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

A República Federativa do Brasil

e

a República Eslovaca,

(doravante denominadas conjuntamente como "Partes"
ou, separadamente, como "Parte"),

No interesse da segurança nacional e para assegurar a proteção das Informações Classificadas trocadas no âmbito de instrumentos de cooperação, contratos e outros acordos assinados entre as Partes, seus indivíduos credenciados, órgãos, bem como entidades públicas e privadas.

Desejando estabelecer um quadro de regras e procedimentos relativos a Informações Classificadas de acordo com as leis e regulamentos nacionais das Partes.

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

Acordaram o seguinte:

ARTIGO I
Objeto

1. Este Acordo estabelece regras e procedimentos para a proteção de Informações Classificadas trocadas entre as Partes acima mencionadas, seus indivíduos credenciados, órgãos, bem como entidades públicas ou privadas sob sua jurisdição.

2. Este Acordo não constitui uma base para obrigar as Partes a fornecer ou trocar Informações Classificadas.

ARTIGO II
Definições

Para os fins deste Acordo, os seguintes termos têm os seguintes significados:

a) "Acordo" significa este acordo, incluindo seus Anexos;
b) "Anexo" significa um anexo a este Acordo;
c) "Contrato Classificado" significa um contrato, incluindo qualquer negociação pré-contratual, cuja execução exija ou envolva acesso ou possível acesso a, ou a criação de, Informações Classificadas;
d) "Informação Classificada" significa a informação, material ou objeto, independentemente de sua forma ou natureza ou de qualquer parte deles, com um determinado Nível de Classificação de Segurança, que, independentemente de como for apresentada, deve ser protegida contra acesso não autorizado, divulgação ou outro tipo de comprometimento para o qual foi designada, a fim de prevenir danos ou prejuízos aos interesses de uma ou ambas as Partes, de acordo com as respectivas leis e regulamentos de cada Parte e este Acordo;
e) "Autoridade de Segurança Competente (ASC)" significa a autoridade de cada Parte responsável pela segurança das Informações Classificadas sob este Acordo;
f) "Contratante" significa qualquer entidade jurídica sob a jurisdição de uma Parte, que participe ou esteja vinculada a um Contrato Classificado;
g) "Autorização de Segurança de Instalação (ASI)" significa a certificação pela Autoridade de Segurança Competente de que uma entidade pública ou privada possui medidas de segurança apropriadas e, portanto, foi credenciada para o Tratamento de Informações Classificadas, de acordo com as leis e regulamentos nacionais de cada Parte;
h) "Tratamento de Informações Classificadas" significa um conjunto de ações relacionadas à produção, recepção, classificação, uso, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, destruição ou controle de Informações Classificadas em um determinado Nível de Classificação de Segurança;
i) "Necessidade de Conhecer" significa o requisito para que um indivíduo acesse, tenha conhecimento de ou possua Informações Classificadas para o desempenho de funções e tarefas oficiais;
j) "Parte Originária" significa a Parte sob cuja autoridade as Informações Classificadas foram criadas;
k) "Credencial de Segurança Pessoal (CSP)" significa a certificação de que um determinado indivíduo foi aprovado em investigação de segurança e, portanto, foi credenciado para o Tratamento de Informações Classificadas, em um

determinado Nível de Classificação de Segurança, de acordo com as leis e regulamentos nacionais de cada Parte;

l) "Entidade Provedora" significa a Parte, ou um Contratante, que fornece Informações Classificadas à Entidade Receptora sob este Acordo;

m) "Entidade Receptora" significa a Parte, ou um Contratante, que recebe Informações Classificadas sob este Acordo;

n) "Violação de Segurança" significa qualquer ação ou omissão intencional ou acidental que resulte em comprometimento real ou possível das Informações Classificadas fornecidas ou geradas sob este Acordo;

o) "Nível de Classificação de Segurança" significa o nível de proteção atribuído às Informações Classificadas, de acordo com as leis e regulamentos nacionais de cada Parte e conforme incorporado no artigo IV, parágrafo 1 deste Acordo; e

p) "Terceira Parte" significa qualquer organização, estado, governo ou indivíduo que não seja uma Parte deste Acordo.

ARTIGO III
Autoridades de Segurança Competentes

1. As Autoridades de Segurança Competentes, responsáveis pela implementação e supervisão deste Acordo, estão listadas no Anexo deste Acordo.

2. A Autoridade de Segurança Competente pode delegar partes de suas responsabilidades a uma autoridade de segurança competente delegada.

3. Cada Parte fornecerá à outra os dados de contato de sua respectiva Autoridade de Segurança Competente, por escrito. As Autoridades de Segurança Competentes das Partes informarão uma à outra por escrito sobre alterações em seus dados de contato.

4. Para assegurar uma cooperação estreita na implementação deste Acordo, as Autoridades de Segurança Competentes poderão consultar-se sempre que necessário.

5. Representantes de ambas as Autoridades de Segurança Competentes podem visitar mutuamente suas instalações com a intenção de adquirir conhecimento sobre os procedimentos e medidas de segurança aplicáveis às Informações Classificadas, sujeito à aprovação da Autoridade de Segurança Competente anfitriã.

6. As Autoridades de Segurança Competentes devem auxiliar-se mutuamente na realização de investigações de Autorização de Segurança de Instalação e Credencial de Segurança Pessoal mediante solicitação e de acordo com suas leis e regulamentos nacionais.

7. A pedido da Autoridade de Segurança Competente de uma Parte, a Autoridade de Segurança Competente da outra Parte emitirá uma confirmação por escrito de que uma Credencial de Segurança Pessoal e/ou Autorização de Segurança de Instalação válida foi emitida.

8. As Autoridades de Segurança Competentes das Partes reconhecerão mutuamente as Credenciais de Segurança Pessoal e as Autorizações de Segurança de Instalação emitidas de acordo com suas respectivas leis e regulamentos e no âmbito deste Acordo.

9. As Autoridades de Segurança Competentes notificarão prontamente uma à outra, por escrito, sobre alterações nas Credenciais de Segurança de Pessoal e Autorizações de Segurança de Instalação para as quais uma confirmação foi fornecida conforme o parágrafo 8 deste artigo.

ARTIGO IV
Níveis de Classificação de Segurança

1. As Partes concordam que os Níveis de Classificação de Segurança, de acordo com suas respectivas leis e regulamentos nacionais, corresponderão entre si na seguinte forma de equivalência:

REPÚBLICA FEDERATIVA DO BRASIL COMO PARTE ORIGINÁRIA	**REPÚBLICA ESLOVACA COMO PARTE RECEPTORA**
ULTRASSECRETO	PRÍSNE TAJNÉ
SECRETO	TAJNÉ
RESERVADO	DÔVERNÉ

REPÚBLICA ESLOVACA COMO PARTE ORIGINÁRIA	**REPÚBLICA FEDERATIVA DO BRASIL COMO PARTE RECEPTORA**
PRÍSNE TAJNÉ	ULTRASSECRETO
TAJNÉ	SECRETO
DÔVERNÉ	RESERVADO
VYHRADENÉ	RESERVADO

2. Qualquer Informação Classificada produzida conforme este Acordo deverá ser marcada com o Nível de Classificação de Segurança equivalente da Parte Originária, conforme o parágrafo 1 deste artigo.

3. A Entidade Receptora deverá marcar todas as Informações Classificadas recebidas sob este Acordo com o Nível de Classificação de Segurança equivalente da Entidade Receptora, conforme o parágrafo 1 deste artigo.

4. As Partes devem notificar uma à outra sobre qualquer alteração e subsequente emenda ao Nível de Classificação de Segurança das Informações Classificadas.

5. A Parte Originária pode marcar as Informações Classificadas com requisitos de tratamento, especificando qualquer limitação quanto ao uso, divulgação, liberação e acesso pela Entidade Receptora.

6. A Entidade Receptora não deve modificar ou revogar a classificação de segurança das Informações Classificadas recebidas sob este Acordo sem a aprovação prévia por escrito da Parte Originária.

7. Informações Classificadas originadas conjuntamente pelas Partes deverão receber um Nível de Classificação de Segurança determinado mutuamente pelas Partes.

ARTIGO V
Proteção de Informações Classificadas

1. As Partes devem tomar todas as medidas apropriadas, de acordo com suas leis e regulamentos nacionais, para garantir a proteção das Informações Classificadas conforme este Acordo. Deverão oferecer às Informações Classificadas trocadas ou geradas sob este Acordo pelo menos a mesma proteção que oferecem às suas próprias Informações Classificadas no Nível de Classificação de Segurança correspondente.

2. O tratamento de qualquer Informação Classificada trocada entre as Partes deve respeitar as disposições deste Acordo.

3. Cada Parte deve garantir que as medidas necessárias sejam implementadas para a proteção das Informações Classificadas processadas, armazenadas ou transmitidas por sistemas de comunicação e informação, de acordo com o Nível de Classificação de Segurança, este Acordo e as leis e regulamentos nacionais.

