PRESIDÊNCIA DO CONSELHO DE MINISTROS

Decreto n.º 6/2020

de 19 de outubro

Sumário: Aprova o Acordo entre a República Portuguesa e a República da Croácia sobre a Proteção Mútua de Informação Classificada, assinado em Zagreb, em 30 de junho de 2020.

O Acordo entre a República Portuguesa e a República da Croácia sobre a Proteção Mútua de Informação Classificada foi assinado em Zagreb, em 30 de junho de 2020.

Com o Acordo sobre a Proteção Mútua de Informação Classificada, a República Portuguesa e a República da Croácia estabelecem as regras para garantir a proteção da informação classificada criada em comum ou trocada entre si.

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

Assim:

Nos termos da alínea *c*) do n.º 1 do artigo 197.º da Constituição, o Governo aprova o Acordo entre a República Portuguesa e a República da Croácia sobre a Proteção Mútua de Informação Classificada, assinado em Zagreb, em 30 de junho de 2020, cujo texto, nas versões autenticadas, nas línguas portuguesa, croata e inglesa, se publica em anexo.

Visto e aprovado em Conselho de Ministros de 1 de outubro de 2020. — *Pedro Gramaxo de Carvalho Siza Vieira — Augusto Ernesto Santos Silva — Mariana Guimarães Vieira da Silva.*

Assinado em 7 de outubro de 2020.

Publique-se.

O Presidente da República, Marcelo Rebelo de Sousa.

Referendado em 9 de outubro de 2020.

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

ACORDO ENTRE A REPÚBLICA PORTUGUESA E A REPÚBLICA DA CROÁCIA SOBRE A PROTEÇÃO MÚTUA DE INFORMAÇÃO CLASSIFICADA

A República Portuguesa e a República da Croácia (doravante designadas por Partes),

Reconhecendo que a boa cooperação pode requerer troca de Informação Classificada entre as Partes,

Desejando estabelecer um conjunto de regras sobre a proteção mútua da Informação Classificada trocada ou criada no decurso da cooperação entre as Partes,

Acordam no seguinte:

Artigo 1.º

Objeto e Âmbito de Aplicação

O presente Acordo estabelece as regras para garantir a proteção da Informação Classificada criada em comum ou trocada entre as Partes.

Artigo 2.º

Definições

Para efeitos do presente Acordo:

(1) «Informação Classificada» designa qualquer informação, independentemente da sua forma, que necessite de proteção contra quebra de segurança e que tenha sido marcada com um grau de classificação de segurança apropriado de acordo com o Direito interno da Parte Transmissora;

(2) «Necessidade de Conhecer» designa a necessidade de ter acesso a Informação Classificada no âmbito de determinada posição oficial e para o desempenho de uma tarefa específica;

(3) «Quebra de Segurança» designa qualquer forma de divulgação não autorizada, uso indevido, alteração, dano ou destruição de Informação Classificada, bem como qualquer ação ou omissão que resulte na perda da sua confidencialidade, integridade e disponibilidade;

(4) «Parte Transmissora» designa a parte que criou a Informação Classificada;

(5) «Parte Destinatária» designa a Parte à qual a Informação Classificada da Parte Transmissora foi transmitida;

(6) «Autoridade Nacional de Segurança» designa a autoridade nacional responsável pela implementação e supervisão do presente Acordo;

(7) «Autoridade Competente» designa a Autoridade Nacional de Segurança ou outra autoridade nacional que, de acordo com o Direito interno, implementa o presente Acordo;

(8) «Contratante» significa uma pessoa singular ou coletiva que tem capacidade jurídica para celebrar Contratos Classificados;

(9) «Contrato Classificado» designa um acordo entre dois ou mais contratantes, que contém ou cuja execução envolve acesso a Informação Classificada;

(10) «Credenciação de Segurança Pessoal» designa a decisão pela Autoridade Nacional de Segurança que confirma que, de acordo com o Direito interno, o indivíduo é elegível para ter acesso a Informação Classificada;

(11) «Credenciação de Segurança Física» designa a decisão pela Autoridade Nacional de Segurança que confirma que, de acordo com o Direito interno, a pessoa coletiva ou singular tem as capacidades físicas e organizacionais para cumprir as condições de acesso e manuseamento de Informação Classificada;

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

Artigo 3.º

Graus de Classificação de Segurança

As Partes acordam que os seguintes graus de classificação de segurança são equivalentes:

Para a República Portuguesa	Para a República da Croácia	Equivalente em Língua Inglesa
MUITO SECRETO	VRLOTAJNO	TOP SECRET
SECRETO	TAJNO	SECRET
CONFIDENCIAL	POVJERLJIVO	CONFIDENTIAL
RESERVADO	OGRANIČENO	RESTRICTED

Artigo 4.º

Autoridades Nacionais de Segurança

1 — As Autoridades Nacionais de Segurança das Partes são:

Pela República Portuguesa:

Autoridade Nacional de Segurança;

Pela República da Croácia:

Gabinete do Conselho Nacional de Segurança.

2 — As Autoridades Nacionais de Segurança fornecerão uma à outra os seus dados de contacto oficiais.

3 — As Partes informar-se-ão mutuamente através da via diplomática sobre as mudanças das Autoridades Nacionais de Segurança, as quais não constituem emendas ao presente Acordo.

4 — A pedido, as Autoridades Nacionais de Segurança informar-se-ão mutuamente sobre o Direito interno em vigor aplicável à proteção de Informação Classificada e trocarão informação sobre os padrões de segurança, procedimentos e práticas para a proteção de Informação Classificada.

Artigo 5.º

Medidas de Proteção e Acesso a Informação Classificada

1 — De acordo com o respetivo Direito interno, as Partes tomam todas as medidas apropriadas para a proteção da Informação Classificada que é trocada ou criada ao abrigo do presente acordo.

