ACORDO ENTRE O GOVERNO DA REPÚBLICA FEDERATIVA DO BRASIL E O GOVERNO DA REPÚBLICA DA ESLOVÊNIA SOBRE A TROCA E PROTEÇÃO MÚTUA DE INFORMAÇÕES CLASSIFICADAS

O Governo da República Federativa do Brasil

e

o Governo da República da Eslovênia,
doravante conjuntamente denominadas "Partes" ou individualmente como "Parte ",

No interesse da segurança nacional e com o objetivo de assegurar a proteção das Informações Classificadas trocadas no âmbito de tratados ou contratos de cooperação celebrados entre eles, seus indivíduos, órgãos credenciados, bem como entidades públicas ou privadas,

Desejando estabelecer um conjunto de regras e procedimentos para a proteção de Informações Classificadas de acordo com as leis e regulamentos nacionais das Partes,

Confirmando que este Acordo não afetará os compromissos das Partes decorrentes de outros acordos internacionais e que não será usado contra os interesses, a segurança e a integridade territorial de outros Estados,

Acordaram o seguinte:

ARTIGO 1
OBJETO E ESCOPO DE APLICAÇÃO

Este Acordo estabelece regras e procedimentos para a proteção de Informações Classificadas trocadas e geradas no processo de cooperação, em respeito aos seus interesses e segurança nacionais, entre as Partes, seus indivíduos, órgãos, agências e entidades credenciadas.

ARTIGO 2
DEFINIÇÕES

Para os fins deste Acordo, o termo:

a) **Contrato Classificado**: significa qualquer contrato ou subcontrato, incluindo as negociações pré-contratuais, entre dois ou mais Contratantes que crie e defina direitos e obrigações executáveis entre eles e contenha ou permita o acesso a Informações Classificadas;

b) **Informações Classificadas**: significa as informações que são protegidas contra acesso ou divulgação não autorizados, independentemente de sua forma, natureza e meio de transmissão, são geradas, classificadas e trocadas entre as partes de acordo com as respectivas leis e regulamentos das Partes;

c) **Autoridade de Segurança Competente (ASC)**: significa uma entidade competente autorizada de acordo com as leis e regulamentos nacionais das Partes, que é responsável pela implementação dos requisitos de segurança cobertos por este Acordo;

d) **Comprometimento**: designa qualquer forma de uso indevido, dano ou acesso não autorizado, alteração, divulgação ou destruição de Informações Classificadas, bem como qualquer outra ação ou omissão, devido a uma Violação de Segurança, resultando na perda de sua confidencialidade, integridade, disponibilidade ou autenticidade;

e) **Contratante**: significa um indivíduo, agência ou entidade com capacidade legal para celebrar contratos;

f) **Certificação de Segurança da Instalação (CSI)**: significa uma determinação, por uma ASC das Partes, de que uma entidade pública ou privada, localizada em seu país, possui autorização de segurança e possui medidas de segurança apropriadas dentro de uma instalação específica para o Tratamento de Informações Classificadas, de acordo com as leis e regulamentos nacionais;

g) **Tratamento da Informação Classificada**: designa um conjunto de ações relativas à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivo, armazenamento, eliminação, avaliação, destino ou controle da Informação Classificada a qualquer nível de classificação;

h) **Autoridade Nacional de Segurança (ANS)**: designa o órgão estatal definido pela legislação nacional das Partes, que é especialmente autorizado na esfera de proteção de Informações Classificadas;

i) **"Necessidade de Conhecer"**: designa a condição pela qual o acesso à Informação Classificada pode ser concedido a um indivíduo que tenha uma necessidade verificada de conhecimento ou posse de tal informação, para poder desempenhar funções oficiais;

j) **Parte Originadora:** a Parte, incluindo quaisquer entidades públicas ou privadas sob sua jurisdição, que divulga Informações Classificadas à Parte Receptora;

k) **Credencial de Segurança Pessoal (CSP):** significa uma determinação, por uma ASC de uma Parte, de que um indivíduo obteve autorização de segurança para o Tratamento de Informações Classificadas, de acordo com suas leis e regulamentos nacionais, com base na qual o indivíduo está autorizado a ter acesso e tratar a Informação Classificada até o nível definido na autorização;

l) **Parte Receptora**: significa a Parte para a qual as Informações Classificadas são transmitidas e recebidas, incluindo quaisquer entidades públicas ou privadas sob sua jurisdição;

m) **Violação de Segurança:** significa uma ação ou omissão, intencional ou acidental, que resulta no real ou possível Comprometimento de Informações Classificadas;

n) **Nível de Classificação de Segurança:** significa uma categoria, de acordo com as leis e regulamentos nacionais das Partes, que caracteriza a importância da Informação Classificada, o nível de restrição de acesso a ela e o nível de sua proteção pelas Partes e, também, uma categoria com base nas quais as informações são marcadas;

o) **Credenciamento de Segurança:** designa o processo de emissão de um CSI ou CSP por um ASC, de acordo com as leis e regulamentos nacionais das Partes;

p) **Terceiro:** designa Estados, organizações internacionais, governos ou indivíduos que representam órgãos ou organizações estatais, incluindo quaisquer entidades públicas e privadas, que não sejam Partes deste Acordo; e

q) **Visita:** significa qualquer acesso a entidades públicas e privadas, para efeitos do presente Acordo, que inclui o Tratamento de Informação Classificada.

ARTIGO 3
NÍVEIS DE CLASSIFICAÇÃO DE SEGURANÇA

1. De acordo com as leis e regulamentos nacionais, as Partes concordam que os Níveis de Classificação de Segurança devem corresponder entre si da seguinte forma e ser considerados equivalentes:

NA REPÚBLICA DA ESLOVÊNIA (Esloveno)	**NA REPÚBLICA FEDERATIVA DO BRASIL** (Português)	**NA LÍNGUA INGLESA**
STROGO TAJNO	ULTRASSECRETO	TOP SECRET
TAJNO	SECRETO	SECRET
ZAUPNO		CONFIDENTIAL
INTERNO	RESERVADO	RESTRICTED

2. A Parte brasileira tratará e protegerá as Informações Classificadas da Eslovênia marcadas como " ZAUPNO" de maneira não menos rigorosa do que a assegurada pelas normas e procedimentos relevantes para as Informações Classificadas marcadas como "SECRETO".

3. A Parte Eslovena tratará e protegerá as Informações Classificadas Brasileiras marcadas como "SECRETO" de maneira não menos rigorosa do que a assegurada pelas normas e procedimentos relevantes para as Informações Classificadas marcadas como "TAJNO".

4. Qualquer Informação Classificada fornecida sob este Acordo deve ser marcada com o Nível de Classificação de Segurança apropriado de acordo com as leis e regulamentos nacionais da Parte Originadora e, quando apropriado, ser prefixado com o nome do país que possui e fornece as Informações Classificadas.

5. As Partes devem marcar todas as Informações Classificadas recebidas da outra Parte com um Nível de Classificação de Segurança equivalente de acordo com os parágrafos 1, 2 e 3 deste Artigo.

6. As Partes devem notificar-se mutuamente sobre todas as alterações de classificação subsequentes às Informações Classificadas transmitidas.

7. A Parte Originadora deverá:

a) Sem demora, notificar a Parte Receptora sobre quaisquer alterações no Nível de Classificação de Segurança das Informações Classificadas divulgadas; e

b) Informar a Parte Receptora sobre quaisquer condições de liberação ou limitações no uso de Informações Classificadas.

ARTIGO 4
PROTEÇÃO DE INFORMAÇÕES CLASSIFICADAS

1. As Partes devem tomar todas as medidas apropriadas de acordo com suas respectivas leis e regulamentos nacionais para garantir que o nível de proteção concedido às Informações Classificadas recebidas esteja de acordo com seu Nível de Classificação de Segurança equivalente e garantir que as Informações Classificadas sejam marcadas com uma marcação de segurança de classificação equivalente, de acordo com os parágrafos 1, 2 e 3 do Artigo 3.

2. Nada neste Acordo prejudicará as leis e regulamentos nacionais das Partes em relação aos direitos dos indivíduos de obter acesso a documentos públicos ou acesso às informações de caráter público, à proteção de dados pessoais ou à proteção de Informações Classificadas.

3. De acordo com as leis e regulamentos nacionais, cada Parte deve garantir que medidas apropriadas sejam implementadas para a proteção de Informações Classificadas processadas, armazenadas ou transmitidas em sistemas de comunicação e informação, desde que seja considerado necessário. Tais medidas devem garantir a confidencialidade, integridade, disponibilidade e, quando aplicável, não repúdio e autenticidade das Informações Classificadas, bem como um nível adequado de responsabilidade e rastreabilidade das ações relacionadas a essas informações.

ARTIGO 5
DIVULGAÇÃO E USO DE INFORMAÇÕES CLASSIFICADAS

1. Cada Parte deve garantir que as Informações Classificadas fornecidas ou trocadas sob este Acordo não sejam:

a) Desclassificadas ou rebaixadas sem o consentimento prévio por escrito da Parte Originadora; e

b) Usadas para fins diferentes dos estabelecidos pela Parte Originadora.