4. Cada Parte deve garantir a confidencialidade, integridade, disponibilidade e, quando aplicável, autenticidade, responsabilidade e rastreabilidade das Informações Classificadas.

5. As Partes não devem divulgar nenhuma Informação Classificada sem o consentimento por escrito da Parte Originária.

ARTIGO VI
Uso de Informações Classificadas

1. Cada Parte deve garantir que a Entidade Provedora:

a) marque as Informações Classificadas com a classificação de segurança apropriada, conforme suas leis e regulamentos nacionais; e
b) informe a Entidade Receptora sobre quaisquer condições de liberação ou limitações quanto ao uso das Informações Classificadas fornecidas, conforme determinado pela Parte Originária.

2. Cada Parte deve garantir que a Entidade Receptora:

a) ofereça o mesmo nível de proteção às Informações Classificadas que oferece às suas Informações Classificadas nacionais de um Nível de Classificação de Segurança equivalente, conforme determinado no artigo IV, parágrafo 1;
b) não desclassifique ou rebaixe as Informações Classificadas sem o consentimento prévio por escrito da Parte Originária;
c) não libere Informações Classificadas a uma Terceira Parte sem o consentimento prévio por escrito da Parte Originária; e
d) use as Informações Classificadas apenas para os fins para os quais foram liberadas e de acordo com os requisitos de tratamento da Parte Originária.

ARTIGO VII
Acesso a Informações Classificadas

1. Cada Parte deve garantir que o acesso às Informações Classificadas seja concedido com base na Necessidade de Conhecer.

2. Cada Parte deve garantir que qualquer indivíduo a quem tenha sido concedido acesso às Informações Classificadas seja informado sobre suas responsabilidades para proteger tais informações e tenha assinado um termo de confidencialidade, conforme as leis e regulamentos nacionais da Entidade Receptora.

3. As Partes devem garantir que o acesso às Informações Classificadas seja concedido apenas a indivíduos que possuam uma Credencial de Segurança Pessoal no nível correspondente ou que estejam devidamente autorizados a acessar as Informações Classificadas em virtude de suas funções, de acordo com as leis e regulamentos nacionais da Entidade Receptora.

ARTIGO VIII
Tradução, Reprodução e Destruição de Informações Classificadas

1. Todas as traduções e reproduções de Informações Classificadas devem ser protegidas e controladas da mesma forma que as Informações Classificadas originais. Elas devem receber o mesmo Nível de Classificação de Segurança das Informações Classificadas originais.

2. As traduções de Informações Classificadas devem conter uma anotação apropriada no idioma da tradução, indicando que contêm Informações Classificadas da Parte Originária.

3. O número de reproduções de Informações Classificadas deve ser limitado à quantidade necessária para seu propósito oficial.

4. Informações Classificadas com Nível de Classificação de Segurança equivalente a Ultrassecreto/Prísne tajné não devem ser reproduzidas ou traduzidas sem o consentimento prévio por escrito da Parte Originária.

5. Todas as Informações Classificadas devem ser destruídas de acordo com as leis e regulamentos nacionais após não serem mais consideradas necessárias pela Entidade Receptora.

6. Informações Classificadas com Nível de Classificação de Segurança equivalente a Ultrassecreto/Prísne tajné não devem ser destruídas sem o consentimento prévio por escrito da Parte Originária. Elas devem ser devolvidas à Parte Originária após não serem mais consideradas necessárias pela Entidade Receptora.

7. Se uma situação de crise tornar impossível para a Entidade Receptora proteger as Informações Classificadas fornecidas sob este Acordo, as Informações Classificadas deverão ser destruídas imediatamente. A Entidade Receptora deve notificar prontamente por escrito a Autoridade de Segurança Competente da Parte Originária sobre a destruição dessas Informações Classificadas.

ARTIGO IX
Transmissão de Informações Classificadas

1. As Informações Classificadas devem ser transmitidas entre as Partes por meio de canais diplomáticos ou conforme acordado entre as Autoridades de Segurança Competentes, de acordo com as leis e regulamentos nacionais.

2. A transmissão eletrônica de Informações Classificadas só poderá ocorrer através da utilização de meios criptográficos aprovados mutuamente pelas Autoridades de Segurança Competentes.

3. Em caso de transferência de Informações Classificadas que exija procedimentos especiais de transporte, um plano logístico deve ser previamente acordado, por escrito, entre ambas as Autoridades de Segurança Competentes.

ARTIGO X
Visitas

1. Visitas a instalações onde haverá acesso a Informações Classificadas estão sujeitas à aprovação prévia por escrito da Autoridade de Segurança Competente da Parte anfitriã, salvo acordo contrário entre as Autoridades de Segurança Competentes. Tal aprovação será concedida apenas a indivíduos que cumpram os requisitos estabelecidos no artigo VII deste Acordo.

2. A solicitação de visita deve ser submetida à Autoridade de Segurança Competente da Parte anfitriã, incluindo os seguintes dados, a serem utilizados apenas para o propósito da visita:

a) o nome completo do visitante, data e local de nascimento, nacionalidade, outras cidadanias e número de documento de identidade/passaporte;
b) o título e função do visitante, bem como o nome e endereço da organização empregadora ou que o visitante representa;
c) a especificação do projeto no qual o visitante participa;
d) a confirmação da Credencial de Segurança Pessoal do visitante, incluindo nível e validade;
e) o nome da instalação a ser visitada;
f) o propósito da visita;
g) o Nível de Classificação de Segurança mais alto previsto para as Informações Classificadas a serem acessadas, processadas ou armazenadas;
h) nome, endereço, telefone, e-mail e ponto de contato da instalação a ser visitada;
i) a data e duração da visita;

j) o período total quando as visitas forem recorrentes; e
k) a data e assinatura de um representante da Autoridade de Segurança Competente do visitante.

3. A solicitação de visita deve ser submetida pelo menos 10 (dez) dias corridos antes da data proposta para a visita, salvo acordo entre as Autoridades de Segurança Competentes para um período diferente.

4. As Autoridades de Segurança Competentes podem acordar uma lista de visitantes autorizados para visitas recorrentes por um período não superior a 12 (doze) meses. As Autoridades de Segurança Competentes definirão os detalhes adicionais dessas visitas recorrentes.

5. A Autoridade de Segurança Competente da Parte anfitriã informará os oficiais de segurança da organização a ser visitada sobre os detalhes dos indivíduos cujas solicitações de visita foram aprovadas. Após a aprovação, os arranjos de visita para indivíduos com aprovação para visitas recorrentes podem ser feitos diretamente com a agência, instalação ou organização em questão.

6. Qualquer Informação Classificada transmitida ao visitante será considerada Informação Classificada sob este Acordo e deverá ser tratada de acordo com as disposições deste Acordo. Além disso, o visitante deve cumprir os regulamentos de segurança da Parte anfitriã.

7. As Partes devem assegurar, em conformidade com suas leis e regulamentos nacionais, a proteção dos dados pessoais dos indivíduos que solicitam uma visita. Os dados pessoais não devem ser utilizados para qualquer outro propósito além de determinar o pedido de visita.

8. Quando autorizado, a Autoridade de Segurança Competente da Parte anfitriã notificará a Parte solicitante sobre a visita o mais rápido possível e informará a instalação a ser visitada.

ARTIGO XI
Violação de Segurança

1. Sempre que a Entidade Receptora suspeitar ou verificar uma Violação de Segurança relacionada a Informações Classificadas sob este Acordo, a Autoridade de Segurança Competente da Parte onde ocorreu a Violação de Segurança deverá informar imediatamente a Autoridade de Segurança Competente da outra Parte. A notificação deve conter detalhes suficientes para que a Parte Originária avalie as consequências e circunstâncias da Violação de Segurança suspeita ou confirmada.

2. A Autoridade de Segurança Competente da Parte onde ocorreu a Violação de Segurança deverá tomar todas as medidas necessárias, de acordo com suas leis e regulamentos nacionais, para investigar qualquer Violação de Segurança suspeita ou confirmada. A Autoridade de Segurança Competente da Parte Originária pode, se acordado, cooperar na investigação. A Parte Originária será sempre informada sobre o resultado da investigação e as medidas tomadas, se houver.

3. A Autoridade de Segurança Competente da Parte onde ocorreu a Violação de Segurança deverá tomar todas as medidas, incluindo medidas legais, de acordo com suas leis e regulamentos nacionais, para mitigar as consequências de uma Violação de Segurança e prevenir qualquer recorrência.

4. Quando uma Violação de Segurança ocorrer em uma Terceira Parte, a Autoridade de Segurança Competente da Parte que transmitiu a informação à Terceira Parte deverá informar imediatamente a Autoridade de Segurança Competente da Parte Originária sobre a Violação de Segurança, assegurar que a Violação de Segurança seja devidamente investigada e comunicar o resultado da investigação e quaisquer medidas tomadas.