2 — O mesmo grau de proteção é assegurado pelas Partes para a referida Informação Classificada conforme marcado para a Informação Classificada nacional de grau de classificação de segurança equivalente, tal como definido no Artigo 3.º do presente Acordo.

3 — A Parte Transmissora informa a Parte Destinatária, por escrito, sobre quaisquer alterações da classificação de segurança da Informação Classificada transmitida, por forma a serem aplicadas as medidas de segurança apropriadas.

4 — A Informação Classificada só será acessível a pessoas autorizadas, de acordo com o Direito interno, a ter acesso a Informação Classificada de grau de classificação de segurança equivalente e que tenham Necessidade de Conhecer.

5 — Nos termos do presente Acordo, cada Parte reconhecerá a Credenciação de Segurança Pessoal e a Credenciação de Segurança Física atribuída pela outra Parte.

6 — A pedido e em conformidade com o Direito interno, as Autoridades Nacionais de Segurança prestam assistência mútua durante os procedimentos de credenciação de segurança necessários à aplicação do presente Acordo.

7 — Nos termos do presente Acordo, as Autoridades Nacionais de Segurança informar-se-ão prontamente sobre qualquer alteração relativa à Credenciação de Segurança Pessoal e à Credenciação de Segurança Física, em particular nos casos de revogação ou alteração do grau de classificação de segurança.

8 — Mediante pedido da Autoridade Nacional de Segurança da Parte Transmissora, a Autoridade Nacional de Segurança da Parte Destinatária emitirá uma confirmação escrita de que um indivíduo pode aceder a Informação Classificada.

9 — A Parte Destinatária:

a) Apenas transmitirá Informação Classificada a uma Terceira Parte mediante consentimento prévio, por escrito, da Parte Transmissora;

b) Marcará a Informação Classificada recebida em conformidade com a equivalência dos graus de classificação de segurança definida no Artigo 3.º;

c) Utilizará a Informação Classificada apenas com a finalidade para a qual foi transmitida.

10 — Representantes das Autoridades Competentes podem efetuar visitas mútuas por forma a analisar a eficiência das medidas adotadas para a proteção da Informação Classificada.

Artigo 6.º

Transmissão de Informação Classificada

1 — A Informação Classificada será transmitida entre as Partes, em conformidade com o Direito interno da Parte Transmissora, normalmente por via diplomática, ou por qualquer outro meio acordado entre as Autoridades Competentes.

2 — A Parte Destinatária confirmará, por escrito, a receção da Informação Classificada de grau CONFIDENCIAL/POVJERLJIVO/CONFIDENTIAL ou superior.

Artigo 7.º

Reprodução e Tradução de Informação Classificada

1 — A Informação Classificada marcada com o grau SECRETO /TAJNO/SECRET ou superior só pode ser traduzida ou reproduzida em casos excecionais mediante consentimento prévio, por escrito, da Parte Transmissora.

2 — Todas as reproduções de Informação Classificada são marcadas da mesma forma e sujeitas ao mesmo controle que a informação original e o número de reproduções é limitado ao necessário para fins oficiais.

3 — A tradução é marcada da mesma forma que a classificação de segurança original e tem uma anotação apropriada na língua para a qual é traduzida indicando que contém Informação Classificada da Parte Transmissora.

Artigo 8.º

Destruição de Informação Classificada

1 — A Informação Classificada é destruída por forma a eliminar a possibilidade da sua parcial ou total reconstrução.

2 — Informação classificada com grau MUITO SECRETO/VRLOTAJNO/TOP SECRET não é destruída e é devolvida à Parte Transmissora logo que deixe de ser considerada necessária.

3 — A Parte Transmissora pode, por marcação adicional ou por uma notificação por escrito subsequente, proibir a destruição de Informação Classificada, a qual lhe será, nesse caso, devolvida.

4 — No caso de uma situação de crise em que é impossível proteger ou devolver a Informação Classificada transmitida ou gerada nos termos do presente Acordo, a Informação Classificada é destruída imediatamente e a Parte Destinatária notifica, logo que possível, a Autoridade Nacional de Segurança da Parte Transmissora sobre tal destruição.

Artigo 9.º

Contratos Classificados

1 — No caso de Contratos Classificados executados no território de uma das Partes, a Autoridade Nacional de Segurança da outra Parte entregará uma garantia escrita prévia de que o contratante proposto detém uma Credenciação de Segurança Física de grau de classificação de segurança apropriado.

2 — O contratante ou subcontratante assegura, em conformidade com o Direito interno, que todas as pessoas com acesso a Informação Classificada estão informadas da sua responsabilidade para com a proteção da Informação Classificada.

3 — Qualquer das Autoridades Nacionais de Segurança pode solicitar à outra uma inspeção de segurança numa instalação situada no território da outra Parte por forma a assegurar o contínuo cumprimento dos padrões de segurança em conformidade com o respetivo Direito interno.

4 — Os Contratos Classificados celebrados entre Contratantes das Partes nos termos das disposições do presente Acordo incluirão uma secção de segurança apropriada identificando, pelo menos, os seguintes aspetos:

a) Lista da Informação Classificada envolvida no Contrato Classificado e respetiva classificação de segurança;

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

c) Canais de comunicação e meios para transmissão eletromagnética;

d) Procedimentos para o transporte da Informação Classificada;

e) Obrigação de notificar a existência ou suspeita de qualquer divulgação não autorizada, apropriação indevida ou perda da Informação Classificada.

5 — Uma cópia da secção de segurança dos Contratos Classificados é remetida à Autoridade Competente da Parte em cujo território o Contrato Classificado será executado, por forma a garantir a adequada supervisão de segurança e controlo.