2. A Parte Receptora não deve divulgar ou permitir o acesso a Informações Classificadas a Terceiros ou seus nacionais sem o consentimento prévio por escrito da Parte Originadora. Cada Parte deverá, de acordo com seus requisitos constitucionais e legislação nacional, respeitar o princípio do consentimento da Parte Originadora.

ARTIGO 6
ACESSO À INFORMAÇÃO CLASSIFICADA

1. Cada Parte deve assegurar que o acesso à Informação Classificada seja concedido com base no princípio da "Necessidade de Conhecer".

2. Cada Parte deve assegurar que todos os indivíduos que têm acesso a Informações Classificadas sejam informados de suas responsabilidades para proteger essas informações de acordo com os regulamentos de segurança apropriados.

3. As Partes assegurarão que o acesso às Informações Classificadas seja concedido apenas a indivíduos que possuam uma CSP apropriada ou que estejam devidamente autorizados em virtude de suas funções de acordo com a legislação nacional.

4. De acordo com suas leis e regulamentos nacionais, cada Parte deve garantir que qualquer entidade sob sua jurisdição que possa receber ou gerar Informações Classificadas tenha a devida credencial de segurança e seja capaz de fornecer proteção adequada, conforme previsto no parágrafo 1 do Artigo 4 deste Acordo, no nível de segurança apropriado.

ARTIGO 7
TRADUÇÃO, REPRODUÇÃO E DESTRUIÇÃO DE INFORMAÇÃO CLASSIFICADA

1. Todas as traduções e reproduções de Informações Classificadas devem conter o Nível de Classificação de Segurança apropriado e devem ser protegidas e controladas como o original pelas Partes em conformidade.

2. Todas as traduções de Informações Classificadas deverão conter uma anotação adequada, no idioma para o qual foram traduzidas, indicando que contêm Informações Classificadas da Parte Originadora.

3. De acordo com o parágrafo 3 do Artigo 6 deste Acordo, os tradutores devem ter uma CSP apropriada no Nível de Classificação de Segurança da Informação Classificada a ser traduzida.

4. As Informações Classificadas marcadas como ULTRASSECRETO/STROGO TAJNO/TOP SECRET devem ser traduzidas ou reproduzidas somente mediante permissão prévia por escrito da Parte Originadora.

5. O número de reproduções deve ser limitado ao mínimo exigido para fins oficiais e deve ser feito apenas por indivíduos com uma CSP apropriada e uma "Necessidade de Conhecer".

6. As Informações Classificadas não devem ser reproduzidas pela Parte Receptora sem o consentimento prévio por escrito da Parte Originadora.

7. As Informações Classificadas recebidas sob este Acordo não serão destruídas. Quando não for mais considerada necessária pela Parte Receptora, deverão ser devolvidas à Parte Originadora.

ARTIGO 8
TRANSMISSÃO ENTRE AS PARTES

1. As Informações Classificadas serão transmitidas entre as Partes por via diplomática ou conforme acordado pelas Partes.

2. As Informações Classificadas devem ser transmitidas através de sistemas de comunicações protegidos, redes ou outros meios eletromagnéticos aprovados por ambas as Partes. Tais transmissões devem ser protegidas por meios criptográficos mutuamente aceitos pelas Autoridades Nacionais de Segurança de acordo com as leis e regulamentos nacionais.

3. As Informações Classificadas marcadas como ULTRASSECRETO / STROGO TAJNO / TOP SECRET devem ser enviadas apenas por via diplomática.

4. A Parte Receptora não transmitirá Informações Classificadas a Terceiros sem o consentimento prévio por escrito da ANS ou ASC da Parte Originadora.

5. Se uma Parte desejar transmitir Informações Classificadas provenientes da outra Parte fora dos territórios das Partes, tais transmissões estarão sujeitas ao consentimento prévio por escrito da ANS ou ASC da Parte Originadora.

6. No caso de transmissão de grandes remessas contendo Informações Classificadas, os procedimentos para transporte serão acordados e avaliados em conjunto, caso a caso, por ambas as Autoridades Nacionais de Segurança das Partes.

ARTIGO 9
VISITAS

1. As Visitas às instalações onde as Informações Classificadas são tratadas ou armazenadas estarão sujeitas ao consentimento prévio por escrito da ANS da Parte anfitriã, salvo acordo em contrário mutuamente aprovado.

2. Um pedido de Visita deve ser submetido à ANS da Parte anfitriã e deve incluir os seguintes dados que serão utilizados apenas para efeitos da Visita:

a) Nome do visitante, data e local de nascimento, nacionalidade e número da carteira de identidade/passaporte;

b) Cargo e função do visitante, bem como o nome e endereço do estabelecimento onde trabalha;

c) Especificação do projeto no qual o visitante está participando;

d) A validade e nível da CSP do visitante;

e) O nome, endereço, número de telefone, e-mail e ponto de contato do estabelecimento a ser visitado;

f) A finalidade da Visita, incluindo a entidade que se pretende visitar e o mais elevado Nível de Classificação de Segurança da informação Classificada envolvida;

g) A data e a duração da Visita. Para Visitas recorrentes, deve ser informado o período total coberto pelas Visitas;

h) Outros dados, desde que acordados pelas Autoridades Nacional de Segurança; e

i) Data e assinatura.

3. Um pedido de Visita deve ser apresentado pelo menos 30 (trinta) dias antes da data prevista da Visita, salvo acordo mútuo entre as Autoridades de Segurança Competentes.

4. Quaisquer Informações Classificadas divulgadas a um visitante devem ser consideradas como Informações Classificadas recebidas sob este Acordo. Um visitante deve cumprir os regulamentos de segurança da Parte anfitriã.

5. As Visitas serão autorizadas por uma Parte aos visitantes da outra Parte, somente se:

a) Possuir CSP válida concedido pelo país de origem; e

b) Estejam autorizados a receber ou ter acesso à Informação Classificada com base na "Necessidade de Conhecer".

6. Uma vez autorizada a Visita, a ANS do país anfitrião deverá notificar a ANS do país do visitante sobre sua autorização com antecedência mínima de 10 (dez) dias da data prevista para a Visita e fornecer cópia do pedido ao estabelecimento a ser visitado.

7. As Autoridades de Segurança Competentes podem acordar uma lista de visitantes com direito a Visitas recorrentes. A lista será válida por um período inicial não superior a 12 (doze) meses e poderá ser prorrogada por um período adicional de tempo não superior a 12 (doze) meses. A solicitação de Visitas recorrentes deverá ser apresentada de acordo com o parágrafo 3 deste Artigo. Uma vez aprovada a lista, as Visitas podem ser agendadas diretamente entre os estabelecimentos envolvidos.

ARTIGO 10
CONTRATOS CLASSIFICADOS RELACIONADOS A ESTE ACORDO

1. No caso de Contratos Classificados concluídos e implementados no território de uma das Partes, a ANS ou ASC da outra Parte deverá obter garantia prévia, por escrito, de que o Contratante proposto possui uma CSI e as Credenciais de Segurança Pessoais necessárias no nível apropriado.

2. A Contratada se compromete a:

a) Assegurar que as suas instalações dispõem de condições adequadas ao Tratamento de Informação Classificada;

b) Ter a CSI apropriada;

c) Assegurar que todas as pessoas com acesso à Informação Classificada tenham a respectiva CSP e sejam informadas da sua responsabilidade na sua proteção, de acordo com as leis e regulamentos nacionais;

d) Não divulgar, ou permitir a divulgação, das Informações Classificadas a Terceiros não expressamente autorizados por escrito pela Parte Originadora; e

e) Permitir inspeções de segurança às suas instalações.

3. Para cada Contrato Classificado adjudicado, a Parte Originadora deverá informar à Parte Receptora do nível das Informações Classificadas transmitidas.

4. O Contrato Classificado também deve fornecer estes termos adicionais:

a) Responsabilidade pelo descumprimento dos procedimentos e medidas de segurança aplicáveis à Informação Classificada;

b) Obrigação de informar à ASC sobre qualquer Violação de Segurança ou Comprometimento de Informação Classificada; e

c) Responsabilidade pelos danos resultantes da Violação de Segurança.

5. Qualquer subcontratado deve cumprir os mesmos requisitos de segurança que o Contratado.

ARTIGO 11
AUTORIDADES NACIONAIS DE SEGURANÇA E COOPERAÇÃO EM SEGURANÇA

1. As Autoridades Nacionais de Segurança responsáveis pela implementação e supervisão deste Acordo serão:

Na República Federativa do Brasil:
Gabinete de Segurança Institucional da Presidência da República

Na República da Eslovênia:
Escritório do Governo da República da Eslovênia para a Proteção de Informações Classificadas ("Urad Vlade Republike Slovenije za varovanje tajnih podatkov")

2. Cada Parte fornecerá à outra Parte os dados de contato necessários de sua respectiva ANS por escrito.

3. As Autoridades Nacionais de Segurança deverão informar-se mutuamente sobre as respetivas leis e regulamentos nacionais em vigor que regulam a proteção de Informação Classificada.

