Secret.
Confidencial.	Εμπιστευτικο.	Confidential.
Reservado.	Περιορισμενησ χρησησ.	Restricted.

Article 4

Security authorities

1 — The national security authorities of the Parties are:

For the Portuguese Republic:

National security authority:

Presidency of the Council of Ministers;

For the Republic of Cyprus:

National security authority:

Ministry of Defence of the Republic of Cyprus.

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

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

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

5 — The national security authorities shall inform each other of their respective national legislation on classified information and of any significant amendments thereto and shall exchange information about the security standards, procedures and practices for the protection of classified information.

Article 5

Protection measures and access to classified information

1 — In accordance with their national legislation, the Parties shall take all necessary measures for the protection of classified information that is created or exchanged under this Agreement.

2 — The Parties shall afford to classified information created or provided under this Agreement the same level of protection as they would to their own classified information of the equivalent security classification level, as set forth in article 3 of this Agreement.

3 — The Providing Party shall inform in writing:

a) The Receiving Party of any conditions of release or limitations on the use of the classified information;

b) The Receiving Party about any change of the security classification level of the transmitted classified information.

4 — Classified information shall only be made accessible to natural persons or legal entities who are authorized in accordance with the respective national legislation to have access to classified information of the equivalent security classification level and on a need-to-know basis.

5 — Within the scope of this Agreement, each Party shall recognise the personnel security clearances and facility security clearances issued by the other Party.

6 — The national security authorities shall, in accordance with their respective national legislation, assist each other, upon request, at carrying out vetting procedures necessary for the application of this Agreement.

7 — Within the scope of this Agreement, the security authorities of the Parties shall inform each other without delay about any alteration with regards to personnel and facility security clearances, in particular about their withdrawal or downgrading.

8 — The Receiving Party shall:

a) Release classified information to any Third Party only upon receipt of the prior written consent of the Providing Party.

b) Mark the received classified information in accordance with article 3 of this Agreement;

c) Use classified information solely for the purposes which it has been provided for.

9 — Upon a request of the national security authority of the Providing Party, the national security authority of the Receiving Party shall issue a written confirmation that an individual has the right to access classified information.

10 — The competent security authorities of the Parties, within the spirit of good will for mutual co-operation, and understanding, may visit each other in order to discuss and exchange views, experiences, lessons learned and technical knowledge in the fields of physical security, electronic security, industrial security, vetting procedures and any other issues related to the security of classified information.

11 — Access to classified information of both Parties, by natural persons from a Third Party shall only be authorized after a written consent of the national security authority of the Providing Party.

Article 6

Transmission of classified information

1 — Classified information shall be transmitted between the Parties, in accordance with the national legislation of the Providing Party, normally through the diplomatic channels, or as otherwise arranged between the competent security authorities.

2 — The Receiving Party shall confirm, in writing, the receipt of the classified information.

3 — Classified information marked as Ακρωσ απορρhto/Muito secreto/Top secret shall be transmitted through Government to Government channels in accordance with the national legislations of the Parties.

4 — As a minimum-security requirement classified information marked as Ακρωσ απορρhto/Muito secreto/Top secret shall be carried by, and under the sole control of a Government courier holding a personnel security clearance of the same level.

5 — The Receiving Party shall confirm the receipt of classified information of level Ακρωσ απορρhto/Muito secreto/Top secret in writing.

6 — Classified information marked as Απορρhto/Secreto/Secret or Εμπιστeytiko/Confidencial/Confidential shall be transmitted through Government to Government channels in accordance with the national legislation of the Parties, or through other secure channels mutually approved by the national security authorities of both Parties.

7 — The Receiving Party shall confirm the receipt of Απορρhto/Secreto/Secret and Εμπιστευτικο/Confidencial/Confidential level of classified information in writing.

8 — Classified information marked as Περιορισμενhσ χρhσhσ/Reservado/Restricted shall be transmitted through secure channels in accordance with the national legislation of the Parties.

9 — The procedures for the carriage of large consignments containing classified information shall be jointly agreed and evaluated, on a case-by-case basis, by the national security authority of both Parties.