5. Qualquer Parte pode solicitar informações sobre o processo de investigação da Violação de Segurança.

ARTIGO XII
Contratos Classificados

1. Se uma Parte ou um Contratante propuser a celebração de um Contrato Classificado com um Contratante sob a jurisdição da outra Parte, deverá primeiro obter uma confirmação por escrito da Autoridade de Segurança Competente da outra Parte de que o Contratante recebeu uma Autorização de Segurança de Instalação no Nível de Classificação de Segurança apropriado.

2. A Autoridade de Segurança Competente da Parte onde o Contrato Classificado é executado deverá assegurar que o Contratante e, se aplicável, seus subcontratantes:

a) garantam que todos os indivíduos com acesso a Informações Classificadas estejam informados sobre suas responsabilidades para proteger as Informações Classificadas, de acordo com as condições definidas neste Acordo e com as leis e regulamentos nacionais;
b) monitorem a conduta de segurança em suas instalações, conforme as leis e regulamentos nacionais;

c) notifiquem prontamente sua Autoridade de Segurança Competente sobre qualquer Violação de Segurança relacionada ao Contrato Classificado; e
d) possuam uma Autorização de Segurança de Instalação apropriada para proteger as Informações Classificadas e que os indivíduos que precisem acessar as Informações Classificadas possuam uma Credencial de Segurança Pessoal apropriada.

3. Todo Contrato Classificado, incluindo subcontratos classificados celebrados conforme este Acordo, deverá incluir requisitos de segurança que identifiquem os seguintes aspectos:

a) um guia de classificação de segurança, que sempre incluirá a tabela do artigo IV, parágrafo 1, especificando os Níveis de Classificação de Segurança aplicáveis a cada parte do Contrato Classificado;
b) um procedimento para comunicação de mudanças no Nível de Classificação de Segurança;
c) os canais e procedimentos a serem usados para o transporte e/ou transmissão de Informações Classificadas;
d) instruções para o tratamento e armazenamento de Informações Classificadas;
e) os dados de contato das Autoridades de Segurança Competentes responsáveis pela supervisão da proteção de Informações Classificadas relacionadas ao Contrato Classificado; e
f) obrigação de notificar quaisquer Violações de Segurança.

4. A Autoridade de Segurança Competente da Parte que autorizar a concessão do Contrato Classificado deverá enviar uma cópia do capítulo de requisitos de segurança à Autoridade de Segurança Competente da Entidade Receptora, para facilitar a supervisão de segurança do Contrato Classificado.

ARTIGO XIII
Custos

Cada Parte arcará com os custos de suas próprias despesas decorrentes da implementação e supervisão de todos os aspectos deste Acordo, salvo determinação em contrário pelas Partes.

ARTIGO XIV
Resolução de Disputas

1. Qualquer disputa que possa surgir entre as Partes quanto à interpretação ou aplicação deste Acordo, ou qualquer questão relacionada, deverá ser resolvida exclusivamente por meio de consultas e negociações entre as Partes, e não será encaminhada a qualquer tribunal internacional ou Terceira Parte para solução.

2. Durante o período de resolução de disputas, ambas as Partes continuarão a cumprir suas obrigações sob este Acordo.

3. Os procedimentos de resolução de disputas entre ambas as Partes serão conduzidos com base no princípio da confidencialidade.

ARTIGO XV
Comunicação

Todas as comunicações formais entre as Partes, relacionadas à implementação deste Acordo, devem ser feitas por escrito, no idioma inglês.

ARTIGO XVI
Entrada em Vigor

Este Acordo entrará em vigor no primeiro dia do segundo mês após o recebimento da última notificação pela qual as Partes informarão uma à outra, por canais diplomáticos, que cumpriram os requisitos legais internos necessários para sua entrada em vigor.

ARTIGO XVII
Emendas

1. Este Acordo, incluindo seu Anexo, poderá ser emendado a qualquer momento, por escrito, mediante consentimento mútuo entre as Partes. As emendas devem ser propostas por meio de canais diplomáticos.

2. As emendas entrarão em vigor nos termos estabelecidos no artigo XVI deste Acordo, exceto as emendas do Anexo, que entrarão em vigor em uma data a ser acordada pelas Partes.

ARTIGO XVIII
Validade e Rescisão

1. Este Acordo é celebrado por prazo indeterminado.

2. Qualquer das Partes poderá, a qualquer momento, rescindir este Acordo mediante notificação por escrito, por meio de canais diplomáticos, à outra Parte.

3. A rescisão produzirá efeitos 6 (seis) meses após a data de recebimento da notificação pela outra Parte.

4. Após a rescisão, qualquer Informação Classificada trocada, liberada ou gerada sob este Acordo continuará a ser protegida de acordo com os termos deste Acordo antes de sua rescisão, enquanto a Informação Classificada permanecer classificada.

ARTIGO XIX
Disposições Finais

As Autoridades de Segurança Competentes deverão informar-se mutuamente sobre suas respectivas leis e regulamentos nacionais e notificar prontamente uma à outra sobre modificações que afetem a proteção de Informações Classificadas fornecidas sob este Acordo e que tenham impacto sobre o mesmo. Em caso de tais mudanças, as Partes deverão discutir a necessidade de revisar este Acordo.

Feito em Brasília, em 10 de dezembro de 2024, em duas cópias originais, em português, eslovaco e inglês, sendo todos os textos igualmente autênticos. Em caso de divergência de interpretação, prevalecerá o texto em inglês.

Em testemunho, os representantes devidamente autorizados das Partes assinaram este Acordo.

PELA REPÚBLICA FEDERATIVA DO BRASIL

Marcos Antonio Amaro dos Santos
Ministro-Chefe do Gabinete de Segurança Institucional da Presidência da República Federativa do Brasil

PELA REPÚBLICA ESLOVACA

Juraj Blanár
Ministro das Relações Exteriores e Assuntos Europeus

ANEXO

As Autoridades de Segurança Competentes Responsáveis pela Implementação e Supervisão deste Acordo são:

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

Pela República Eslovaca:
Autoridade Nacional de Segurança da República Eslovaca

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

The Federative Republic of Brazil

and

the Slovak Republic,

(hereinafter referred to together as "Parties",
or separately, as "Party"),

In the interests of national security and in order to ensure the protection of Classified Information exchanged within the scope of cooperation instruments, contracts and other agreements signed between the Parties, their accredited individuals, bodies, as well as public and private entities;

Desiring to establish a framework of rules and procedures related to Classified Information in accordance with the national laws and regulations of the Parties;

Confirming that this Agreement will not affect the commitments of both Parties that derive from other international agreements and that it will not be used against the interests, security and territorial integrity of other States;

Have agreed upon the following:

ARTICLE I
Purpose

1. This Agreement establishes rules and procedures for the protection of Classified Information exchanged between the aforementioned Parties, their accredited individuals, bodies, as well as public or private entities under their jurisdiction.

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

ARTICLE II
Definitions

For the purposes of this Agreement, the term:

a) "Agreement" means this agreement including its Annexes;
b) "Annex" means an attachment to this Agreement;
c) "Classified Contract" means an agreement, including any pre-contractual negotiations, the performance of which requires or involves access or potential access to or the creation of Classified Information;
d) "Classified Information" means the information, material or object, regardless of its form or nature or any parts thereof, with a certain Security Classification Level, which regardless of how it is presented must be protected against unauthorized access, disclosure or other type of compromise for which it was designated, to prevent damage or harm in the interests of one or both of the Parties, in accordance with the respective laws and regulations of each Party and this Agreement;
e) "Competent Security Authority (CSA)" means the authority of each Party responsible for the security of Classified Information under this Agreement;
f) "Contractor" means any legal entity under the jurisdiction of a Party, entering into or otherwise bound by a Classified Contract;
g) "Facility Security Clearance (FSC)" means the determination by the Competent Security Authority that a public or private entity has in place appropriate security measures and has therefore been accredited for the Handling of Classified Information, in accordance with the national laws and regulations of each Party;
h) "Handling of Classified Information" means a set of actions related to the production, reception, classification, use, access, reproduction, transport, transmission, distribution, archiving, storage, destruction or control of Classified Information at a certain Security Classification Level;
i) "Need-to-Know" means the requirement for an individual to access, have knowledge of or possess Classified Information for the performance of official functions and tasks;
j) "Originating Party" means the Party under whose authority Classified Information has been created;
k) "Personnel Security Clearance (PSC)" means the determination that a given individual has been security cleared and has therefore been accredited for the Handling of Classified Information, at a given Security Classification Level, in accordance with the national laws and regulations of each Party;
l) "Providing Entity" means the Party, or a Contractor, which provides Classified Information to the Receiving Entity under this Agreement;

m) "Receiving Entity" means the Party, or a Contractor, which receives Classified Information under this Agreement;
n) "Security Breach" means any intentional or accidental action or omission that result in an actual or possible compromise of Classified Information provided or generated under this Agreement;
o) "Security Classification Level" means the level of protection assigned to Classified Information, in accordance with the national laws and regulations of each Party and as incorporated in article IV, paragraph 1 of this Agreement; and
p) "Third Party" means any organization, state, government or individual that is not a Party to this Agreement.