4. As Autoridades Nacionais de Segurança deverão informar-se mutuamente sobre quaisquer modificações que lhes digam respeito ou relativas às Credenciais de Segurança de indivíduos, agências e entidades.

5. Visando assegurar uma estreita cooperação na implementação deste Acordo, as Autoridades Nacionais de Segurança poderão ser consultadas sempre que solicitadas por uma delas.

6. Os representantes da ANS de uma Parte podem visitar os estabelecimentos da ANS da outra Parte com o intuito de adquirir conhecimento dos procedimentos e medidas de segurança aplicáveis às Informações Classificadas.

7. As Partes, por meio de suas Autoridades Nacionais de Segurança, notificar-se-ão, tempestivamente, sobre qualquer mudança de titularidade de tais órgãos ou transferências de suas competências para outros órgãos, de acordo com o Artigo 20.

8. Se solicitado, as Partes, por meio de suas Autoridades Nacionais de Segurança, tendo em vista as respectivas leis e regulamentos nacionais, colaborarão entre si no curso dos procedimentos necessários para a CSP de seus indivíduos que viveram ou vivem no território da outra parte.

9. As Partes reconhecem mutuamente as Credenciais de Segurança Pessoais e as Certificações de Segurança de Instalações e devem informar-se prontamente sobre quaisquer alterações nas Credenciais de Segurança Pessoais e as Certificações de Segurança de Instalações mutuamente reconhecidas.

10. Para alcançar e manter padrões de segurança comparáveis, as Autoridades de Segurança Competentes devem, mediante solicitação, fornecer informações sobre suas normas de segurança nacional, procedimentos e práticas para a proteção de Informações Classificadas. Se necessário, as Autoridades de Segurança Competentes podem realizar reuniões regulares.

11. Mediante solicitação, as Partes prestarão assistência mútua nos procedimentos para obtenção de Credenciais de Segurança Pessoais.

ARTIGO 12
ASSISTÊNCIA PARA PROCEDIMENTOS DE CREDENCIAMENTO DE SEGURANÇA

1. Mediante solicitação, as Autoridades Nacionais de Segurança das Partes, levando-se em conta suas respectivas leis e regulamentos nacionais, prestarão assistência mútua durante os procedimentos de Credenciamento de Segurança.

2. As Partes reconhecerão as Credenciais de Segurança emitidas de acordo com as leis e regulamentos nacionais da outra Parte.

ARTIGO 13
VIOLAÇÃO DE SEGURANÇA

1. No caso de uma Violação de Segurança relacionada a Informações Classificadas que envolva as Partes deste Acordo, a ANS da Parte onde ocorreu a Violação de Segurança deverá informar imediatamente a ANS da outra Parte.

2. Quando a Violação de Segurança ocorrer em um Terceiro, a ANS da Parte Originadora informará a ANS da outra Parte, o mais rápido possível, e garantirá a devida investigação.

3. A Parte competente deve tomar todas as medidas de acordo com as leis e regulamentos nacionais para limitar as consequências da violação referida no parágrafo 1 deste Artigo e prevenir novas violações. A pedido, a outra Parte prestará assistência adequada; será informada do resultado do processo e das medidas tomadas devido à violação.

4. A Parte onde ocorreu a Violação de Segurança deverá investigar ou acompanhar a investigação do incidente e, ao final, informar imediatamente a outra Parte sobre o resultado da investigação e as medidas corretivas aplicadas.

5. A outra Parte deverá, se necessário, cooperar na investigação.

ARTIGO 14
CUSTOS

Cada Parte arcará com seus próprios custos incorridos pela implementação e supervisão de todos os aspectos deste Acordo.

ARTIGO 15
RESOLUÇÃO DE DIVERGÊNCIAS

1. Qualquer divergência que surja entre as Partes sobre a interpretação ou implementação deste Acordo, ou qualquer assunto relacionado, será resolvida por meio de consultas e negociações entre as Partes por via diplomática.

2. Durante o período de resolução da divergência, as Partes continuarão a cumprir todas as suas obrigações decorrentes do presente Acordo.

ARTIGO 16
COMUNICAÇÃO

Todas as comunicações entre as Partes relacionadas à implementação deste Acordo serão feitas por escrito, em inglês.

ARTIGO 17
ENTRADA EM VIGOR

Este Acordo entrará em vigor no primeiro dia do segundo mês após o recebimento da última notificação, pela qual as Partes tenham informado uma à outra, por via diplomática, que seus requisitos legais internos necessários para sua entrada em vigor foram cumpridos.

ARTIGO 18
ALTERAÇÕES

1. Este Acordo pode ser alterado a qualquer momento, por escrito, por consentimento mútuo das Partes.

2. As emendas entrarão em vigor nos termos do Artigo 17 deste Acordo.

ARTIGO 19
VALIDADE E RESCISÃO

1. Este Acordo permanecerá em vigor por tempo indeterminado.

2. Qualquer Parte pode, a qualquer momento, rescindir este Acordo mediante notificação por escrito à outra Parte.

3. A rescisão deverá ser notificada por escrito pelos canais diplomáticos e entrará em vigor 6 (seis) meses após a data em que a outra Parte tiver recebido a notificação de rescisão.

4. Em caso de rescisão, quaisquer informações Classificadas trocadas de acordo com este Acordo continuarão a ser protegidas de acordo com as disposições aqui estabelecidas, a menos que a Parte Originadora isente a Parte Receptora dessa obrigação.

ARTIGO 20
DISPOSIÇÕES FINAIS

1. As Partes devem notificar imediatamente uma à outra sobre quaisquer alterações em suas respectivas leis e regulamentos nacionais que afetem a proteção de Informações Classificadas divulgadas sob este Acordo. No caso de tais alterações, as Partes deverão consultar-se para considerar possíveis alterações a este Acordo. Enquanto isso, as Informações Classificadas continuarão a ser protegidas conforme descrito neste documento, a menos que solicitado de outra forma por escrito pela Parte Originadora.

2. Após a entrada em vigor deste Acordo, a Parte em cujo território o Acordo for concluído tomará medidas imediatas para que o Acordo seja registrado pelo Secretariado das Nações Unidas de acordo com o Artigo 102 da Carta das Nações Unidas. A outra Parte será notificada do registro e do número de registro na Série de Tratados das Nações Unidas assim que o Secretariado das Nações Unidas notificar que o Acordo foi registrado.

Feito em Rio de Janeiro, em 11 de abril de 2023, em dois exemplares originais, cada um nos idiomas português, esloveno e inglês, sendo todos os textos igualmente autênticos. Em caso de divergências de interpretação, prevalecerá o texto em inglês.

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

PELO GOVERNO DA REPÚBLICA FEDERATIVA DO BRASIL

MARCO EDSON GONÇALVES DIAS
Ministro de Estado Chefe do Gabinete de Segurança Institucional da Presidência da República

PELO GOVERNO DA REPÚBLICA DA ESLOVÊNIA

MARJAN ŠAREC
Ministro da Defesa

AGREEMENT BETWEEN THE GOVERNMENT OF THE FEDERATIVE REPUBLIC OF BRAZIL AND THE GOVERNMENT OF THE REPUBLIC OF SLOVENIA ON THE EXCHANGE AND MUTUAL PROTECTION OF CLASSIFIED INFORMATION

The Government of the Federative Republic of Brazil

and

the Government of the Republic of Slovenia,
hereinafter jointly referred to as the "Parties" or individually as a "Party",

In the interest of national security and for the purpose of ensuring the protection of Classified Information exchanged within the sphere of cooperation treaties or contracts entered into between them, their accredited individuals, bodies, as well as public or private entities,

Wishing to establish a set of rules and procedures for the protection of Classified Information in accordance with the national laws and regulations of the Parties,

Confirming that this Agreement shall not affect the commitments of the Parties which stem from other international agreements and that it shall not be used against the interests, security, and territorial integrity of other States,

Have agreed as follows:

ARTICLE 1
OBJECT AND SCOPE OF APPLICATION

This Agreement establishes rules and procedures for the protection of Classified Information exchanged and generated in the process of cooperation, in respect of their national interests and security, between the Parties, their accredited individuals, bodies, agencies and entities.