Artigo 10.º

Visitas

1 — As visitas que envolvam acesso a Informação Classificada estão sujeitas a autorização prévia, por escrito, conferida pelas Autoridades Nacionais de Segurança, em conformidade como respetivo Direito interno, com exceção das visitas que envolvam acesso a Informação Classificada de grau RESERVADO/OGRANIČENO/RESTRICTED, as quais podem ser acordadas diretamente entre os encarregados de segurança das respetivas entidades.

2 — O pedido de visita é submetido através da Autoridade Nacional de Segurança da Parte anfitriã pelo menos vinte (20) dias antes da visita e inclui:

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

b) O nome da entidade que o visitante representa;

c) Nome e morada da entidade a visitar incluindo o nome e número de telefone do ponto de contacto;

d) Confirmação da Credenciação de Segurança Pessoal do visitante e da sua validade;

e) Propósito da visita, incluindo o grau mais elevado da Informação Classificada envolvida;

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

g) A data, a assinatura e a aposição do selo oficial da Autoridade Nacional de Segurança.

3 — Em caso de urgência, o pedido de visita é submetido com pelo menos sete (7) dias de antecedência.

4 — A Autoridade Nacional de Segurança da Parte que recebe o pedido de visita informa, atempadamente, a Autoridade Nacional de Segurança da Parte requerente sobre a decisão.

5 — As visitas de indivíduos de uma Terceira Parte que envolvam acesso a Informação Classificada da Parte Transmissora apenas podem ser autorizadas por consentimento escrito da Autoridade Nacional de Segurança da Parte Transmissora.

6 — A Autoridade Nacional de Segurança da Parte anfitriã providenciará uma cópia do pedido de visita aprovado aos encarregados de segurança da entidade a ser visitada.

7 — A validade da autorização de visita não excederá os doze (12) meses.

8 — As Autoridades Nacionais de Segurança podem acordar estabelecer uma lista de pessoas autorizadas a efetuar visitas recorrentes, válida por um período inicial de doze (12) meses, o qual, mediante acordo, pode ser prorrogado por um período adicional que não exceda outros doze (12) meses.

9 — Após a lista de visitas recorrentes ter sido aprovada pelas Autoridades Nacionais de Segurança, os termos das visitas específicas são diretamente acordados com os encarregados de segurança das entidades a serem visitadas.

10 — Qualquer Informação Classificada acedida por um visitante deve ser considerada Informação Classificada divulgada sob o presente Acordo.

Artigo 11.º

Quebra de Segurança

1 — Se ocorrer uma Quebra de Segurança ou suspeita de tal, a Autoridade Nacional de Segurança da Parte onde a mesma tenha ocorrido informa por escrito, sem demora, a Autoridade

Nacional de Segurança da Parte Transmissora e inicia os procedimentos apropriados, em conformidade com o Direito interno, por forma a apurar as circunstâncias da Quebra de Segurança, a extensão dos danos e as medidas adotadas para a sua mitigação.

2 — As conclusões dos referidos procedimentos serão comunicadas à Autoridade Nacional de Segurança da Parte Transmissora.

3 — Se ocorrer uma Quebra de Segurança no território de um Estado terceiro, a Autoridade Nacional de Segurança da Parte Transmissora levará a cabo, sem demora, as ações previstas nos números 1 e 2 do presente Artigo.

4 — A outra Parte, se necessário, coopera nos procedimentos referidos no n.º 1 do presente Artigo.

Artigo 12.º

Encargos

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

Artigo 13.º

Solução de Controvérsias

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

Artigo 14.º

Revisão

1 — O presente acordo pode ser objeto de revisão, por consentimento mútuo escrito das Partes.

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

Artigo 15.º

Vigência e Denúncia

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

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

3 — A denúncia do presente Acordo produzirá os seus efeitos seis (6) meses após a referida notificação.

4 — Não obstante a denúncia, toda a Informação Classificada transmitida ao abrigo do presente Acordo continuará a ser protegida em conformidade com as disposições do mesmo, até que a Parte Transmissora dispense a Parte Destinatária desta obrigação.

Artigo16.º

Entrada em vigor

O presente Acordo entra em vigor trinta (30) dias após a data de receção da última notificação, por escrito e por via diplomática, informando que foram cumpridos os procedimentos internos necessários de cada Parte para esse efeito.

Artigo 17.º

Registo

Após a entrada em vigor do presente Acordo, a Parte em cujo território o Acordo for assinado submetê-lo-á para registo junto do Secretariado das Nações Unidas, nos termos do Artigo 102.º da

Carta das Nações Unidas, e notificará a outra Parte da conclusão deste procedimento, indicando-lhe o respetivo número de registo.

Feito em Zagreb, aos 30 de junho de 2020, em dois originais, cada um nas línguas Portuguesa, Croata e Inglesa, sendo todos os textos autênticos. Em caso de divergência de interpretação, o texto na língua inglesa prevalecerá.

Pela República Portuguesa:

Jorge Silva Lopes, Embaixador de Portugal.

Pela República da Croácia:

Maja Čavlović, Diretora do Gabinete do Conselho Nacional de Segurança.

UGOVOR IZMEĐU PORTUGALSKE REPUBLIKE I REPUBLIKE HRVATSKE O UZAJAMNOJ ZAŠTITI KLASIFICIRANIH PODATAKA

Portugalska Republika i Republika Hrvatska (u daljnjem tekstu „stranke“),

shvaćajući da dobra suradnja može zahtijevati razmjenu klasificiranih podataka između stranaka,

želeći uspostaviti skup pravila koja uređuju uzajamnu zaštitu klasificiranih podataka koji se razmjenjuju ili nastaju tijekom suradnje između stranaka,

sporazumjele su se kako slijedi:

Članak 1.