ARTICLE III
Competent Security Authorities

1. The Competent Security Authorities, responsible for the implementation and supervision of this Agreement, are listed in the Annex to this Agreement.

2. The Competent Security Authority may delegate parts of its responsibilities to a delegated competent security authority.

3. Each Party shall provide the other with the contact details of their respective Competent Security Authority, in writing. The Competent Security Authorities of the Parties shall inform each other in writing about changes in their contact details.

4. In order to ensure close cooperation in the implementation of this Agreement, the Competent Security Authorities may consult each other whenever necessary.

5. Representatives of both Competent Security Authorities may mutually visit their facilities with the intention of acquiring knowledge of security procedures and measures applicable to Classified Information, subject to the approval of the host Competent Security Authority.

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

7. Upon request of the Competent Security Authority of one Party, the Competent Security Authority of the other Party shall issue a written confirmation that a valid Personnel Security Clearance and/or Facility Security Clearance has been issued.

8. The Competent Security Authorities of the Parties shall mutually recognize their Personnel Security Clearances and Facility Security Clearances issued in accordance with their respective laws and regulations and within the scope of this Agreement.

9. The Competent Security Authorities shall promptly notify each other in writing about changes in recognized Personnel Security Clearances and Facility Security Clearances for whom or for which a confirmation has been provided according to paragraph 8 of this article.

ARTICLE IV
Security Classification Levels

1. The Parties agree that the Security Classification Levels, in accordance with their respective national laws and regulations, shall correspond to each other in the following form of equivalence:

THE FEDERATIVE REPUBLIC OF BRAZIL AS ORIGINATING PARTY	THE SLOVAK REPUBLIC AS RECEIVING PARTY
ULTRASSECRETO	PRÍSNE TAJNÉ
SECRETO	TAJNÉ
RESERVADO	DÔVERNÉ

THE SLOVAK REPUBLIC AS ORIGINATING PARTY	THE FEDERATIVE REPUBLIC OF BRAZIL AS RECEIVING PARTY
PRÍSNE TAJNÉ	ULTRASSECRETO
TAJNÉ	SECRETO
DÔVERNÉ	RESERVADO
VYHRADENÉ	RESERVADO

2. Any Classified Information produced pursuant to this Agreement shall be marked with the Originating Party's equivalent Security Classification Level in accordance with paragraph 1 of this article.

3. The Receiving Entity shall mark all the Classified Information under this Agreement that it has received from the Providing Entity with the equivalent Security Classification Level of the Receiving Entity in accordance with paragraph 1 of this article.

4. The Parties shall notify each other of any change and subsequent amendment to the Security Classification Level of Classified Information.

5. The Originating Party may mark the Classified Information with handling requirements, to specify any limitation on its use, disclosure, release and access by the Receiving Entity.

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

7. Classified Information jointly originated by the Parties shall be assigned a Security Classification Level that is mutually determined by the Parties.

ARTICLE V
Protection of Classified Information

1. The Parties shall take all appropriate measures under their national laws and regulations to ensure the protection of Classified Information in accordance with this Agreement. They shall afford Classified Information exchanged or generated under this Agreement at least the same protection as they afford to their own Classified Information at the corresponding Security Classification Level.

2. The handling of any Classified Information exchanged between the Parties shall respect the provisions of this Agreement.

3. Each Party shall ensure that the necessary measures are implemented for the protection of Classified Information processed, stored or transmitted by communication and information systems, in accordance with the Security Classification Level, with this Agreement, and with national laws and regulations.

4. Each Party shall ensure confidentiality, integrity, availability and, where applicable, authenticity, accountability and traceability of Classified Information.

5. The Parties shall not disclose any Classified Information without the Originating Party's written consent.

ARTICLE VI
Use of Classified Information

1. Each Party shall ensure that the Providing Entity:

a) marks Classified Information with the appropriate security classification in accordance with its national laws and regulations; and
b) informs the Receiving Entity of any conditions of release or limitations on the use of the Classified Information provided, as determined by the Originating Party.

2. Each Party shall ensure that the Receiving Entity:

a) affords the same level of protection to the Classified Information as afforded to its national Classified Information of an equivalent Security Classification Level as determined in article IV, paragraph I;
b) shall not declassify or downgrade Classified Information without the prior written consent of the Originating Party;
c) shall not release Classified Information to a Third Party without prior written consent of the Originating Party; and
d) shall use Classified Information only for the purposes that it has been released for and in accordance with any handling requirements of the Originating Party.

ARTICLE VII
Access to Classified Information

1. Each Party shall ensure that access to Classified Information is granted on a Need-to-Know basis.

2. Each Party shall ensure that any individual who has been granted access to Classified Information is informed on its responsibilities to protect such information and has signed a statement of confidentiality in accordance with national laws and regulations of the Receiving Entity.

3. The Parties shall ensure that access to Classified Information is granted only to individuals who hold a Personnel Security Clearance at the corresponding level or who are duly authorized to access Classified Information by virtue of their duties pursuant to national laws and regulations of the Receiving Entity.

ARTICLE VIII
Translation, Reproduction and Destruction of Classified Information

1. All translations and reproductions of Classified Information must be protected and controlled in the same manner as the original Classified Information. It shall receive the same Security Classification Level as the original Classified Information.

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

3. The number of reproductions of Classified Information shall be limited to the amount required for its official purpose.

4. Classified Information with Security Classification Level equivalent to Ultrassecreto/Prísne tajné shall not be reproduced or translated without the prior written consent of the Originating Party.

5. All Classified Information shall be destroyed in accordance with national laws and regulations after it is no longer considered necessary by the Receiving Entity.

6. Classified Information with Security Classification Level equivalent to Ultrassecreto/Prísne tajné shall not be destroyed without the prior written consent of the Originating Party. It shall be returned to the Originating Party after it is no longer considered necessary by the Receiving Entity.

7. If a crisis situation makes it impossible for the Receiving Entity to protect Classified Information provided under this Agreement, the Classified Information shall be destroyed immediately. Receiving Entity shall promptly notify in writing the Competent Security Authority of the Originating Party about the destruction of this Classified Information.

ARTICLE IX
Transmission of Classified Information

1. Classified Information shall be transmitted between the Parties, through diplomatic channels or as otherwise agreed between the Competent Security Authorities in accordance with national laws and regulations.

2. Electronic transmission of Classified Information may take place only by using cryptographic means in accordance with procedures mutually approved by the Competent Security Authorities.

3. In the case of transfer of Classified Information that requires special procedures for its transport, a logistical plan must be previously agreed, in writing, by both Competent Security Authorities.

ARTICLE X
Visits

1. Visits to facilities where Classified Information will be accessed are subject to the prior written approval of the Competent Security Authority of the host Party, unless otherwise agreed by the Competent Security Authorities. Such approval will only be granted to individuals who meet the requirements set forth in article VII of this Agreement.

2. The visit request must be submitted to the Competent Security Authority of the host Party, including the following data that will be used only for the purpose of the visit:

a) the visitor's first and last name, date and place of birth, nationality, other citizenships and identification card number/passport number;
b) the visitor's title and function, as well as the name and address of the organization by whom the visitor is employed or that the visitor represents;
c) the specification of the project in which the visitor is participating;
d) the confirmation of the visitor's Personnel Security Clearance and its level and validity;
e) the name of the facility to be visited ;
f) the purpose of the visit;
g) the anticipated highest Security Classification Level of the Classified Information to be accessed, processed or stored;
h) the name, address, phone number, e-mail address and point of contact of the facility to be visited;
i) the date and duration of the visit;
j) the total period when visits are recurring; and
k) the date and signature of a representative of the visitor's Competent Security Authority.

3. The visit request must be submitted at least 10 (ten) calendar days in advance of the proposed visit date, unless the Competent Security Authorities agree on a different period.

4. The Competent Security Authorities may agree on a list of visitors entitled to recurring visits for a period not exceeding 12 (twelve) months. The Competent Security Authorities shall agree on the further details of these recurring visits.

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

6. Any Classified Information transmitted to the visitor shall be deemed Classified Information under this Agreement and shall be handled in accordance with the provisions of this Agreement. In addition, the visitor must comply with the host Party's security regulations.

7. The Parties shall ensure, pursuant to their national laws and regulations, the protection of personal data of the individuals requesting a visit. The personal data shall not be used for any other purpose than determining the request for a visit.