ARTICLE 2
DEFINITIONS

For the purpose of this Agreement, the term:

a) **Classified Contract**: means any contract or sub-contract including the pre-contractual negotiations, between two or more Contractors that creates and defines enforceable rights and obligations between them and contains or allows access to Classified Information;

b) **Classified Information**: means the information, regardless of its form, nature, and means of transmission, determined in accordance with the respective laws and regulations of the Parties, protected against unauthorized access or disclosure, which has been classified and is exchanged between, or generated by the Parties;

c) **Competent Security Authority (CSA)**: means a competent entity authorized in accordance with the national laws and regulations of the Parties which is responsible for implementing the security requirements covered by this Agreement;

d) **Compromise**: designates any form of misuse, damage or unauthorized access, alteration, disclosure, or destruction of Classified Information, as well as any other action or omission, due to a Security Breach, resulting in loss of its confidentiality, integrity, availability, or authenticity;

e) **Contractor**: means an individual, agency or entity possessing the legal capacity to conclude contracts;

f) **Facility Security Clearance (FSC)**: means a determination by a CSA of a Party that a public or private entity located in its country is security cleared and has in place appropriate security measures within a specific facility for the Handling of Classified Information, in accordance with the national laws and regulations;

g) **Handling of Classified Information**: designates a set of actions relating to production, reception, classification, use, access, reproduction, transportation, transmission, distribution, archiving, storage, disposal, evaluation, destination, or control of Classified Information at any classification level;

h) **National Security Authority (NSA)**: designates the state body defined by the national legislation of the Parties which is specially authorized in the sphere of protection of Classified Information;

i) **"Need to know"**: designates the condition by which access to Classified Information may be granted to an individual who has a verified requirement for knowledge of or possession of such information in order to be able to perform official duties and tasks;

j) **Originating Party**: the Party, including any public or private entities under its jurisdiction, which releases Classified Information to the Receiving Party;

k) **Personnel Security Clearance (PSC)**: means a determination by a CSA of a Party that an individual has been security cleared for the Handling of Classified Information, in accordance with its national laws and regulations, on the basis of which the individual is authorized to have access to and handle Classified Information up to the level defined in the clearance;

l) **Receiving Party**: means a Party, including any public or private entities under its jurisdiction, to which Classified Information is transmitted and received;

m) **Security Breach**: means an action or omission, whether intentional or accidental, which results in the actual or possible Compromise of Classified Information;

n) **Security Classification Level**: means a category, in accordance with the national laws and regulations of the Parties, which characterizes the importance of Classified Information, the level of restriction of access to it and the level of its protection by the Parties, and also a category on the basis of which information is marked;

o) **Security Clearance**: designates the process for issuing a FSC or PSC by a CSA, in accordance with the national laws and regulations of the Parties;

p) **Third Party**: designates States, international organizations, governments or individuals representing state bodies or organizations, including any public and private entities, which are not Parties to this Agreement; and

q) **Visit**: means any access to public and private entities, for the purpose of this Agreement, which includes the Handling of Classified Information.

ARTICLE 3
SECURITY CLASSIFICATION LEVELS

1. In accordance with the national laws and regulations, the Parties agree that the Security Classification Levels shall correspond to one another as follows and be considered as equivalent:

IN THE REPUBLIC OF SLOVENIA (Slovenian)	**IN THE FEDERATIVE REPUBLIC OF BRAZIL** (Portuguese)	**IN THE ENGLISH LANGUAGE**
STROGO TAJNO	ULTRASSECRETO	TOP SECRET
TAJNO	SECRETO	SECRET
ZAUPNO		CONFIDENTIAL
INTERNO	RESERVADO	RESTRICTED

2. The Brazilian Party will handle and protect Slovenian Classified Information marked as "ZAUPNO" in a manner not less stringent than that ensured by standards and procedures relevant for Classified Information marked as "SECRETO".

3. The Slovenian Party will handle and protect Brazilian Classified Information marked as "SECRETO" in a manner not less stringent than that ensured by standards and procedures relevant for Classified Information marked as "TAJNO".

4. Any Classified Information provided under this Agreement shall be marked with the appropriate Security Classification Level in accordance with the national laws and regulations of the Originating Party and, where appropriate, be prefixed with the name of the country owning and providing the Classified Information.

5. The Parties shall mark all the Classified Information received from the other Party with an equivalent Security Classification Level in accordance with paragraphs 1, 2 and 3 of this Article.

6. The Parties shall notify each other about all subsequent classification alterations to the transmitted Classified Information.

7. The Originating Party shall:

a) Without delay, notify the Receiving Party of any changes to the Security Classification Level of the released Classified Information; and

b) Inform the Receiving Party of any conditions of release or limitations on the use of Classified Information.

ARTICLE 4
PROTECTION OF CLASSIFIED INFORMATION

1. The Parties shall take all appropriate measures in accordance with their respective national laws and regulations to ensure that the level of protection granted to Classified Information received shall be in accordance with their equivalent Security Classification Level and ensure that the Classified Information is marked with an equivalent security classification marking in accordance with paragraphs 1, 2 and 3 of Article 3.

2. Nothing in this Agreement shall cause prejudice to the national laws and regulations of the Parties regarding the rights of individuals to obtain access to public documents or access to information of public character, the protection of personal data or the protection of Classified Information.

3. In accordance with national laws and regulations, each Party shall ensure that appropriate measures are implemented for the protection of Classified Information processed, stored, or transmitted in communication and information systems as long as it is deemed necessary. Such measures shall ensure the confidentiality, integrity, availability and, where applicable, non-repudiation and authenticity of Classified Information, as well as an appropriate level of accountability and traceability of actions in relation to that information.

ARTICLE 5
DISCLOSURE AND USE OF CLASSIFIED INFORMATION

1. Each Party shall ensure that Classified Information provided or exchanged under this Agreement is not:

   a) Declassified or downgraded without the prior written consent of the Originating Party; and

   b) Used for purposes other than those established by the Originating Party.

2. The Receiving Party shall not release or allow access to Classified Information to a Third Party or its nationals without prior written consent of the Originating Party. Each Party shall, in accordance with its constitutional requirements and national legislation, respect the principle of consent of the Originating Party.

ARTICLE 6
ACCESS TO CLASSIFIED INFORMATION

1. Each Party shall ensure that access to Classified Information is granted based on the principle of "Need to know".

2. Each Party shall ensure that all individuals who are granted access to Classified Information are informed of their responsibilities to protect such information in accordance with the appropriate security regulations.

3. The Parties shall ensure that access to Classified Information is granted only to individuals who hold an appropriate PSC or who are otherwise duly authorized by virtue of their functions in accordance with national legislation.

4. In accordance with its national laws and regulations, each Party shall ensure that any entity under its jurisdiction that may receive or generate Classified Information is appropriately security cleared and is capable of providing suitable protection, as provided for in paragraph 1 of Article 4 of this Agreement, at the appropriate security level.

ARTICLE 7
TRANSLATION, REPRODUCTION AND DESTRUCTION OF CLASSIFIED INFORMATION

1. All translations and reproductions of Classified Information shall bear the appropriate Security Classification Level and shall be protected and controlled as the original by the Parties accordingly.

2. All translations of Classified Information shall contain a suitable annotation, in the language to which they were translated, indicating that they contain Classified Information of the Originating Party.

3. In accordance with paragraph 3 of Article 6 of this Agreement the translators must have an appropriate PSC at Security Classification Level of the Classified Information to be translated.

4. Classified Information marked as ULTRASSECRETO / STROGO TAJNO / TOP SECRET shall be translated or reproduced only upon prior written permission of the Originating Party.

5. The number of reproductions shall be limited to the minimum required for an official purpose and shall be made only by individuals with an appropriate PSC and a "Need to know".

6. Classified Information shall not be reproduced by the Receiving Party without the prior written consent of the Originating Party.

7. Classified Information received under this Agreement shall not be destroyed. When it is no longer considered necessary by the Receiving Party it shall be returned to the Originating Party.

ARTICLE 8
TRANSMISSION BETWEEN THE PARTIES

1. The Classified Information shall be transmitted between the Parties through diplomatic channels or as otherwise agreed by the Parties.

2. The Classified Information must be transmitted through protected communications systems, networks, or other electromagnetic media approved by both Parties. Such transmissions shall be protected by cryptographic means that are mutually accepted by the National Security Authorities in accordance with the national laws and regulations.

3. Classified Information marked as ULTRASSECRETO / STROGO TAJNO / TOP SECRET shall be sent only through diplomatic channels.

4. The Receiving Party shall not transmit Classified Information to a Third Party without the prior written consent of the NSA or CSA of the Originating Party.

5. If a Party wishes to transmit Classified Information originating from the other Party outside the territories of the Parties, such transmissions shall be subject to the prior written consent of the NSA or CSA of the Originating Party.

6. In case of transmission of large consignment containing Classified Information, procedures for transport shall be jointly agreed and evaluated, on a case-by-case basis, by both National Security Authorities of the Parties.

ARTICLE 9
VISITS

1. Visits to facilities where Classified Information is handled or stored shall be subject to prior written consent by the NSA of the host Party, unless otherwise mutually approved.

2. A request for a Visit shall be submitted to the NSA of the host Party and shall include the following data that shall be used for the purpose of the Visit only:

a) The visitor's name, date and place of birth, nationality, and identification card/passport number;

b) Position and function of the visitor as well as the name and address of the facility where he/she is employed;

c) Specification of the project in which the visitor is participating;

d) The validity and level of the visitor's PSC;

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

f) The purpose of the Visit, including the entity that they intend to visit and the highest Security Classification Level of Classified Information involved;

g) The date and duration of the Visit. For recurring Visits, the total period covered by the Visits shall be stated;

h) Other data, if agreed upon by the National Security Authorities; and

i) Date and signature.