10 — If classified information marked as Απορρhto/Secreto/Secret, Εμπιστευτικο/Confidencial/Confidential or Περιορισμενhσ χρhσhσ/Reservado/Restricted is to be transmitted electronically between the Parties, it shall not be sent in clear text.

11 — Electronic transmission of the specific classification levels referred in the previous article shall be carried out through certified cryptographic means mutually approved by the national security authorities.

12 — The main points of entry and exit for the classified information exchange under this Agreement shall be:

For the Portuguese Republic:

The Central Registry at the National Security Authority;

For the Republic of Cyprus:

The Central Top Secret Registry at the Ministry of Foreign Affairs.

13 — Without prejudice to paragraph 12 of this article, whenever deemed necessary, by the security forces, the military forces or the police, to exchange classified information, this exchange shall be done in accordance with the national legislation of the Parties.

14 — The main points of entry and exit for this category of classified information shall be agreed by the security forces, military forces, or the police upon a prior written consent and approval of the national security authorities of the Parties.

Article 7

Reproduction and translation of classified information

1 — Translations and reproductions of classified information shall be made in accordance with the national legislation of the Receiving Party and the following procedures:

a) The translations and the reproductions shall be marked and protected as the original classified information;

b) The translations and the number of copies shall be limited to that required for official purposes;

c) The translations shall bear an appropriate annotation in the language of the translation indicating that it contains classified information received from the Providing Party.

2 — Classified information marked as Απορρhto/Secreto/Secret or Ακρωσ απορρhto/Muito secreto/Top secret shall be translated or reproduced only upon the prior written consent of the Providing Party.

Article 8

Destruction of classified information

1 — Classified information shall be destroyed in a way that prevents its partial or total reconstruction.

2 — Classified information marked up to Απορρhto/Secreto/Secret shall be destroyed in accordance with the national legislation of the Parties.

3 — Classified information marked as Ακρωσ απορρhto/Muito secreto/Top secret shall not be destroyed and shall be returned to the national security authority of the Providing Party.

4 — A report on destruction of classified information shall be made and its translation in English shall be delivered to the national security authority of the Providing Party.

5 — In case of a crisis situation in which it is impossible to protect or return classified information it shall be destroyed immediately, and the Receiving Party shall inform the national security authority of the Providing Party about this destruction as soon as possible.

Article 9

Classified contracts

1 — The national security authority of a Party shall provide to the national security authority of the other Party prior written assurance that a contractor or a sub-contractor wishing to undertake a classified contract marked as Εμπιστευτικο/Confidencial/Confidential and Απορρhto/Secreto/Secret, holds or is in the process of obtaining a facility security clearance of the appropriate security classification level.

2 — Each national security authority may request the other to carry out a security inspection in a facility located in their State's territory in order to ensure continuing compliance with security standards according to the respective national legislation.

3 — Each classified contract in accordance with this Agreement shall include:

a) A commitment to comply with the provisions of the present Agreement;

b) A commitment of the contractor or sub-contractor to ensure that their premises have necessary conditions for handling and storing classified information of a given security classification level;

c) A commitment of the contractor or sub-contractor to ensure that persons who perform duties requiring access to classified information are duly authorised in accordance with their national legislation to have access to classified information of the equivalent security classification level and have been regularly security briefed;

d) A list of classified information involved and a list of areas in which classified information will be handled and stored;

e) The procedures for the transportation of classified information;

f) Communication channels and means for electronic transmission.

g) A commitment of the contractor or sub-contractor to notify its national security authority of any actual or suspected breach of security;

h) A commitment of the contractor or sub-contractor to forward a copy of the classified contract to the national security authority of both Parties.

4 — A facility security clearance and a personnel security clearance are not required for classified contracts that are limited to classified information marked as Περιορισμενhσ χρhσhσ/Reservado/Restricted.

5 — Classified contracts referred to in paragraph 4 of this article, shall contain an appropriate security requirement clause defining the minimum security requirement to be applied by the contractor to classified information that is generated and/or provided as a result of the contract.