8. When authorized, the Competent Security Authority of the host Party shall notify the requesting Party, as soon as possible, of the visit and also notify the facility to be visited.

ARTICLE XI
Security Breach

1. When a Security Breach related to Classified Information under this Agreement is suspected or ascertained by the Receiving Entity, the Competent Security Authority of the Party where the Security Breach occurred shall immediately inform the Competent Security Authority of the other Party. The notice must contain sufficient details for the Originating Party to assess the consequences and circumstances of the suspected or ascertained Security Breach.

2. The Competent Security Authority of the Party where the Security Breach occurred shall immediately take all necessary steps, in accordance with its national laws and regulations, to investigate any suspected or ascertained Security Breach. The Competent Security Authority of the Originating Party may, if agreed, cooperate in the investigation. The Originating Party shall always be informed about the outcome of the investigation and the measures taken, if any.

3. The Competent Security Authority of the Party where the Security Breach occurred shall take all steps, including but not limited to legal steps, in accordance with its national laws and regulations, to mitigate the consequences of a Security Breach and to prevent any recurrence.

4. When a Security Breach has occurred in a Third Party, the Competent Security Authority of the Party that transmitted the information to the Third Party shall immediately inform the Competent Security Authority of the Originating Party about the Security Breach,

make sure the Security Breach is investigated properly and communicate the outcome of the investigation and any measures taken.

5. Any Party may request information regarding the Security Breach investigation process.

ARTICLE XII
Classified Contracts

1. If a Party or a Contractor proposes to grant a Classified Contract, with a Contractor under the jurisdiction of the other Party, it must first obtain written confirmation from the Competent Security Authority of the other Party that the Contractor has received a Facility Security Clearance at the appropriate Security Classification Level.

2. The Competent Security Authority of the Party where the Classified Contract is performed shall ensure that the Contractor and if applicable its sub-contractor:

a) ensures that all individuals granted access to Classified Information are informed of their responsibilities to protect Classified Information in accordance with the conditions defined in this Agreement and with national laws and regulations;
b) monitors the security conduct within its facilities in accordance with national laws and regulations;
c) notifies promptly its Competent Security Authority of any Security Breach relating to the Classified Contract; and
d) holds an appropriate Facility Security Clearance in order to protect the Classified Information and that the individuals requiring access to Classified Information hold an appropriate Personnel Security Clearance.

3. Every Classified Contract including classified sub-contracts concluded in accordance with this Agreement shall include security requirements which identify the following aspects:

a) a security classification guide, which shall always include the table of article IV, paragraph I specifying the applicable Security Classification Levels of each part of the Classified Contract;
b) a procedure for communication of changes in the Security Classification Level;
c) the channels and procedures to be used for the transport and/or transmission of Classified Information;
d) instructions for the handling and storage of Classified Information;

e) contact details of the Competent Security Authorities responsible for overseeing the protection of Classified Information related to the Classified Contract; and
f) obligation to notify any Security Breaches.

4. The Competent Security Authority of the Party authorising the award of the Classified Contract shall forward a copy of the security requirements chapter, to the Competent Security Authority of the Receiving Entity, to facilitate the security oversight of the Classified Contract.

ARTICLE XIII
Costs

Each Party shall bear the costs of its own expenses resulting from the implementation and supervision of all aspects of this Agreement, unless otherwise mutually determined by the Parties.

ARTICLE XIV
Dispute settlement

1. Any dispute that may arise between the Parties regarding the interpretation or application of this Agreement, or any related matter, shall be resolved exclusively through consultations and negotiations between the Parties and shall not be referred to any international court or Third Party for settlement.

2. During the dispute settlement period, both Parties will continue to fulfil their obligations under this Agreement.

3. Dispute settlement procedures between both Parties shall be conducted based on the principle of confidentiality.

ARTICLE XV
Communication

All formal communications between the Parties relating to the implementation of this Agreement shall be in writing, in the English language.

ARTICLE XVI
Entry into force

This Agreement shall enter into force on the first day of the second month following the receipt of the last notification by which the Parties shall inform each other, through diplomatic channels, that their domestic legal requirements necessary for its entry into force have been fulfilled.

ARTICLE XVII
Amendments

1. This Agreement, including its Annex, may be amended at any time, in writing, by means of amendments and with the mutual consent between the Parties. Amendments shall be proposed through diplomatic channels.

2. The amendments shall enter into force under the terms set out in article XVI of this Agreement, with the exception of amendments of the Annex, which shall enter into force on a date to be agreed upon by the Parties.

ARTICLE XVIII
Validity and Termination

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

2. Either Party may, at any time, terminate this Agreement by giving written notice, through diplomatic channels, to the other Party.

3. Termination shall take effect 6 (six) months after the date on which the other Party receives notice of termination.

4. Upon termination, any Classified Information exchanged, released or generated under this Agreement shall continue to be protected in accordance with the terms of this Agreement before it was terminated, for as long as the Classified Information remains classified.

ARTICLE XIX
Final Dispositions

The Competent Security Authorities shall inform each other about their respective national laws and regulations and shall promptly notify each other about modifications that

affect the protection of Classified Information provided under this Agreement and have an impact on this Agreement. In the event of such changes, the Parties shall discuss the necessity of reviewing this Agreement.

Done in Brasilia, on December 10th, 2024, in two original copies each in the Portuguese, Slovak, and English languages, all texts being equally authentic. In case of divergence of interpretation, the English text shall prevail.

In witness whereof, the duly authorized representatives of the Parties have signed this Agreement.

FOR THE FEDERATIVE REPUBLIC OF BRAZIL	FOR THE SLOVAK REPUBLIC
Marcos Antonio Amaro dos Santos Chief Minister of the Institutional Security Cabinet of the Presidency of the Federative Republic of Brazil	**Juraj Blanár** Minister of Foreign and European Affairs

ANNEX

The Competent Security Authorities, responsible for the implementation and supervision of this Agreement, are:

On behalf of the Federative Republic of Brazil:
The Institutional Security Cabinet of the Presidency of the Federative Republic of Brazil

On behalf of the Slovak Republic:
National Security Authority of the Slovak Republic

DOHODA MEDZI VLÁDOU BRAZÍLSKEJ FEDERATÍVNEJ REPUBLIKY A VLÁDOU SLOVENSKEJ REPUBLIKY O VÝMENE A VZÁJOMNEJ OCHRANE UTAJOVANÝCH SKUTOČNOSTÍ

Vláda Brazílskej Federatívnej Republiky

a

Vláda Slovenskej Republiky,

(ďalej spoločne označované ako „zmluvné strany" a každá z nich jednotlivo ako „zmluvná strana".)

V záujme národnej bezpečnosti a s cieľom zabezpečiť ochranu utajovaných skutočností vymieňaných v rámci spolupráce, zmlúv a iných dohôd podpísaných medzi zmluvnými stranami, ich oprávnenými osobami, subjektmi verejnej moci a súkromného sektora;

Želajúc si vytvoriť rámec pravidiel a postupov týkajúcich sa utajovaných skutočností v súlade s vnútroštátnymi právnymi predpismi zmluvných strán;

Potvrdzujúc, že táto dohoda nebude mať vplyv na záväzky oboch zmluvných strán vyplývajúce z iných medzinárodných dohôd a že nebude použitá proti záujmom, bezpečnosti a územnej celistvosti iných štátov,

Sa dohodli nasledovne:

ČLÁNOK 1
CIEĽ A ROZSAH PÔSOBNOSTI

1. Táto dohoda stanovuje pravidlá a postupy na ochranu utajovaných skutočností vymieňaných medzi uvedenými zmluvnými stranami, ich oprávnenými osobami, subjektmi verejnej moci a súkromného sektora, ktoré spadajú pod výkon právomoci jednej zo zmluvných strán.

2. Táto dohoda nezakladá práva a povinnosti zmluvným stranám, tak aby boli nútené poskytovať alebo nútené vymieňať si utajované skutočnosti.