Svrha i područje primjene

Ovaj Ugovor uspostavlja pravila za osiguravanje zaštite klasificiranih podataka koji zajednički nastaju ili se razmjenjuju između stranaka.

Članak 2.

Definicije

Za potrebe ovog Ugovora:

(1) „klasificirani podaci“označava bilo koje podatke, neovisno o obliku, koje treba zaštititi od povrede sigurnosti i koji su klasificirani u skladu s nacionalnim zakonima i propisima stranke pošiljateljice;

(2) „nužnost pristupa podacima za obavljanje poslova iz djelokruga“označava nužnost pristupa klasificiranim podacima u okviru radnog mjesta i za obavljanje određenog zadatka;

(3) „povreda sigurnosti“označava bilo koji oblik neovlaštenog otkrivanja, zlouporabe, izmjene, oštećivanja ili uništavanja klasificiranih podataka, kao i bilo koje drugo činjenje ili nečinjenje, čiji je rezultat gubitak njihove povjerljivosti, cjelovitosti ili dostupnosti;

(4) „stranka pošiljateljica“označava stranku koja je stvorila klasificirane podatke;

(5) „stranka primateljica“označava stranku kojoj se prenose klasificirani podaci stranke pošiljateljice;

(6) „nacionalno sigurnosno tijelo“označava nacionalno tijelo odgovorno za provedbu i nadzor ovog Ugovora;

(7) „nadležno tijelo“označava nacionalno sigurnosno tijelo ili drugo nacionalno tijelo koje, u skladu s nacionalnim zakonima i propisima, provodi ovaj Ugovor;

(8) „ugovaratelj“označava fizičku ili pravnu osobu koja ima pravnu sposobnost sklapanja klasificiranih ugovora;

(9) „klasificirani ugovor“označava ugovor između dva ili više ugovaratelja koji sadrži klasificirane podatke ili čija provedba zahtijeva pristup klasificiranim podacima;

(10) „uvjerenje o sigurnosnoj provjeri osobe“označava potvrdu nadležnog sigurnosnog tijela kojom se, u skladu s nacionalnim zakonima i propisima, potvrđuje da fizička osoba ispunjava uvjete za pristup klasificiranim podacima;

(11) „uvjerenje o sigurnosnoj provjeri pravne osobe“označava potvrdu nadležnog sigurnosnog tijela kojom se, u skladu s nacionalnim zakonima i propisima, potvrđuje da pravna ili fizička osoba ima fizičke i organizacijske kapacitete kojima se ispunjavaju uvjeti za pristup i postupanje s klasificiranim podacima;

(12) „treća strana“označava bilo koju državu, organizaciju ili pravnu osobu koja nije stranka ovog Ugovora.

Članak 3.

Stupnjevi tajnosti

Stranke su suglasne da su sljedeći stupnjevi tajnosti istoznačni:

Za Portugalsku Republiku	Za Republiku Hrvatsku	Istoznačnica na engleskom
MUITO SECRETO	VRLO TAJNO	TOP SECRET
SECRETO	TAJNO	SECRET
CONFIDENCIAL	POVJERLJIVO	CONFIDENTIAL
RESERVADO	OGRANIČENO	RESTRICTED

Članak 4.

Nacionalna sigurnosna tijela

1 — Nacionalna sigurnosna tijela stranaka su:

Za Portugalsku Republiku:

Nacionalno sigurnosno tijelo.

Za Republiku Hrvatsku:

Ured Vijeća za nacionalnu sigurnost;

2 — Nacionalna sigurnosna tijela dostavljaju jedno drugom svoje službene kontakt podatke.

3 — Stranke diplomatskim putem obavješćuju jedna drugu o promjenama nacionalnih sigurnosnih tijela, što ne predstavlja izmjenu i dopunu ovog Ugovora.

4 — Nacionalna sigurnosna tijela obavješćuju jedno drugo, na zahtjev, o važećim nacionalnim zakonima i propisima kojima se uređuje zaštita klasificiranih podataka i razmjenjuju podatke o sigurnosnim standardima, postupcima i praksama za zaštitu klasificiranih podataka.

Članak 5.

Mjere zaštite i pristup klasificiranim podacima

1 — Stranke, u skladu sa svojim nacionalnim zakonima i propisima, provode sve odgovarajuće mjere za zaštitu klasificiranih podataka koji se razmjenjuju ili nastaju u skladu s ovim Ugovorom.

2 — Stranke osiguravaju isti stupanj zaštite za ranije navedene klasificirane podatke kao što je predviđen za nacionalne klasificirane podatke istoznačnog stupnja tajnosti, kako je određeno u članku 3. ovog Ugovora.

3 — Stranka pošiljateljica pisano obavješćuje stranku primateljicu o bilo kojoj promjeni stupnja tajnosti ustupljenih klasificiranih podataka, kako bi se primijenile odgovarajuće sigurnosne mjere.

4 — Pristup klasificiranim podacima imaju samo osobe kojima je, u skladu s nacionalnim zakonima i propisima, odobren pristup klasificiranim podacima istoznačnog stupnja tajnosti i kojima je to nužno za obavljanje poslova iz djelokruga.

5 — U okviru područja primjene ovog Ugovora, svaka stranka priznaje uvjerenje o sigurnosnoj provjeri osobe i uvjerenje o sigurnosnoj provjeri pravne osobe koje je izdala druga stranka.

6 — Nadležna sigurnosna tijela, na zahtjev i u skladu s nacionalnim zakonima i propisima, pomažu jedno drugom u provedbi sigurnosnih provjera nužnih za primjenu ovog Ugovora.