6 — The security clause referred to in paragraph 5 of this article, shall include a provision concerning the appointment, by the contractor, of a person who has the overall responsibility of the protection of classified information marked as Περιορισμενhσ χρhσhσ/Reservado/Restricted.

7 — A copy of the security requirement provision referred to in paragraph 6 of this article shall be provided to the national security authority, only upon request.

Article 10

Visits

1 — Visits related to classified contracts and involving access to classified information are subject to prior written authorisation (approval) given by the national security authority of the host Party.

2 — The national security authority of the host Party shall receive a request for a visit at least 20 (twenty) days in advance.

3 — In urgent cases, the request for a visit is submitted in shorter time.

4 — The request for a visit shall include:

a) The visitor's name and surname, place and date of birth, citizenship, passport or identification document number;

b) The name of the legal person represented by the visitor and position of the visitor in the legal entity;

c) The name, address and contact information of the legal entity and the facility to be visited;

d) The confirmation of the visitor's personnel security clearance, its validity and level;

e) The object and purpose of the visit and the highest security classification level of classified information to be involved;

f) The expected date and duration of the requested visit and, in case of recurring visits, the total period covered by the visits shall be stated;

g) The date, signature and the official seal of the national security authority.

5 — Once the visit has been approved, the national security authority of the host Party shall provide a copy of the request for visit to the security officer of the legal entity to be visited.

6 — The validity of visit approval shall not exceed twelve (12) months.

7 — The national security authority of the Party that receives the request for visit shall inform, in due time, the national security authority of the requesting Party about the decision.

8 — The national security authorities of the Parties may draw up lists of individuals authorised to make recurring visits and shall be valid for an initial period of twelve (12) months and, upon agreement, may be extended for a further period of time not exceeding another twelve (12) months.

9 — The terms of the respective visits shall be directly arranged with the appropriate points of contact in the legal entity to be visited, in accordance with the terms and conditions agreed upon.

Article 11

Breach of security

1 — In case of actual or suspected breach of security, the national security authority of the Party where it has occurred shall inform, without delay and in writing, the national security authority of the Providing Party and initiate appropriate proceedings in accordance with national laws and regulations, in order to determine the circumstances of the breach of security, the extent of the damage and the measures adopted for its mitigation.

2 — If a breach of security occurs in a Third Party, the national security authority of the Party who released the information to the Third Party shall take all necessary measures in order to ensure that the actions prescribed in paragraph 1 of this article are initiated.

3 — The Providing Party shall, upon request, cooperate in the investigation in accordance with paragraph 1 of this article.

4 — The Providing Party shall be informed of the results of the investigation and shall receive the final report on the causes and degree of damage.

Article 12

Expenses

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

Article 13

Settlement of disputes

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

Article 14

Amendments

1 — This agreement may be amended on the basis of mutual written approval of the Parties.
2 — The amendments shall enter into force according to the terms specified in article 16.

Article 15

Duration and termination

1 — This Agreement shall remain in force for an undetermined period.
2 — Each Party may, at any time, terminate this Agreement by written notification to the other Party through diplomatic channels.
3 — The Agreement shall be terminated six (6) months following the date of the receipt of the aforementioned notification.
4 — Notwithstanding the termination of this Agreement, the Parties shall ensure that all classified information shall continue to be protected until the Providing Party exonerates the Receiving Party from this obligation.

Article 16

Entry into force

The present agreement shall enter into force on the first day of the second month after the date of the receipt of the last written notification by which the Parties have notified each other, through diplomatic channels, that their national legal requirements necessary for its entry into force have been fulfilled.

Article 17

Registration

Upon the entry into force of this Agreement, the Party in whose territory this Agreement is signed shall transmit it to the Secretariat of the United Nations for registration, in accordance with article 102 of the Charter of the United Nations and shall notify the other Party of the completion of this procedure as well as of its registration number.

Done at Nicosia on 8 October 2022 in two originals, each in the Portuguese, Greek, and English languages, all texts being equally authentic. In case of any divergence of interpretation, the English text shall prevail.

For the Portuguese Republic:

João Gomes Cravinho, Minister of Foreign Affairs.

For the Republic of Cyprus:

Charalambos Petrides, Minister of Defence.

116498343