3. A request for a Visit shall be submitted at least 30 (thirty) days prior to the expected date of the Visit unless otherwise mutually agreed by the Competent Security Authorities.

4. Any Classified Information released to a visitor shall be considered as Classified Information received under this Agreement. A visitor shall comply with the security regulations of the host Party.

5. The Visits shall be authorized by one Party to the visitors of the other Party, only if those:

a) Have a valid PSC granted by their country of origin; and

b) Are authorized to receive or have access to the Classified Information as per the "Need to know" basis.

6. Once the Visit is authorized, the NSA of the host country shall notify the NSA of the visitor's country about its authorization with a minimum notice of 10 (ten) days prior to the expected date of the Visit and supply a copy of the request to the entity to be visited.

7. The Competent Security Authorities may agree on a list of visitors entitled to recurring Visits. The list shall be valid for an initial period not exceeding 12 (twelve) months and may be extended for a further period of time not exceeding 12 (twelve) months. A request for recurring Visits shall be submitted in accordance with paragraph 3 of this Article. Once the list has been approved, Visits may be arranged directly between the facilities involved.

ARTICLE 10
CLASSIFIED CONTRACTS RELATED TO THIS AGREEMENT

1. In case of Classified Contracts concluded and implemented in the territory of one of the Parties, the NSA or CSA of the other Party shall obtain prior written assurance that the proposed Contractor holds a FSC and the necessary Personnel Security Clearances at the appropriate level.

2. The Contractor commits itself to:

a) Ensure that its premises have adequate conditions for the Handling of Classified Information;

b) Have the appropriate FSC;

c) Ensure that all persons with access to Classified Information have the appropriate PSC and are informed of their responsibility towards its protection, in accordance with national laws and regulations;

d) Not disclose, or permit the disclosure of, the Classified Information to a Third Party not expressly authorized in writing by the Originating Party; and

e) Allow security inspections of their premises.

3. For each Classified Contract awarded, the Originating Party shall inform the Receiving Party of the level of the Classified Information transmitted.

4. The Classified Contract must also provide these additional terms:

a) Liability for the non-compliance with the security procedures and measures applicable to the Classified Information;

b) Obligation to inform the CSA of any Security Breach or Compromise of Classified Information; and

c) Liability for the damage resulting from Security Breach.

5. Any subcontractor must fulfill the same security requirements as the Contractor.

ARTICLE 11
NATIONAL SECURITY AUTHORITIES AND SECURITY COOPERATION

1. The National Security Authorities responsible for the implementation and supervision of this Agreement shall be:

In the Federative Republic of Brazil:
Institutional Security Cabinet of the Presidency of the Republic
("Gabinete de Segurança Institucional da Presidência da República")

In the Republic of Slovenia:
The Office of the Government of the Republic of Slovenia for the Protection of Classified Information
("Urad Vlade Republike Slovenije za varovanje tajnih podatkov")

2. Each Party shall provide the other Party with the necessary contact data of their respective NSA in writing.

3. The National Security Authorities shall inform each other about their respective national laws and regulations in effect that regulate the protection of Classified Information.

4. The National Security Authorities shall inform each other about any modifications concerning them or regarding the Security Clearances of individuals, agencies, and entities.

5. Aiming at ensuring a close cooperation in the implementation of this Agreement, the National Security Authorities may be consulted whenever it is requested by one of them.

6. Representatives of the NSA of one Party may visit the establishments of the NSA of the other Party with the intent of acquiring knowledge of security procedures and measures applicable to Classified Information.

7. The Parties, through their National Security Authorities, shall notify each other, in time, about any changes in the title of such bodies or transfers of its competences to other bodies in accordance with Article 20.

8. If requested, the Parties, through their National Security Authorities, bearing in mind the respective national laws and regulations, shall collaborate with each other in the course of the necessary procedures for the PSC of their individuals that have lived or live in the territory of the other Party.

9. The Parties mutually recognize each other's Personnel Security Clearances and Facility Security Clearances and shall promptly inform each other about any changes in mutually recognized Personnel Security Clearances and Facility Security Clearances.

10. To achieve and maintain comparable standards of security, the Competent Security Authorities shall, on request, provide each other with information about their national security standards, procedures, and practices for the protection of Classified Information. If required, the Competent Security Authorities may conduct regular meetings.

11. Upon request, the Parties shall provide mutual assistance in procedures for obtaining Personnel Security Clearances.

ARTICLE 12
ASSISTANCE FOR SECURITY CLEARANCE PROCEDURES

1. On request, the National Security Authorities of the Parties, taking into account their respective national laws and regulations, shall assist each other during the Security Clearance procedures.

2. The Parties shall recognize Security Clearances issued in accordance with national laws and regulations of the other Party.

ARTICLE 13
SECURITY BREACH

1. In case of a Security Breach related to Classified Information that involves the Parties of this Agreement, the NSA of the Party where the Security Breach occurred shall immediately inform the NSA of the other Party.

2. When the Security Breach has occurred in a Third Party, the NSA of the Originating Party shall inform the NSA of the other Party, as soon as possible, and ensure the appropriate investigation.

3. The competent Party shall undertake all measures in accordance with the national laws and regulations so as to limit the consequences of the breach referred to in paragraph 1 of this Article and to prevent further breaches. On request, the other Party shall provide appropriate assistance; it shall be informed of the outcome of the proceedings and the measures undertaken due to the breach.

4. The Party where the Security Breach happened shall investigate or accompany the investigation of the incident and, at the end, immediately inform the other Party about the result of the investigation and the applied corrective measures.

5. The other Party shall, if required, co-operate in the investigation.

ARTICLE 14
COSTS

Each Party shall bear its own costs incurred by the implementation and supervision of all aspects of this Agreement.

ARTICLE 15
DISPUTE RESOLUTION

1. Any dispute that should arise between the Parties regarding the interpretation or implementation of this Agreement, or any related matter, shall be resolved by consultations and negotiations between the Parties through diplomatic channels.

2. During the period of resolution of the dispute, the Parties shall continue to fulfill all of their obligations under this Agreement.

ARTICLE 16
COMMUNICATION

All communication between the Parties related to the implementation of this Agreement shall be made in writing, in English.

ARTICLE 17
ENTRY INTO FORCE

This Agreement shall enter into force the first day of the second month after the receipt of the last notification, by which the Parties have informed each other, through diplomatic channels, that their internal legal requirements necessary for its entry into force were complied with.

ARTICLE 18
AMENDMENTS

1. This Agreement may be amended at any time, in writing, by mutual consent of the Parties.

2. The amendments shall enter into force in accordance with the terms of Article 17 of this Agreement.

ARTICLE 19
VALIDITY AND TERMINATION

1. This Agreement shall remain in force indefinitely.

2. Any Party may, at any time, terminate this Agreement by written notification to the other Party.

3. The termination must be notified in writing through diplomatic channels and shall come into effect 6 (six) months after the date on which the other Party has received the termination notice.

4. In case of termination, any Classified Information exchanged according to this Agreement shall continue to be protected in accordance with the provisions set out herein, unless the Originating Party exempts the Receiving Party from that obligation.

ARTICLE 20
FINAL PROVISIONS

1. The Parties shall promptly notify each other of any changes to its respective national laws and regulations that affect the protection of Classified Information released under this Agreement. In the event of such changes, the Parties shall consult to consider possible changes to this Agreement. In the meantime, the Classified Information shall continue to be protected as described herein, unless otherwise requested by the Originating Party in writing.

2. After the entry into force of this Agreement, the Party in whose territory the Agreement is concluded shall take immediate measures to have the Agreement registered by the Secretariat of the United Nations in accordance with Article 102 of the United Nations Charter. The other Party shall be notified of the registration and of the registration number in the United Nations Treaty Series as soon as the Secretariat of the United Nations has notified that the Agreement had been registered.

Done in Rio de Janeiro, on 11 April 2023, in two originals, each in the Portuguese, Slovenian and English languages, all texts being equally authentic. In case of divergences of interpretation, the English text shall prevail.