7 — U okviru područja primjene ovog Ugovora, nacionalna sigurnosna tijela bez odgode obavješćuju jedno drugo o bilo kojoj izmjeni u pogledu uvjerenja o sigurnosnoj provjeri osobe i uvjerenja o sigurnosnoj provjeri pravne osobe, posebice u vezi s povlačenjem ili promjenom stupnja tajnosti.

8 — Na zahtjev nacionalnog sigurnosnog tijela stranke pošiljateljice, nacionalno sigurnosno tijelo stranke primateljice izdaje pisanu potvrdu da fizička osoba ima pravo pristupa klasificiranim podacima.

9 — Stranka primateljica:

a) dostavlja klasificirane podatke trećoj strani samo na temelju prethodnog pisanog pristanka stranke pošiljateljice;

b) označava primljene klasificirane podatke u skladu s istoznačnim stupnjem tajnosti utvrđenim u članku 3.;

c) koristi klasificirane podatke samo za svrhe za koje su dostavljeni.

10 — Predstavnici nadležnih tijela mogu se međusobno posjećivati kako bi analizirali učinkovitost mjera usvojenih za zaštitu klasificiranih podataka.

Članak 6.

Prijenos klasificiranih podataka

1 — Klasificirani podaci prenose se između stranaka, u skladu s nacionalnim zakonima i propisima stranke pošiljateljice, najčešće diplomatskim putem, ili na drugi način koji dogovore nadležna tijela.

2 — Stranka primateljica pisano potvrđuje primitak klasificiranih podataka označenih kao CONFIDENCIAL/POVJERLJIVO/CONFIDENTIAL ili više.

Članak 7.

Umnožavanje i prevođenje klasificiranih podataka

1 — Podaci označeni kao SECRETO/TAJNO/SECRET ili više prevode se ili umnožavaju samo u iznimnim slučajevima, na temelju prethodnog pisanog pristanka stranke pošiljateljice.

2 — Svi umnoženi primjerci klasificiranih podataka označavaju se izvornom oznakom stupnja tajnosti i takvi umnoženi podaci stavljaju se pod isti nadzor kao izvorni podaci, dok je broj umnoženih primjeraka ograničen na broj potreban u službene svrhe.

3 — Prijevod se označava izvornom oznakom stupnja tajnosti i nosi odgovarajuću napomenu na jeziku prijevoda da prijevod sadrži klasificirane podatke stranke pošiljateljice.

Članak 8.

Uništavanje klasificiranih podataka

1 — Klasificirani podaci uništavaju se na način koji onemogućava njihovo djelomično ili potpuno obnavljanje.

2 — Podaci označeni kao MUITO SECRETO/VRLO TAJNO/TOP SECRET ne uništavaju se i vraćaju se stranci pošiljateljici nakon što ih se prestane smatrati potrebnima.

3 — Stranka pošiljateljica može, dodatnim označavanjem ili slanjem naknadne pisane obavijesti, zabraniti uništavanje klasificiranih podataka, a ako je uništavanje klasificiranih podataka zabranjeno, oni se vraćaju stranci pošiljateljici.

4 — U kriznoj situaciji, kada je nemoguće zaštititi ili vratiti klasificirane podatke koji su razmijenjeni ili nastali u skladu s ovim Ugovorom, klasificirani podaci se odmah uništavaju, a stranka primateljica što je prije moguće obavješćuje nacionalno sigurnosno tijelo stranke pošiljateljice o tom uništavanju.

Članak 9.

Klasificirani ugovori

1 — U slučaju klasificiranih ugovora koji se provode na državnom području jedne od stranaka, nadležno sigurnosno tijelo druge stranke dostavlja prethodnu pisanu potvrdu da predloženi ugovaratelj posjeduje uvjerenje o sigurnosnoj provjeri pravne osobe odgovarajućeg stupnja tajnosti.

2 — Ugovaratelj ili podugovaratelj, u skladu s nacionalnim zakonima i propisima, osigurava da su sve osobe koje imaju pristup klasificiranim podacima informirane o svojoj odgovornosti u smislu zaštite klasificiranih podataka.

3 — Svako nacionalno sigurnosno tijelo može zatražiti od drugoga obavljanje sigurnosne inspekcije u objektu koji se nalazi na državnom području njegove države kako bi se osiguralo kontinuirano poštivanje sigurnosnih standarda u skladu s važećim nacionalnim zakonima i propisima.

4 — Klasificirani ugovori sklopljeni između ugovaratelja stranaka u skladu s odredbama ovog Ugovora uključuju odgovarajuće projektno-sigurnosne upute kojima se određuju najmanje sljedeći aspekti:

a) popis klasificiranih podataka uključenih u klasificirani ugovor i njihov stupanj tajnosti;

b) postupak za komunikaciju o promjeni stupnja tajnosti podataka;

c) komunikacijski putovi i sredstva za elektromagnetski prijenos;

d) postupak za prijevoz klasificiranih podataka;

e) obveza obavješćivanja o bilo kojem stvarnom neovlaštenom otkrivanju, zlouporabi ili gubitku klasificiranih podataka, ili o sumnji u neovlašteno otkrivanje, zlouporabu ili gubitak klasificiranih podataka.

5 — Primjerak projektno-sigurnosnih uputa klasificiranog ugovora prosljeđuje se nadležnom tijelu stranke u kojoj se klasificirani ugovor treba provesti, kako bi se omogućilo odgovarajuće sigurnosno nadgledanje i nadzor.

Članak 10.

Posjeti

1 — Posjeti koji zahtijevaju pristup klasificiranim podacima podliježu prethodnom pisanom pristanku koji daju nadležna sigurnosna tijela u skladu s važećim nacionalnim zakonima i propisima, uz izuzetak posjeta koji zahtijevaju pristup klasificiranim podacima označenim kao RESERVADO/OGRANIČENO/RESTRICTED, koji se mogu dogovarati izravno između savjetnika za informacijsku sigurnost odnosnih tijela.