ČLÁNOK 2
VYMEDZENIE POJMOV

Na účely tejto dohody:

a) „Dohoda" je tento dokument vrátane jeho príloh;
b) „Príloha" je príloha k tomuto dokumentu;
c) „Utajovaná zmluva" je právne vynútiteľná zmluva o poskytovaní tovaru alebo služieb, ktorú uzavrie jedna zo zmluvných strán s kontrahentom alebo medzi kontrahentmi zmluvných strán navzájom, ktorá obsahuje utajované skutočnosti alebo ktorej plnenie si vyžaduje prístup k utajovaným skutočnostiam alebo taký prístup predpokladá na vytváranie, používanie alebo prenos utajovaných skutočností;
d) „Utajované skutočnosti" sú informácie, materiály alebo predmety bez ohľadu na ich formu alebo povahu, alebo časti, označené stupňom utajenia jednou zo zmluvných strán, ktorej vyzradenie, neoprávnená úprava, ohrozenie alebo strata by mohla spôsobiť rôzny rozsah ujmy na záujmoch jednej alebo oboch zmluvných strán;
e) „Príslušný bezpečnostný orgán" je štátny orgán zmluvnej strany zodpovedný za vykonávanie tejto Dohody a dohľad nad ňou;
f) „Kontrahent" je fyzická osoba, právnická osoba alebo iná forma organizácie, spadajúca pod výkon právomoci zmluvnej strany, ktorá je právne spôsobilá uzatvárať utajovanú zmluvu alebo je ňou viazaná;
g) „Previerka priemyselnej bezpečnosti" je potvrdenie vydané príslušným bezpečnostným orgánom, že podnikateľ má zavedené vhodné bezpečnostné opatrenia na prístup k utajovaným skutočnostiam a na ich ochranu do určitého stupňa utajenia, v súlade s vnútroštátnymi právnymi predpismi;
h) „Manipulácia s utajovanými skutočnosťami" je súbor činností súvisiacich s tvorbou, prijímaním, utajením, používaním, prístupom, reprodukciou, prepravou, prenosom, distribúciou, archiváciou, uchovávaním, zničením alebo kontrolou utajovaných skutočností určitého stupňa utajenia;
i) „Need-to-know" je požiadavka na fyzickú osobu, právnickú osobu alebo inú formu organizácie, ktorá má mať prístup, má sa oboznámiť alebo sa u nej utajované skutočnosti uložia, za účelom plnenia svojich úloh a povinností;
j) „Pôvodca" je zmluvná strana, ktorá utajované skutočnosti vytvorila a rozhodla o ich utajení;
k) „Previerka personálnej bezpečnosti" je osvedčenie vydané príslušným bezpečnostným orgánom, že osoba bola bezpečnostne preverená na prístup k utajovaným skutočnostiam a na manipuláciu s nimi do určitého stupňa utajenia, v súlade s vnútroštátnymi právnymi predpismi;
m) „Odovzdávajúca strana" je zmluvná strana alebo kontrahent, ktorý poskytuje utajované skutočnosti prijímajúcej strane na základe tejto Dohody;

n) „Prijímajúca strana“ je zmluvná strana alebo kontrahent, ktorý prijíma utajované skutočnosti od odovzdávajúcej strany podľa tejto Dohody;
o) „Bezpečnostný incident“ je vyzradenie, zmena, ohrozenie, strata, prístup, manipulácia, ukladanie alebo zničenie utajovaných skutočností v rozpore s vnútroštátnymi právnymi predpismi prijímajúcej strany alebo s touto Dohodou;
p) „Stupeň utajenia“ je stupeň ochrany pridelený utajovaným skutočnostiam v súlade s vnútroštátnymi zákonmi a predpismi každej zmluvnej strany a ako je uvedené v článku 4 ods. 1; a
q) „Tretia strana“ je medzinárodná organizácia, vláda alebo štát vrátane fyzických osôb, právnických osôb alebo iných foriem organizácií spadajúcich pod výkon ich právomoci, ktorá nie je zmluvnou stranou tejto Dohody.

ČLÁNOK 3
PRÍSLUŠNÉ BEZPEČNOSTNÉ ORGÁNY

1. Príslušné bezpečnostné orgány zmluvných strán sú uvedené v Prílohe.

2. Príslušný bezpečnostný orgán môže delegovať časť svojich povinností na iný príslušný bezpečnostný orgán.

3. Každá zmluvná strana písomne poskytne druhej zmluvnej strane kontaktné údaje príslušného bezpečnostného orgánu. Príslušné bezpečnostné orgány zmluvných strán sa navzájom písomne informujú o zmenách svojich kontaktných údajov.

4. S cieľom zabezpečiť úzku spoluprácu pri vykonávaní tejto Dohody môžu príslušné bezpečnostné orgány v prípade potreby uskutočniť vzájomné konzultácie.

5. Zástupcovia príslušných bezpečnostných orgánov môžu vzájomne navštíviť svoje zariadenia s cieľom získať poznatky o bezpečnostných postupoch a opatreniach týkajúcich sa utajovaných skutočností, ak to hostiteľský príslušný bezpečnostný orgán schváli.

6. Príslušné bezpečnostné orgány si navzájom poskytujú súčinnosť pri vykonávaní previerok priemyselnej bezpečnosti a previerok personálnej bezpečnosti na požiadanie v súlade so svojimi vnútroštátnymi právnymi predpismi.

7. Na žiadosť príslušného bezpečnostného orgánu jednej zmluvnej strany vydá príslušný bezpečnostný orgán druhej zmluvnej strany písomné potvrdenie, či bola vydaná platná previerka personálnej bezpečnostnej alebo platná previerka priemyselnej bezpečnosti.

8. Príslušné bezpečnostné orgány zmluvných strán uznávajú previerky personálnej bezpečnosti a previerky priemyselnej bezpečnosti vydané v súlade s vnútroštátnymi právnymi predpismi druhej zmluvnej strany a v rozsahu pôsobnosti tejto Dohody.

9. Príslušné bezpečnostné orgány sa navzájom bezodkladne písomne informujú o zmenách majúcich vplyv na uznané previerky personálnej bezpečnosti a previerky priemyselnej bezpečnosti, pre ktoré bolo vydané potvrdenie v súlade s odsekom 8.

ČLÁNOK 4
STUPNE UTAJENIA

1. Zmluvné strany sa dohodli, že nasledujúce stupne utajenia sú rovnocenné a zodpovedajú stupňom utajenia uvedeným vo vnútroštátnych právnych predpisoch zmluvných strán:

BRAZÍLSKA FEDERATÍVNA REPUBLIKA AKO PÔVODCA	**SLOVENSKÁ REPUBLIKA AKO PRIJÍMAJÚCA STRANA**
ULTRASSECRETO	PRÍSNE TAJNÉ
SECRETO	TAJNÉ
RESERVADO	DÔVERNÉ

SLOVENSKÁ REPUBLIKA AKO PÔVODCA	**BRAZÍLSKA FEDERATÍVNA REPUBLIKA AKO PRIJÍMAJÚCA STRANA**
PRÍSNE TAJNÉ	ULTRASSECRETO
TAJNÉ	SECRETO
DÔVERNÉ	RESERVADO
VYHRADENÉ	RESERVADO

2. Utajované skutočnosti vytvorené na základe tejto Dohody sa označia ekvivalentným stupňom utajenia Pôvodcu v súlade s odsekom 1.

3. Prijímajúca strana označí utajované skutočnosti, ktoré prijala od odovzdávajúcej strany alebo ktoré vytvorila podľa tejto Dohody, stupňom utajenia prijímajúcej strany, ktorý zodpovedá stupňu utajenia udelenému pôvodcom v súlade so schémou uvedenou v odseku 1.

4. Zmluvné strany si navzájom oznámia každú zmenu a následnú úpravu stupňa utajenia utajovaných skutočností vymieňaných alebo vytvorených podľa tejto Dohody.

5. Pôvodca môže utajované skutočnosti dodatočne označiť osobitnými požiadavkami na manipuláciu s nimi, aby upresnil všetky obmedzenia ich použitia, sprístupnenia, uvoľnenia a prístupu prijímajúcej strany.

6. Prijímajúca strana nesmie zmeniť alebo zrušiť stupeň utajenia, prijatých utajovaných skutočností podľa tejto Dohody, bez písomného súhlasu pôvodcu.

7. Utajovaným skutočnostiam, ktoré spoločne vytvorili zmluvné strany, sa pridelí stupeň utajenia, ktorý si zmluvné strany určia po vzájomnej dohode.

ČLÁNOK 5
OCHRANA UTAJOVANÝCH SKUTOČNOSTÍ

1. Zmluvné strany poskytnú utajovaným skutočnostiam vymieňaným alebo vytváraným podľa tejto Dohody najmenej takú ochranu, akú poskytujú vlastným utajovaným skutočnostiam zodpovedajúceho stupňa utajenia.

2. Pri manipulácii s utajovanými skutočnosťami, ktoré si zmluvné strany vymieňajú, sa dodržiavajú ustanovenia tejto Dohody.

3. Každá zo Zmluvných strán zabezpečí, aby boli zavedené príslušné bezpečnostné opatrenia na ochranu utajovaných skutočností spracúvaných, uchovávaných alebo prenášaných komunikačnými a informačnými systémami v súlade so stupňom utajenia, s touto Dohodou a s vnútroštátnymi právnymi predpismi.

4. Každá zo Zmluvných strán zabezpečí dôvernosť, integritu, dostupnosť, a ak je to možné pravosť a vysledovateľnosť utajovaných skutočností.