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

FOR THE GOVERNMENT OF THE FEDERATIVE REPUBLIC OF BRAZIL

MARCO EDSON GONÇALVES DIAS
Minister of State Head of the Institutional Security Cabinet of the Presidency of the Republic

FOR THE GOVERNMENT OF THE REPUBLIC OF SLOVENIA

MARJAN ŠAREC
Ministry of Defense

SPORAZUM MED VLADO FEDERATIVNE REPUBLIKE BRAZILIJE IN VLADO REPUBLIKE SLOVENIJE O IZMENJAVI IN MEDSEBOJNEM VAROVANJU TAJNIH PODATKOV

Vlada Federativne Republike Brazilije

in

Vlada Republike Slovenije,
v nadaljnjem besedilu: skupaj »pogodbenici« ali posamično »pogodbenica«, sta se

zaradi državne varnosti in zagotavljanja varovanja tajnih podatkov, izmenjanih v okviru mednarodnih pogodb ali pogodb o sodelovanju, sklenjenih med njima, njunimi pooblaščenimi posamezniki, organi in javnimi ali zasebnimi subjekti;

v želji, da določita pravila in postopke za varovanje tajnih podatkov v skladu z notranjimi zakoni in drugimi predpisi pogodbenic;

ob potrditvi, da sporazum ne vpliva na obveznosti pogodbenic, ki izhajajo iz drugih mednarodnih sporazumov, in se ne uporablja v nasprotju z interesi, varnostjo in ozemeljsko celovitostjo drugih držav,

dogovorili:

1. ČLEN

NAMEN IN PODROČJE UPORABE

Sporazum določa pravila in postopke za varovanje tajnih podatkov, ki jih pogodbenici, njuni pooblaščeni posamezniki, organi, agencije in subjekti izmenjajo ter nastanejo pri sodelovanju v zvezi z njunimi državnimi interesi in varnostjo.

2. ČLEN

POMEN IZRAZOV

V tem sporazumu izrazi pomenijo:

a) **pogodba s tajnimi podatki**: pogodba ali podizvajalska pogodba, vključno s pogajanji pred sklenitvijo pogodbe, med dvema izvajalcema ali več izvajalci, ki daje in določa izvršljive pravice ter obveznosti med njimi in vsebuje tajne podatke ali dovoljuje dostop do njih;

b) **tajni podatek**: podatek, ki je ne glede na svojo obliko, naravo in način prenosa določen v skladu z zakoni in drugimi predpisi obeh pogodbenic, zaščiten pred nepooblaščenim dostopom ali razkritjem, je bil označen kot tajen in ga pogodbenici izmenjata ali pri njiju nastane;

c) **pristojni varnostni organ**: pristojni subjekt, ki je pooblaščen v skladu z notranjimi zakoni in drugimi predpisi pogodbenic ter je odgovoren za izvajanje varnostnih zahtev po sporazumu;

d) **ogrožanje**: vsaka oblika zlorabe, poškodbe tajnih podatkov ali nepooblaščenega dostopa do njih, njihovega spreminjanja, razkritja ali uničenja in vsako drugo dejanje ali opustitev dejanja, ki zaradi kršitve varovanja tajnosti privede do izgube tajnosti, celovitosti, razpoložljivosti ali verodostojnosti tajnih podatkov;

e) **izvajalec**: posameznik, agencija ali subjekt s pravno sposobnostjo za sklepanje pogodb;

f) **varnostno dovoljenje organizacije**: opredelitev pristojnega varnostnega organa pogodbenice, da je javni ali zasebni subjekt, ki je v njeni državi, varnostno preverjen in ima vzpostavljene ustrezne varnostne ukrepe v posebnem prostoru za obravnavanje tajnih podatkov v skladu z notranjimi zakoni in drugimi predpisi;

g) **obravnavanje tajnih podatkov**: skupek dejanj v zvezi z ustvarjanjem, prejemanjem,

določanjem tajnosti, uporabo tajnih podatkov katere koli stopnje tajnosti, dostopom do njih, njihovim razmnoževanjem, prevozom, prenosom, distribucijo, arhiviranjem, hrambo, uničenjem, vrednotenjem, namembnostjo ali nadzorom nad njimi;

h) **nacionalni varnostni organ**: državni organ, opredeljen v notranji zakonodaji pogodbenic, ki je posebej pooblaščen na področju varovanja tajnih podatkov;

i) **potreba po seznanitvi**: načelo, po katerem se posamezniku, ki ima preverjeno potrebo, da se s tajnimi podatki seznani ali jih ima za opravljanje svojih uradnih dolžnosti in nalog, lahko dovoli dostop do tajnih podatkov;

j) **pogodbenica izvora**: pogodbenica, vključno z javnimi ali zasebnimi subjekti v njeni pristojnosti, ki daje tajne podatke pogodbenici prejemnici;

k) **dovoljenje za dostop do tajnih podatkov**: ugotovitev pristojnega varnostnega organa pogodbenice, da je posameznik varnostno preverjen za obravnavanje tajnih podatkov v skladu z njenimi notranjimi zakoni in drugimi predpisi, na podlagi katere je ta posameznik pooblaščen za dostop do tajnih podatkov do stopnje tajnosti, navedene v dovoljenju, in za ravnanje z njimi;

l) **pogodbenica prejemnica**: pogodbenica, vključno z javnimi ali zasebnimi subjekti v njeni pristojnosti, ki se ji pošljejo tajni podatki in prejme tajne podatke;

m) **kršitev varovanja tajnosti**: namerno ali nenamerno dejanje ali opustitev dejanja, ki dejansko ogrozi ali bi lahko ogrozila tajne podatke;

n) **stopnja tajnosti**: v skladu z notranjimi zakoni in drugimi predpisi pogodbenic določa pomembnost tajnih podatkov, stopnjo omejitve dostopa do njih in stopnjo varovanja, ki jo zagotavljata pogodbenici, in je tudi stopnja, na podlagi katere so podatki označeni;

o) **varnostno preverjanje**: postopek, v katerem pristojni varnostni organ izda varnostno dovoljenje organizacije ali dovoljenje za dostop do tajnih podatkov v skladu z notranjimi zakoni in drugimi predpisi pogodbenic;

p) **tretja stran**: država, mednarodna organizacija, vlada ali posameznik, ki predstavlja državni organ ali organizacijo, vključno z javnimi in zasebnimi subjekti, ki ni pogodbenik sporazuma, in

q) **obisk**: vsak dostop do javnih in zasebnih subjektov za namene sporazuma, ki vključuje obravnavanje tajnih podatkov.

3. ČLEN
STOPNJE TAJNOSTI

1. Pogodbenici v skladu z notranjimi zakoni in drugimi predpisi soglašata, da si naslednje stopnje tajnosti ustrezajo in so si enakovredne:

V REPUBLIKI SLOVENIJI (slovenščina)	**V FEDERATIVNI REPUBLIKI BRAZILIJI** (portugalščina)	**V ANGLEŠKEM JEZIKU**
STROGO TAJNO	ULTRASSECRETO	TOP SECRET
TAJNO	SECRETO	SECRET
ZAUPNO		CONFIDENTIAL
INTERNO	RESERVADO	RESTRICTED

2. Brazilska pogodbenica bo obravnavala in varovala slovenske tajne podatke stopnje tajnosti »ZAUPNO« na način, ki ni manj strog od tistega, ki ga zagotavljajo standardi in postopki za tajne podatke stopnje tajnosti »SECRETO«.

3. Slovenska pogodbenica bo obravnavala in varovala brazilske tajne podatke stopnje tajnosti »SECRETO« na način, ki ni manj strog od tistega, ki ga zagotavljajo standardi in postopki za tajne podatke stopnje tajnosti »TAJNO«.

4. Tajni podatki, dani na podlagi sporazuma, so označeni z ustrezno stopnjo tajnosti v skladu z notranjimi zakoni in drugimi predpisi pogodbenice izvora, pred njo pa je po potrebi navedeno ime države, ki je lastnica tajnih podatkov in jih zagotavlja.

5. Pogodbenici vse tajne podatke, ki jih prejmeta druga od druge, označita z enakovredno stopnjo tajnosti v skladu s prvim, drugim in tretjim odstavkom tega člena.

6. Pogodbenici se uradno obveščata o vseh nadaljnjih spremembah stopenj tajnosti poslanih tajnih podatkov.

7. Pogodbenica izvora:

a) brez odlašanja uradno obvesti pogodbenico prejemnico o vsaki spremembi stopnje tajnosti danih tajnih podatkov in

b) obvesti pogodbenico prejemnico o pogojih za dajanje tajnih podatkov ali o omejitvah pri njihovi uporabi.

4. ČLEN

VAROVANJE TAJNIH PODATKOV

1. Pogodbenici sprejmeta vse ustrezne ukrepe v skladu s svojimi notranjimi zakoni in drugimi predpisi, da zagotovita prejetim tajnim podatkom stopnjo varovanja v skladu s svojo enakovredno stopnjo tajnosti in zagotovita, da so tajni podatki označeni z enakovredno stopnjo tajnosti v skladu s prvim, drugim in tretjim odstavkom 3. člena.

2. Nič v sporazumu ne posega v notranje zakone in druge predpise pogodbenic o pravicah posameznikov, da pridobijo dostop do javnih dokumentov ali informacij javnega značaja, o varstvu osebnih podatkov ali varovanju tajnih podatkov.

3. Vsaka pogodbenica v skladu z notranjimi zakoni in drugimi predpisi zagotovi izvajanje ustreznih ukrepov za varovanje tajnih podatkov, ki se obdelujejo, hranijo ali prenašajo v komunikacijskih in informacijskih sistemih, dokler je to potrebno. Ti ukrepi zagotovijo zaupnost, celovitost, razpoložljivost, in kjer je primerno, nezatajljivost in verodostojnost tajnih podatkov ter ustrezno raven odgovornosti in sledljivosti dejanj, povezanih s takimi podatki.