2 — Zahtjev za posjet podnosi se putem nadležnog sigurnosnog tijela stranke domaćina najmanje dvadeset (20) dana prije posjeta i uključuje:

a) ime i prezime posjetitelja, mjesto i datum rođenja, državljanstvo, broj putovnice ili osobne iskaznice;

b) naziv tijela koje posjetitelj predstavlja;

c) naziv i adresu tijela koje se posjećuje, uključujući ime i telefonski broj osobe za kontakt;

d) potvrdu o uvjerenju o sigurnosnoj provjeri osobe posjetitelja i njegovoj valjanosti;

e) svrhu posjeta, uključujući najviši stupanj klasificiranih podataka koji će biti uključeni;

f) očekivani datum i trajanje posjeta, a u slučaju ponovljenih posjeta, navodi se ukupno razdoblje pokriveno posjetima;

g) datum, potpis i otisak službenog pečata nadležnog sigurnosnog tijela.

3 — U žurnim slučajevima, zahtjev za posjet podnosi se najmanje sedam (7) dana unaprijed.

4 — Nacionalno sigurnosno tijelo stranke koja primi zahtjev za posjet o odluci pravodobno obavješćuje nacionalno sigurnosno tijelo stranke koja podnosi zahtjev.

5 — Posjet fizičkih osoba iz treće stranke koji zahtijeva pristup klasificiranim podacima stranke pošiljateljice odobrava se samo pisanim pristankom nacionalnog sigurnosnog tijela stranke pošiljateljice.

6 — Nacionalno sigurnosno tijelo stranke domaćina daje primjerak odobrenog zahtjeva za posjet savjetnicima za informacijsku sigurnost tijela koje se posjećuje.

7 — Valjanost odobrenja posjeta nije dulja od dvanaest (12) mjeseci.

8 — Nacionalna sigurnosna tijela mogu usuglasiti sastavljanje popisa osoba ovlaštenih za ponovljene posjete, koji je valjan tijekom početnog razdoblja od dvanaest (12) mjeseci i može se, temeljem dogovora, produljiti za daljnje razdoblje koje ne prelazi sljedećih dvanaest (12) mjeseci.

9 — Nakon što su nacionalna sigurnosna tijela odobrila popis za ponovljene posjete, uvjeti pojedinih posjeta izravno se dogovaraju sa savjetnicima za informacijsku sigurnost tijela koja se posjećuju.

10 — Bilo koji klasificirani podaci koje posjetitelj dobije smatraju se klasificiranim podacima ustupljenim na temelju ovog Ugovora.

Članak 11.

Povreda sigurnosti

1 — U slučaju stvarne povrede sigurnosti ili sumnje u povredu sigurnosti, nacionalno sigurnosno tijelo stranke u kojoj je do nje došlo bez odgode pisano obavješćuje nacionalno sigurnosno tijelo stranke pošiljateljice i pokreće odgovarajući postupak, u skladu s nacionalnim zakonima i propisima, kako bi se utvrdile okolnosti povrede sigurnosti, razmjer štete i mjere provedene za njezino ublažavanje.

2 — Zaključci ranije navedenih postupaka prosljeđuju se nacionalnom sigurnosnom tijelu stranke pošiljateljice.

3 — Ako do povrede sigurnosti dođe u trećoj državi, nacionalno sigurnosno tijelo stranke pošiljateljice bez odgode poduzima radnje iz stavaka 1. i 2. ovog članka.

4 — Druga stranka, ako je potrebno, surađuje u postupcima iz stavka 1. ovog članka.

Članak 12.

Troškovi

Svaka stranka snosi svoje vlastite troškove koji nastanu u provedbi ovog Ugovora i njegovom nadzoru.

Članak 13.

Rješavanje sporova

Bilo koji spor u vezi s tumačenjem ili primjenom ovog Ugovora rješavat će se pregovorima između stranaka diplomatskim putem.

Članak 14.

Izmjene i dopune

1 — Stranke mogu izmijeniti i dopuniti ovaj Ugovor na temelju uzajamnog pisanog pristanka.

2 — Izmjene i dopune stupaju na snagu u skladu s uvjetima naznačenim u članku 16. ovog Ugovora.

Članak 15.

Trajanje i prestanak

1 — Ovaj Ugovor ostaje na snazi na neodređeno vrijeme.

2 — Bilo koja stranka može, u svako doba, okončati ovaj Ugovor pisanom obaviješću drugoj stranci diplomatskim putem.

3 — Ovaj Ugovor prestaje šest (6) mjeseci nakon datuma primitka ranije spomenute obavijesti.

4 — Usprkos prestanku, svi klasificirani podaci ustupljeni u skladu s ovim Ugovorom nastavljaju se štititi u skladu s ovdje navedenim odredbama, sve dok stranka pošiljateljica ne oslobodi stranku primateljicu te obveze.

Članak 16.

Stupanje na snagu

Ovaj Ugovor stupa na snagu trideset (30) dana nakon datuma primitka posljednje pisane obavijesti, diplomatskim putem, kojom se priopćuje okončanje unutarnjih postupaka svake stranke potrebnih za tu svrhu.

Članak 17.

Registracija

Nakon stupanja na snagu ovog Ugovora, stranka na čijem je državnom području potpisan ovaj Ugovor dostavlja ga radi registracije Tajništvu Ujedinjenih naroda, u skladu s člankom 102. Povelje Ujedinjenih naroda, te obavješćuje drugu stranku o okončanju ovog postupka, navodeći odnosni broj registracije.