5. Zmluvné strany nezverejnia utajované skutočnosti bez písomného súhlasu pôvodcu.

ČLÁNOK 6
POUŽITIE UTAJOVANÝCH SKUTOČNOSTÍ

1. Zmluvné strany zabezpečia, že poskytujúca strana:

a) označí utajované skutočnosti príslušným stupňom utajenia v súlade so svojimi vnútroštátnymi právnymi predpismi a;
b) informuje prijímajúcu stranu o všetkých podmienkach uvoľnenia alebo obmedzeniach použitia poskytnutých utajovaných skutočností.

2. Zmluvné strany sa uistia, že prijímajúca strana:

a) poskytuje utajovaným skutočnostiam rovnakú úroveň ochrany, akú poskytuje vlastným utajovaným skutočnostiam rovnakého stupňa utajenia podľa Článku 4, odsek 1;
b) nesmie odtajniť alebo znížiť stupeň utajenia utajovaných skutočností bez predchádzajúceho písomného súhlasu pôvodcu;
c) utajované skutočnosti nesprístupní alebo neposkytne tretej strane bez predchádzajúceho písomného súhlasu pôvodcu, ak sa to považuje za potrebné a sú splnené konkrétne podmienky; a
d) používa utajované skutočnosti výlučne na účel, na ktorý jej boli poskytnuté, a v súlade s osobitnými požiadavkami na ich ochranu zo strany pôvodcu.

ČLÁNOK 7
PRÍSTUP K UTAJOVANÝM SKUTOČNOSTIAM

1. Každá zo zmluvných strán zabezpečí, aby sa prístup k utajovaným skutočnostiam udeľoval na základe zásady need-to-know.

2. Každá zo zmluvných strán sa uistí, že prístup k utajovaným skutočnostiam sa udeľuje len tým fyzickým osobám, ktoré sú poučené o svojich povinnostiach pri ochrane utajovaných skutočností a podpísali vyhlásenie o zachovaní mlčanlivosti v súlade s vnútroštátnymi právnymi predpismi prijímajúcej strany.

3. Zmluvné strany sa uistia, že prístup k utajovaným skutočnostiam sa udeľuje len osobám, ktoré sú držiteľmi previerky personálnej bezpečnosti príslušného stupňa alebo ktoré sú inak riadne oprávnené na prístup k utajovaným skutočnostiam z titulu svojej funkcie v súlade s vnútroštátnymi právnymi predpismi prijímajúcej strany.

ČLÁNOK 8
PREKLAD, ROZMNOŽOVANIE A NIČENIE UTAJOVANÝCH SKUTOČNOSTÍ

1. Kópia alebo preklad utajovanej skutočnosti sa označí rovnakým stupňom utajenia, akým je označená pôvodná utajovaná skutočnosť a zabezpečí sa rovnaká úroveň ochrany, ako pôvodnej utajovanej skutočnosti.

2. Na každom preklade utajovanej skutočnosti sa uvedie záznam obsahujúci údaje o pôvodcovi utajovanej skutočnosti, ktorý je vyhotovený v rovnakom jazyku.

3. Vyhotovovanie kópie a prekladu utajovanej skutočnosti sa obmedzí len na nevyhnutné množstvo pre účely tejto Dohody.

4. Utajované skutočnosti označené ekvivalentom stupňa utajenia „ULTRASSECRETO/PRÍSNE TAJNÉ“ sa nesmú rozmnožovať ani prekladať bez predchádzajúceho písomného súhlasu pôvodcu.

5. Všetky utajované skutočnosti sa zničia v súlade s vnútroštátnymi právnymi predpismi po tom, ako ich prijímajúca strana už nepotrebuje pre svoju činnosť.

6. Utajované skutočnosti označené ekvivalentom stupňa utajenia „ULTRASSECRETO/PRÍSNE TAJNÉ“ sa zničia len na základe predchádzajúceho písomného súhlasu pôvodcu. Prijímajúca strana tieto utajované skutočnosti vracia pôvodcovi, ak ich už nepotrebuje pre svoju činnosť.

7. Ak krízová situácia znemožní prijímajúcej strane chrániť utajované skutočnosti poskytnuté podľa tejto Dohody, utajované skutočnosti sa bezodkladne zničia. Prijímajúca strana bezodkladne písomne informuje príslušný bezpečnostný orgán pôvodcu o zničení týchto utajovaných skutočností.

ČLÁNOK 9
PRENÁŠANIE UTAJOVANÝCH SKUTOČNOSTÍ

1. Utajované skutočnosti sa medzi zmluvnými stranami odovzdávajú diplomatickou cestou alebo iným spôsobom dohodnutým medzi príslušnými bezpečnostnými orgánmi v súlade s vnútroštátnymi právnymi predpismi.

2. Elektronické prenášanie utajovaných skutočností sa môže uskutočňovať len pomocou prostriedkov šifrovej ochrany informácií v súlade s postupmi, ktoré schvália príslušné bezpečnostné orgány.

3. V prípade prenosu utajovaných skutočností, ktoré si vyžadujú osobitné postupy pri ich preprave, musia logistický plán vopred písomne odsúhlasiť oba príslušné bezpečnostné orgány.

ČLÁNOK 10
NÁVŠTEVY

1. Návštevy, ktoré si vyžadujú prístup k utajovaným skutočnostiam, podliehajú predchádzajúcemu písomnému súhlasu príslušného bezpečnostného orgánu hostiteľskej strany, pokiaľ sa príslušné bezpečnostné orgány nedohodnú inak. Takýto súhlas sa udelí len osobám, ktoré spĺňajú podmienky stanovené v Článku 7.

2. Žiadosť o návštevu sa musí predložiť príslušnému bezpečnostnému orgánu hostiteľskej strany vrátane nasledujúcich údajov, ktoré sa použijú len na účely návštevy:

a) meno a priezvisko návštevníka, dátum a miesto narodenia, štátna príslušnosť, prípadne iné občianstvo a číslo preukazu totožnosti/číslo pasu;
b) titul a funkciu návštevníka, ako aj názov a adresu organizácie, v ktorej je návštevník zamestnaný alebo ktorú zastupuje;
c) špecifikáciu projektu, na ktorom sa návštevník zúčastňuje;
d) potvrdenie o previerke personálnej bezpečnosti návštevníka, o jej stupni a platnosti;
e) názov subjektu, ktorý sa má navštíviť;
f) účel návštevy;
g) predpokladaný najvyšší stupeň utajenia utajovaných skutočností, ku ktorým sa má pristupovať, ktoré sa majú spracúvať alebo uchovávať;
h) názov, adresu, telefónne číslo, e-mailovú adresu a kontaktnú osobu zariadenia, ktoré má byť navštívené;
i) dátum a trvanie návštevy;
j) celkové obdobie, počas ktorého sa návštevy opakujú, a
k) dátum a podpis zástupcu príslušného bezpečnostného orgánu návštevníka.

3. Žiadosť o návštevu sa musí predložiť najmenej 10 (desať) kalendárnych dní pred navrhovaným dátumom návštevy, pokiaľ sa príslušné bezpečnostné orgány nedohodnú na inej lehote.

4. Príslušné bezpečnostné orgány sa môžu dohodnúť na zozname návštevníkov oprávnených na opakované návštevy na obdobie nepresahujúce dvanásť mesiacov. Príslušné bezpečnostné orgány sa dohodnú na ďalších podrobnostiach opakovaných návštev.

5. Príslušný bezpečnostný orgán hostiteľskej strany informuje bezpečnostného zamestnanca organizácie, ktorá sa má navštíviť, o podrobnostiach týkajúcich sa osôb, ktorých žiadosť o návštevu bola schválená. Po udelení súhlasu sa môže návšteva jednotlivcov, ktorým bola schválená opakovaná návšteva, dohodnúť priamo s príslušným orgánom alebo organizáciou.

6. S utajovanými skutočnosťami, ktoré návštevník poskytne alebo získa, sa zaobchádza v súlade s ustanoveniami tejto Dohody. Okrem toho musí návštevník dodržiavať bezpečnostné predpisy hostiteľskej strany.

7. Zmluvné strany zabezpečia v súlade so svojimi vnútroštátnymi právnymi predpismi ochranu osobných údajov osôb, ktoré žiadajú o návštevu vyžadujúcu prístup k utajovaným skutočnostiam. Tieto osobné údaje sa nesmú použiť na iný účel ako vo veci rozhodnutia o žiadosti o návštevu.

8. Ak je návšteva povolená, príslušný bezpečnostný orgán hostiteľskej strany o nej čo najskôr informuje žiadajúcu stranu a zariadenie, ktoré sa má navštíviť.

ČLÁNOK 11
BEZPEČNOSTNÝ INCIDENT

1. V prípade, že prijímajúca strana má podozrenie alebo zistí porušenie ochrany utajovaných skutočností pôvodcom, čo najskôr o tom písomne informuje svoj príslušný bezpečnostný orgán. Oznámenie musí obsahovať dostatočné podrobnosti, aby mohol pôvodca posúdiť dôsledky a okolnosti podozrenia alebo skutočného porušenia.