5. ČLEN

RAZKRITJE IN UPORABA TAJNIH PODATKOV

1. Vsaka pogodbenica za po sporazumu dane ali izmenjane tajne podatke zagotovi, da se:

a) ne prekliče ali zniža stopnja njihove tajnosti brez predhodnega pisnega soglasja pogodbenice izvora in

b) ne uporabijo za druge namene od tistih, ki jih opredeli pogodbenica izvora.

2. Pogodbenica prejemnica tretji strani ali njenim državljanom ne da tajnih podatkov ali dovoli dostopa do njih brez predhodnega pisnega soglasja pogodbenice izvora. Vsaka pogodbenica v skladu s svojimi ustavnimi zahtevami in notranjo zakonodajo spoštuje načelo soglasja pogodbenice izvora.

6. ČLEN
DOSTOP DO TAJNIH PODATKOV

1. Vsaka pogodbenica zagotovi, da se dostop do tajnih podatkov dovoli na podlagi načela potrebe po seznanitvi.

2. Vsaka pogodbenica zagotovi, da so vsi posamezniki, ki se jim dovoli dostop do tajnih podatkov, seznanjeni s svojo odgovornostjo za varovanje takih podatkov v skladu z ustreznimi varnostnimi predpisi.

3. Pogodbenici zagotovita, da se dostop do tajnih podatkov dovoli samo posameznikom, ki imajo ustrezno dovoljenje za dostop do tajnih podatkov ali so drugače pravilno pooblaščeni zaradi svoje funkcije v skladu z notranjo zakonodajo.

4. Vsaka pogodbenica v skladu s svojimi notranjimi zakoni in drugimi predpisi zagotovi, da je vsak subjekt v njeni pristojnosti, ki lahko prejme tajne podatke ali pri katerem lahko nastanejo tajni podatki, ustrezno varnostno preverjen in sposoben zagotavljati primerno varovanje glede na ustrezno stopnjo tajnosti, kot določa prvi odstavek 4. člena sporazuma.

7. ČLEN
PREVAJANJE, RAZMNOŽEVANJE IN UNIČENJE TAJNIH PODATKOV

1. Vsi prevodi in izvodi tajnih podatkov so označeni z ustrezno stopnjo tajnosti, pogodbenici pa jih ustrezno varujeta in nadzorujeta kot izvirnik.

2. Vsak prevod tajnih podatkov ima v jeziku prevoda ustrezno navedbo, da prevod vsebuje tajne podatke pogodbenice izvora.

3. Prevajalec mora v skladu s tretjim odstavkom 6. člena sporazuma imeti ustrezno dovoljenje za dostop do tajnih podatkov za stopnjo tajnosti tajnih podatkov, ki jih prevaja.

4. Tajni podatki stopnje tajnosti ULTRASSECRETO/STROGO TAJNO/TOP SECRET se prevajajo ali razmnožujejo izključno s predhodnim pisnim dovoljenjem pogodbenice izvora.

5. Število izvodov je omejeno na najmanjšo količino, ki je potrebna za uradne namene, naredijo pa jih samo posamezniki z ustreznim dovoljenjem za dostop do tajnih podatkov in s potrebo po seznanitvi.

6. Pogodbenica prejemnica tajnih podatkov ne razmnožuje brez predhodnega pisnega soglasja pogodbenice izvora.

7. Tajni podatki, prejeti na podlagi sporazuma, se ne uničijo. Ko jih pogodbenica prejemnica ne potrebuje več, se vrnejo pogodbenici izvora.

8. ČLEN

PRENOS MED POGODBENICAMA

1. Prenos tajnih podatkov med pogodbenicama poteka po diplomatski poti ali v skladu z dogovorom med pogodbenicama.

2. Tajni podatki se prenašajo po zaščitenih komunikacijskih sistemih, mrežah ali drugih elektromagnetnih medijih, ki jih odobrita pogodbenici. Taki prenosi so varovani s kriptografskimi rešitvami, ki sta jih nacionalna varnostna organa skupaj odobrila v skladu z notranjimi zakoni in drugimi predpisi.

3. Tajni podatki stopnje tajnosti ULTRASSECRETO/STROGO TAJNO/TOP SECRET se pošiljajo le po diplomatski poti.

4. Pogodbenica prejemnica ne da tajnih podatkov tretji strani brez predhodnega pisnega soglasja nacionalnega varnostnega organa ali pristojnega varnostnega organa pogodbenice izvora.

5. Če pogodbenica želi tajne podatke druge pogodbenice poslati zunaj ozemelj pogodbenic, je za tak prenos potrebno predhodno pisno soglasje nacionalnega varnostnega organa ali pristojnega varnostnega organa pogodbenice izvora.

6. Pri pošiljanju velike pošiljke, ki vsebuje tajne podatke, se nacionalna varnostna organa pogodbenic skupaj dogovorita o postopkih za prevoz in jih ovrednotita za vsak primer posebej.

9. ČLEN

OBISKI

1. Za obiske organizacij, ki obravnavajo ali hranijo tajne podatke, je potrebno predhodno pisno soglasje nacionalnega varnostnega organa pogodbenice gostiteljice, razen če ni vzajemno drugače dogovorjeno.

2. Zaprosilo za obisk se predloži nacionalnemu varnostnemu organu pogodbenice gostiteljice in vsebuje podatke, ki se uporabijo le za namen obiska:

a) ime in priimek obiskovalca, datum in kraj rojstva, državljanstvo in identifikacijsko izkaznico/številko potnega lista;

b) položaj in funkcijo obiskovalca ter ime in naslov organizacije, v kateri je zaposlen;

c) podatke o projektu, pri katerem obiskovalec sodeluje;

d) veljavnost in stopnjo tajnosti obiskovalčevega dovoljenja za dostop do tajnih podatkov;

e) ime, naslov, telefonsko številko, elektronski naslov organizacije, v kateri bo obisk, in točko za stike v tej organizaciji;

f) namen obiska, vključno s subjektom, ki ga obiskovalec namerava obiskati, in najvišjo stopnjo tajnosti obravnavanih tajnih podatkov;

g) datum in trajanje obiska. Pri večkratnih obiskih se navede celotno obdobje, v katerem bodo potekali;

h) druge podatke, če se tako dogovorita nacionalna varnostna organa, in

i) datum in podpis.

3. Zaprosilo za obisk se predloži vsaj 30 (trideset) dni pred predvidenim dnevom obiska, razen če se pristojna varnostna organa ne dogovorita drugače.

4. Vsak tajni podatek, ki je dan obiskovalcu, se šteje za tajni podatek, prejet na podlagi sporazuma. Obiskovalec spoštuje varnostne predpise pogodbenice gostiteljice.

5. Pogodbenica odobri obiske obiskovalcev iz druge pogodbenice le, če:

a) imajo veljavno dovoljenje za dostop do tajnih podatkov, ki jim ga je dala njihova država izvora, in

b) so pooblaščeni za prejem tajnih podatkov ali dostop do njih na podlagi potrebe po seznanitvi.

6. Ko je obisk odobren, nacionalni varnostni organ države gostiteljice uradno obvesti nacionalni varnostni organ države obiskovalca o odobritvi najmanj 10 (deset) dni pred predvidenim dnevom obiska in kopijo zaprosila pošlje subjektu, ki bo obiskan.

7. Pristojna varnostna organa se lahko dogovorita o seznamu obiskovalcev, ki so upravičeni do večkratnih obiskov. Seznam velja za začetno obdobje, ki ni daljše od 12 (dvanajstih) mesecev in se lahko podaljša za največ 12 (dvanajst) mesecev. Zaprosilo za večkratne obiske se predloži v skladu s tretjim odstavkom tega člena. Ko je seznam potrjen, se sodelujoče organizacije lahko neposredno dogovarjajo o obiskih.

10. ČLEN

POGODBE S TAJNIMI PODATKI, POVEZANE S SPORAZUMOM

1. Pri pogodbah s tajnimi podatki, ki se sklenejo in izvajajo na ozemlju ene od pogodbenic, nacionalni varnostni organ ali pristojni varnostni organ druge pogodbenice pridobi predhodno pisno zagotovilo, da ima predlagani izvajalec varnostno dovoljenje organizacije in potrebna dovoljenja za dostop do tajnih podatkov ustrezne stopnje tajnosti.

2. Izvajalec se zavezuje:

a) zagotoviti, da ima v svojih prostorih ustrezne možnosti za obravnavanje tajnih podatkov;

b) da ima ustrezno varnostno dovoljenje organizacije;

c) zagotoviti, da imajo vse osebe z dostopom do tajnih podatkov ustrezno dovoljenje za dostop do tajnih podatkov in so seznanjene s svojo odgovornostjo za varovanje tajnih podatkov v skladu z notranjimi zakoni in drugimi predpisi;

d) da ne bo razkril ali dovolil razkritja tajnih podatkov tretji strani, ki je pogodbenica izvora ni izrecno pisno pooblastila, in

e) da dovoli varnostni pregled svojih prostorov.