Sastavljeno u Zagrebu, dana 30. lipnja 2020. u dva izvornika, svaki na portugalskom, hrvatskom i engleskom jeziku, pri čemu su svi tekstovi jednako vjerodostojni. U slučaju razlika u tumačenju, mjerodavan je engleski tekst.

ZA PORTUGALSKU REPUBLIKU:

Jorge Silva Lopes, veleposlanik Portugala.

ZA REPUBLIKU HRVATSKU:

*Maja Čavlo*vić, predstojnica Ureda Vijeća za nacionalnu sigurnost.

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

The Portuguese Republic and the Republic of Croatia (hereinafter referred to as «the Parties»),

Realizing that the good cooperation may require exchange of Classified Information between the Parties,

Desiring to establish a set of rules regulating the mutual protection of Classified Information exchanged or generated in the course of the cooperation between the Parties,

Have agreed as follows:

Article 1

Purpose and Scope

This Agreement sets up the rules to ensure the protection of Classified Information that is commonly generated or exchanged between the Parties.

Article 2

Definitions

For the purposes of this Agreement:

(1) «Classified Information» means any information, irrespective of the form, which requires protection against security breach and has been classified in accordance with national laws and regulations of the originating Party;

(2) «Need-to-Know» means the need to have access to Classified Information in the scope of a given official position and for the performance of a specific task;

(3) «Breach of Security» means any form of unauthorized disclosure, misuse, alteration, damage or destruction of Classified Information, as well as any other action or inaction, resulting in loss of its confidentiality, integrity or availability;

(4) «Originating Party» means the Party that has created the Classified Information;

(5) «Receiving Party» means the Party to which Classified Information of the Originating Party is transmitted;

(6) «National Security Authority» means the national authority responsible for the implementation and supervision of this Agreement;

(7) «Competent Authority» means the National Security Authority or another national authority which, in accordance with national laws and regulations, implements this Agreement;

(8) «Contractor» means an individual or a legal entity possessing the legal capacity to conclude Classified Contracts;

(9) «Classified Contract» means an agreement between two or more Contractors, which contains or the execution of which requires access to Classified Information;

(10) «Personnel Security Clearance» means the determination by the National Security Authority confirming, in accordance with national laws and regulations, that the individual is eligible to have access to Classified Information;

(11) «Facility Security Clearance» means the determination by the National Security Authority confirming, in accordance with national laws and regulations, that the legal entity or individual has the physical and organizational capabilities to meet the conditions for access to and handling of Classified Information;

(12) «Third Party» means any state, organization or legal entity that is not a party to this Agreement.

Article 3

Security Classification Levels

The Parties agree that the following security classification levels are equivalent:

For the Portuguese Republic	For the Republic of Croatia	Equivalent in English
MUITO SECRETO	VRLO TAJNO	TOP SECRET
SECRETO	TAJNO	SECRET
CONFIDENCIAL	POVJERLJIVO	CONFIDENTIAL
RESERVADO	OGRANIČENO	RESTRICTED

Article 4

National Security Authorities

1 — The National Security Authorities of the Parties are:

For the Portuguese Republic:

National Security Authority.

For the Republic of Croatia:

Office of the National Security Council;

2 — The National Security Authorities shall provide each other with their official contact details.

3 — The Parties shall inform each other through the diplomatic channels of the changes of the National Security Authorities, which shall not constitute an amendment to this Agreement.

4 — On request, the National Security Authorities shall inform each other of national laws and regulations in force regulating the protection of Classified Information and shall exchange information about the security standards, procedures and practices for the protection of Classified Information.

Article 5

Protection Measures and Access to Classified Information

1 — In accordance with their national laws and regulations, the Parties shall take all appropriate measures for the protection of Classified Information which is exchanged or generated under this Agreement.

2 — The same level of protection shall be ensured by the Parties for aforementioned Classified Information as it is provided for the national Classified Information of the equivalent security classification level, as defined in Article 3 of this Agreement.

3 — The Originating Party shall inform the Receiving Party in writing about any change of the security classification level of the released Classified Information, in order to apply the appropriate security measures.

4 — Classified Information shall only be made accessible to persons who are authorized in accordance with national laws and regulations to have access to Classified Information of the equivalent security classification level and who have a Need-to-Know.

5 — Within the scope of this Agreement, each Party shall recognize the Personnel Security Clearance and Facility Security Clearance issued by the other Party.

6 — The National Security Authorities shall assist each other upon request and in accordance with national laws and regulations in carrying out vetting procedures necessary for the application of this Agreement.

7 — Within the scope of this Agreement, the National Security Authorities shall inform each other without delay about any alteration with regard to Personnel Security Clearance and Facility Security Clearance, in particular about the revocation or alteration of the security classification level.

8 — Upon the request of the National Security Authority of the Originating Party, the National Security Authority of the Receiving Party shall issue a written confirmation that an individual has the right to access Classified Information.

9 — The Receiving Party shall:

a) Submit Classified Information to a Third Party only upon prior written consent of the Originating Party;

b) Mark the received Classified Information in accordance with the security classification level equivalence set forth in Article 3;

c) Use Classified Information only for the purposes that it has been provided for.

10 — Representatives of the Competent Authorities may visit each other in order to analyze the efficiency of the measures adopted for the protection of Classified Information.

Article 6

Transmission of Classified Information

1 — Classified Information shall be transmitted between the Parties, in accordance with the national laws and regulations of the Originating Party, normally through the diplomatic channels, or as otherwise arranged between the Competent Authorities.

2 — Receiving Party shall confirm in writing the receipt of the Classified Information marked as CONFIDENCIAL/POVJERLJIVO/CONFIDENTIAL or above.

Article 7

Reproduction and Translation of Classified Information

1 — Information classified as SECRETO /TAJNO/SECRET or above shall be translated or reproduced only in exceptional cases upon prior written consent of the Originating Party.