2. Príslušný bezpečnostný orgán zmluvnej strany, v ktorej došlo k porušeniu bezpečnosti, bezodkladne podnikne všetky potrebné kroky v súlade so svojimi vnútroštátnymi právnymi predpismi na vyšetrenie podozrenia alebo zisteného porušenia bezpečnosti. Príslušný bezpečnostný orgán pôvodcu môže na základe dohody spolupracovať pri vyšetrovaní. Pôvodca je vždy informovaný o výsledku vyšetrovania a prípadných prijatých bezpečnostných opatreniach.

3. Príslušný bezpečnostný orgán zmluvnej strany, v ktorej došlo k porušeniu bezpečnosti, zamedzí ďalšiemu porušeniu a môže podniknúť právne kroky, v súlade so svojimi vnútroštátnymi právnymi predpismi, aby zmiernil následky porušenia bezpečnosti a zabránil jeho opakovaniu.

4. Ak dôjde k porušeniu bezpečnosti u tretej strany, príslušný bezpečnostný orgán zmluvnej strany, ktorá odovzdala utajované skutočnosti tretej strane, bezodkladne informuje príslušný bezpečnostný orgán pôvodcu o porušení bezpečnosti, zabezpečí riadne vyšetrenie bezpečnostného incidentu a oznámi výsledok vyšetrovania a všetky prijaté opatrenia.

5. Každá zo zmluvných strán môže požiadať o informácie týkajúce sa procesu vyšetrovania bezpečnostného incidentu.

ČLÁNOK 12
UTAJOVANÉ ZMLUVY

1. Ak zmluvná strana alebo kontrahent navrhuje uzavrieť utajovanú zmluvu so zmluvnou stranou, spadajúcou pod výkon právomoci zmluvnej strany, musí najprv získať písomné potvrdenie od príslušného bezpečnostného orgánu druhej zmluvnej strany, že kontrahent získal previerku priemyselnej bezpečnosti na príslušný stupeň utajenia.

2. Príslušný bezpečnostný orgán zmluvnej strany, v ktorej sa utajovaná zmluva vykonáva, zabezpečí, aby kontrahent a prípadne jeho subdodávateľ:

a) informoval všetky osoby, ktorým bol udelený prístup k utajovaným skutočnostiam, o svojich povinnostiach chrániť utajované skutočnosti v súlade s podmienkami vymedzenými v tejto Dohode a v súlade so svojimi vnútroštátnymi právnymi predpismi;
b) monitoroval bezpečnostné správanie vo svojich zariadeniach;
c) bezodkladne oznámil svojmu príslušnému bezpečnostnému orgánu akýkoľvek bezpečnostný incident vyplývajúci z utajovanej zmluvy; a
d) spĺňal všetky podmienky ochrany utajovaných skutočností a bol držiteľom platnej previerky priemyselnej bezpečnosti a aby osoby, ktoré potrebujú prístup k utajovaným skutočnostiam, mali platnú previerku personálnej bezpečnosti na príslušný stupeň utajenia.

3. Každá utajovaná zmluva vrátane utajovaných subdodávateľských zmlúv, uzavretých v súlade s touto Dohodou, musí obsahovať bezpečnostné požiadavky, ktoré obsahujú najmä tieto časti:

a) príručku určovania stupňov utajenia, vrátane tabuľky uvedenej v článku 4 ods. 1, v ktorej sú špecifikované príslušné stupne utajenia každej časti utajovanej zmluvy;
b) postup oznamovania zmien stupňa utajenia;
c) spôsoby a postupy, ktoré sa majú používať na prepravu alebo prenos utajovaných skutočností
d) pokyny na manipuláciu s utajovanými skutočnosťami, ich ukladanie, ničenie a vrátenie;
e) kontaktné údaje príslušných bezpečnostných orgánov zodpovedných za dohľad nad ochranou utajovaných skutočností súvisiacich s utajovanou zmluvou; a
f) povinnosť oznámiť každý bezpečnostný incident.

4. Príslušný bezpečnostný orgán zmluvnej strany alebo kontrahenta, ktorý uzavrel utajovanú zmluvu, zašle kópiu bezpečnostných požiadaviek príslušnému bezpečnostnému orgánu prijímajúcej zmluvnej strany s cieľom uľahčiť kontrolu nad dodržiavaním utajovanej zmluvy.

ČLÁNOK 13
NÁKLADY

Každá zmluvná strana znáša svoje vlastné náklady, ktoré jej vznikli v priebehu vykonávania a plnenia jej povinností podľa tejto Dohody, pokiaľ zmluvné strany vzájomne neurčia inak.

ČLÁNOK 14
RIEŠENIE SPOROV

1. Akýkoľvek spor vyplývajúci z výkladu, vykonávania alebo uplatňovania tejto Dohody sa rieši výlučne prostredníctvom konzultácií alebo rokovaní medzi zmluvnými stranami a nepredkladá sa na riešenie žiadnemu vnútroštátnemu alebo medzinárodnému súdu alebo tretej strane.
2. Počas obdobia urovnávania sporov budú obe zmluvné strany naďalej plniť svoje povinnosti vyplývajúce z tejto Dohody.
3. Postupy urovnávania sporov medzi oboma zmluvnými stranami sa uskutočňujú na základe zásady dôvernosti.

ČLÁNOK 15
KOMUNIKÁCIA

Všetka formálna komunikácia medzi zmluvnými stranami týkajúca sa vykonávania tejto Dohody sa uskutočňuje písomne v anglickom jazyku.

ČLÁNOK 16
NADOBUDNUTIE PLATNOSTI

Táto Dohoda nadobúda platnosť prvým dňom druhého mesiaca nasledujúceho po prijatí posledného oznámenia, ktorým sa zmluvné strany diplomatickou cestou navzájom informujú o splnení svojich vnútroštátnych právnych požiadaviek potrebných na nadobudnutie jej platnosti.

ČLÁNOK 17
ZMENY A DOPLNENIA

1. Táto Dohoda sa môže meniť a dopĺňať so vzájomným súhlasom zmluvných strán. Ktorákoľvek zmluvná strana môže kedykoľvek navrhnúť zmeny a doplnenia tejto Dohody diplomatickou cestou.

2. Takéto zmeny a doplnenia nadobudnú platnosť za podmienok stanovených v článku 16, s výnimkou zmeny a doplnenia prílohy, ktorá nadobudne platnosť v deň, na ktorom sa zmluvné strany dohodnú.

ČLÁNOK 18
PLATNOSŤ A UKONČENIE PLATNOSTI

1. Táto Dohoda sa uzatvára na dobu neurčitú.

2. Zmluvná strana môže túto Dohodu kedykoľvek písomne vypovedať diplomatickou cestou.

3. Ukončenie zmluvy nadobúda účinnosť 6 (šesť) mesiacov odo dňa, keď druhá zmluvná strana dostane oznámenie o ukončení zmluvy.

4. V prípade ukončenia tejto Dohody zostávajú všetky utajované skutočnosti vymenené, sprístupnené alebo vytvorené na základe tejto Dohody chránené v súlade s podmienkami tejto Dohody pred jej ukončením, pokiaľ to ich povaha a klasifikácia umožňuje.

ČLÁNOK 19
ZÁVEREČNÉ USTANOVENIA

Príslušné bezpečnostné orgány sa navzájom informujú o svojich vnútroštátnych zákonoch a iných právnych predpisoch a bezodkladne sa informujú o zmenách, ktoré majú vplyv na ochranu utajovaných skutočností poskytovaných na základe tejto Dohody a majú vplyv na túto Dohodu. V prípade takýchto zmien zmluvné strany prerokujú potrebu revízie tejto Dohody.

Dané v Brazílii dňa 10. decembra 2024 v dvoch pôvodných vyhotoveniach v portugalskom, slovenskom a anglickom jazyku, pričom všetky znenia sú rovnako autentické. V prípade rozdielneho výkladu je rozhodujúce znenie v anglickom jazyku.

Na dôkaz toho zástupcovia zmluvných strán, riadne na to splnomocnení, podpísali túto Dohodu.

ZA BRAZÍLSKU FEDERATÍVNU REPUBLIKU	ZA SLOVENSKÚ REPUBLIKU
Marcos Antonio Amaro dos Santos	**Juraj Blanár**

PRÍLOHA

Príslušné bezpečnostné orgány zodpovedné za vykonávanie tejto Dohody a dohľad nad ňou sú:

Príslušným bezpečnostným orgánom pre Brazílsku federatívnu republiku je:
Inštitucionálny bezpečnostný kabinet Úrad prezidenta Brazílskej federatívnej republiky

Príslušným bezpečnostným orgánom pre Slovenskú republiku je:
Národný bezpečnostný úrad Slovenskej republiky