3. Pri vsaki dodeljeni pogodbi s tajnimi podatki pogodbenica izvora obvesti pogodbenico prejemnico o stopnji tajnosti poslanih tajnih podatkov.

4. Pogodba s tajnimi podatki mora vsebovati tudi te dodatne pogoje:

a) odgovornost za neupoštevanje varnostnih postopkov in ukrepov, ki veljajo za tajne podatke;

b) obveznost obveščanja pristojnega varnostnega organa o vsaki kršitvi varovanja tajnosti ali ogrožanju tajnih podatkov;

c) odgovornost za škodo, ki nastane zaradi kršitve varovanja tajnosti.

5. Vsak podizvajalec mora izpolnjevati enake varnostne zahteve kot izvajalec.

11. ČLEN

NACIONALNA VARNOSTNA ORGANA IN VARNOSTNO SODELOVANJE

1. Nacionalna varnostna organa, pristojna za izvajanje sporazuma in nadzor nad njim, sta:

v Federativni republiki Braziliji:

Urad predsedstva republike za institucionalno varnost
(Gabinete de Segurança Institucional da Presidência da República)

v Republiki Sloveniji:

Urad Vlade Republike Slovenije za varovanje tajnih podatkov

2. Pogodbenici si pisno zagotavljata potrebne podatke za stike svojih nacionalnih varnostnih organov.

3. Nacionalna varnostna organa se medsebojno obveščata o veljavnih notranjih zakonih in drugih predpisih, ki urejajo varovanje tajnih podatkov.

4. Nacionalna varnostna organa se medsebojno obveščata o vseh spremembah v zvezi z njima ali v zvezi z varnostnim preverjanjem posameznikov, agencij in subjektov.

5. Nacionalna varnostna organa se na zaprosilo enega od njiju lahko medsebojno posvetujeta, da zagotovita tesno sodelovanje pri izvajanju sporazuma.

6. Predstavniki nacionalnega varnostnega organa ene pogodbenice lahko obiščejo prostore nacionalnega varnostnega organa druge pogodbenice, da bi se seznanili z varnostnimi postopki in ukrepi, ki veljajo za tajne podatke.

7. Pogodbenici se po svojih nacionalnih varnostnih organih pravočasno uradno obvestita o vsaki spremembi v imenu teh organov ali prenosu njihovih pristojnosti na druge organe v skladu z 20. členom.

8. Pogodbenici po svojih nacionalnih varnostnih organih na zaprosilo ter v skladu s svojimi notranjimi zakoni in drugimi predpisi sodelujeta v potrebnih postopkih za pridobitev dovoljenja za dostop do tajnih podatkov svojih posameznikov, ki so prebivali ali prebivajo na ozemlju druge pogodbenice.

9. Pogodbenici medsebojno priznavata dovoljenja za dostop do tajnih podatkov in varnostna dovoljenja organizacij ter se takoj obvestita o vsaki spremembi medsebojno priznanih dovoljenj za dostop do tajnih podatkov in varnostnih dovoljenj organizacij.

10. Zaradi doseganja in ohranjanja primerljivih varnostnih standardov pristojna varnostna organa na podlagi zaprosila zagotovita drug drugemu informacije o svojih nacionalnih varnostnih standardih, postopkih in praksah za varovanje tajnih podatkov. Po potrebi lahko pristojna varnostna organa organizirata redne sestanke.

11. Pogodbenici si na zaprosilo medsebojno pomagata pri postopkih za pridobitev dovoljenj za dostop do tajnih podatkov.

12. ČLEN

POMOČ PRI POSTOPKIH VARNOSTNEGA PREVERJANJA

1. Nacionalna varnostna organa pogodbenic si na zaprosilo pomagata pri postopkih varnostnega preverjanja v skladu z notranjimi zakoni in drugimi predpisi.
2. Pogodbenica priznava varnostna dovoljenja organizacij in dovoljenja za dostop do tajnih podatkov, ki so izdana v skladu z notranjimi zakoni in drugimi predpisi druge pogodbenice.

13. ČLEN

KRŠITEV VAROVANJA TAJNOSTI

1. Ob kršitvi varovanja tajnosti v zvezi s tajnimi podatki, ki se nanašajo na pogodbenici sporazuma, nacionalni varnostni organ pogodbenice, v kateri nastane kršitev varovanja tajnosti, takoj obvesti nacionalni varnostni organ druge pogodbenice.
2. Kadar nastane kršitev varovanja tajnosti pri tretji strani, nacionalni varnostni organ pogodbenice izvora čim prej obvesti nacionalni varnostni organ druge pogodbenice in zagotovi ustrezno preiskavo.
3. Pristojna pogodbenica sprejme vse ukrepe v skladu z notranjimi zakoni in drugimi predpisi, da omeji posledice kršitve iz prvega odstavka tega člena in prepreči nadaljnje kršitve. Druga pogodbenica ji na zaprosilo zagotovi ustrezno pomoč; obveščena je o izidu postopkov in ukrepih, sprejetih zaradi kršitve.
4. Pogodbenica, v kateri nastane kršitev varovanja tajnosti, opravi ali spremlja preiskavo dogodka in po njej takoj obvesti drugo pogodbenico o rezultatu preiskave in izvedenih popravljalnih ukrepih.
5. Druga pogodbenica po potrebi sodeluje v preiskavi.

14. ČLEN

STROŠKI

Vsaka pogodbenica krije svoje stroške, ki nastanejo pri izvajanju vseh vidikov sporazuma in nadzoru nad njimi.

15. ČLEN

REŠEVANJE SPOROV

1. Spor med pogodbenicama v zvezi z razlago ali izvajanjem sporazuma ali s tem povezano zadevo se rešuje s posvetovanji in pogajanji med pogodbenicama po diplomatski poti.
2. Med reševanjem spora pogodbenici še naprej izpolnjujeta vse obveznosti po sporazumu.

16. ČLEN

KOMUNICIRANJE

Komuniciranje med pogodbenicama v zvezi z izvajanjem sporazuma v celoti poteka pisno v angleškem jeziku.

17. ČLEN

ZAČETEK VELJAVNOSTI

Sporazum začne veljati prvi dan drugega meseca po prejemu zadnjega uradnega obvestila, s katerim se pogodbenici po diplomatski poti obvestita, da so izpolnjene njune notranjepravne zahteve za začetek njegove veljavnosti.

18. ČLEN

SPREMEMBE

1. Sporazum se lahko kadar koli spremeni s pisnim medsebojnim soglasjem pogodbenic.
2. Spremembe začnejo veljati v skladu s pogoji iz 17. člena sporazuma.

19. ČLEN

VELJAVNOST IN ODPOVED

1. Sporazum velja nedoločen čas.

2. Pogodbenica lahko sporazum kadar koli odpove s pisnim uradnim obvestilom drugi pogodbenici.

3. Odpoved se pisno uradno sporoči po diplomatski poti in začne veljati 6 (šest) mesecev po dnevu, ko druga pogodbenica prejme obvestilo o odpovedi.

4. Ob odpovedi sporazuma se vsi tajni podatki, izmenjani v skladu s sporazumom, še naprej varujejo v skladu z njegovimi določbami, razen če pogodbenica izvora oprosti pogodbenico prejemnico te obveznosti.

20. ČLEN

KONČNE DOLOČBE

1. Pogodbenici druga drugo takoj uradno obvestita o vsaki spremembi svojih notranjih zakonov in drugih predpisov, ki vplivajo na varovanje tajnih podatkov, danih na podlagi sporazuma. V takem primeru se pogodbenici posvetujeta o morebitnih spremembah sporazuma. Medtem se vsi tajni podatki še naprej varujejo v skladu s sporazumom, razen če ni pogodbenica izvora pisno zahtevala drugače.

2. Po začetku veljavnosti sporazuma pogodbenica, na ozemlju katere je sporazum sklenjen, takoj sprejme ukrepe za registracijo sporazuma pri sekretariatu Združenih narodov v skladu s 102. členom Ustanovne listine Organizacije združenih narodov. Druga pogodbenica se uradno obvesti o registraciji in registracijski številki v zbirki pogodb Združenih narodov, takoj ko sekretariat Združenih narodov pošlje uradno obvestilo, da je bil sporazum registriran.

Sklenjeno v Rio de Janeiro 11 aprila 2023 v dveh izvirnikih v portugalskem, slovenskem in angleškem jeziku, pri čemer so vsa besedila enako verodostojna. Pri različni razlagi prevlada angleško besedilo.

V potrditev tega sta podpisana, ki sta bila za to pravilno pooblaščena, podpisala ta sporazum.

ZA VLADO
FEDERATIVNE REPUBLIKE BRAZILIJE

MARCO EDSON GONÇALVES DIAS
državni minister vodja Urada predsedstva republike za institucionalno varnost

ZA VLADO
REPUBLIKE SLOVENIJE

MARJAN ŠAREC
minister za obrambo