2 — All copies of Classified Information shall be marked with the original security classification marking and such reproduced information shall be placed under the same control as the original information, the number of copies being restricted to that required for official purposes.

3 — The translation shall be marked with the original security classification marking and shall bear an appropriate note in the language into which it is translated that the translation contains Classified Information of the Originating Party.

Article 8

Destruction of Classified Information

1 — Classified Information shall be destroyed in a manner to eliminate the possibility of its partial or total reconstruction.

2 — Information classified as MUITO SECRETO/VRLO TAJNO /TOP SECRET shall not be destroyed and shall be returned to the Originating Party after it is no longer considered necessary.

3 — The Originating Party may, by additional marking or by a subsequent written notice, prohibit the destruction of Classified Information and if the destruction of Classified Information is prohibited, it shall be returned to the Originating Party.

4 — In a crisis situation in which it is impossible to protect or return Classified Information exchanged or generated under this Agreement, the Classified Information shall be destroyed immediately and the Receiving Party shall inform the National Security Authority of the Originating Party about this destruction as soon as possible.

Article 9

Classified Contracts

1 — In case of Classified Contracts implemented in the territory of one of the Parties, the National Security Authority of the other Party shall deliver prior written assurance that the proposed contractor holds a Facility Security Clearance of an appropriate security classification level.

2 — The contractor or subcontractor shall, according to the national laws and regulations, ensure that all persons with access to Classified Information are informed of their responsibility towards the protection of Classified Information.

3 — Each National Security Authority may request the other to carry out a security inspection in a facility located in their State's territory in order to ensure continuing compliance with security standards according to the respective national laws and regulations.

4 — Classified Contracts concluded between Contractors of the Parties under the provisions of this Agreement shall include an appropriate security section identifying, at least, the following aspects:

a) List of Classified Information involved in the Classified Contract and their security classification;

b) Procedure for the communication of alteration in the security classification of information;

c) Communication channels and means for electromagnetic transmission;

d) Procedure for the transportation of Classified Information;

e) Obligation to notify any actual or suspected unauthorized disclosure, misappropriation or loss of Classified Information.

5 — A copy of the security section of Classified Contracts shall be forwarded to the Competent Authority of the Party where the Classified Contracts are to be performed to allow adequate security supervision and control.

Article 10

Visits

1 — Visits entailing access to Classified Information are subject to prior written consent given by the National Security Authorities according to the respective national laws and regulations, with exception of visits entailing access to Classified Information marked as RESERVADO /OGRANIČENO /RESTRICTED, which may be arranged directly between security officers of the respective entities.

2 — The request for visit shall be submitted through the National Security Authority of the host Party at least twenty (20) days before the visit and shall include:

a) Visitor's first and last name, place and date of birth, citizenship, passport or identification card number;

b) Name of the entity the visitor represents;

c) Name and address of the entity to be visited including the name and phone number of the point of contact;

d) Confirmation of the visitor's Personnel Security Clearance and its validity;

e) Purpose of the visit including the highest level of the Classified Information to be involved;

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

g) Date, signature and stamping of the official seal of the National Security Authority.

3 — In urgent cases, the request for visit shall be submitted at least seven (7) days in advance.

4 — The National Security Authority of the Party that receives the request for visit shall inform, in due time, the National Security Authority of the requesting Party about the decision.

5 — Visit of individuals from a Third Party entailing access to Classified Information of the Originating Party shall only be authorized by a written consent of the National Security Authority of the Originating Party.

6 — The National Security Authority of the host Party shall provide a copy of the approved request for visit to the security officers of the entity to be visited.

7 — The validity of the visit authorization shall not exceed twelve (12) months.

8 — The National Security Authorities may agree to establish a list of authorized persons to make recurring visits, which is valid for an initial period of twelve (12) months and, upon agreement, may be extended for a further period of time not exceeding another twelve (12) months.

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

10 — Any Classified Information acquired by a visitor shall be considered as Classified Information released under this Agreement.

Article 11

Breach of Security

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

2 — The conclusions of the aforementioned proceedings shall be forwarded to the National Security Authority of the Originating Party.

3 — When the Breach of Security has occurred in a third state, the National Security Authority of the Originating Party shall take the actions referred to in paragraphs 1 and 2 of this Article without delay.

4 — The other Party shall, if required, cooperate in the proceedings referred to in paragraph 1 of this Article.

Article 12

Expenses

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

Article 13

Settlement of Disputes

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

Article 14

Amendments

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

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

Article 15

Duration and Termination

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

2 — Either Party may, at any time, terminate this Agreement, by means of a notification in writing to the other Party through the diplomatic channels.

3 — The Agreement shall terminate six (6) months following the date of the receipt of the aforementioned notification.

4 — Notwithstanding termination, all Classified Information released under this Agreement shall continue to be protected according to the provisions set forth herein, until the Originating Party dispenses the Receiving Party from this obligation.

Article 16

Entry into Force

This Agreement shall enter into force thirty (30) days following the date of the receipt of the last written notification, through the diplomatic channels, conveying the completion of the internal procedures of each Party required for that purpose.

Article 17

Registration

After the entry into force of this Agreement, the Party in whose territory this Agreement was signed shall transmit it for registration to the Secretariat of the United Nations, according to Article

102 of the Charter of the United Nations, and shall notify the other Party of the conclusion of this proceeding, indicating the respective number of registration.

Done at Zagreb on 30 June 2020 in two originals, each in the Portuguese, Croatian, and English languages, all texts being equally authentic. In case of any divergence of interpretation, the English text shall prevail.

For the Portuguese Republic:

Jorge Silva Lopes, Ambassador of Portugal.

For the Republic of Croatia

Maja Čavlović, Director of the Office of the National Security Council.

113630001