# P.Z. br. 120

**HRVATSKI SABOR**

KLASA: 022-03/21-01/20
URBROJ: 65-21-02

Zagreb, 25. veljače 2021.

Hs**NP*022-03/21-01/20*65-21-02**Hs

**ZASTUPNICAMA I ZASTUPNICIMA**
**HRVATSKOGA SABORA**

**PREDSJEDNICAMA I PREDSJEDNICIMA**
**RADNIH TIJELA**

Na temelju članaka 178. i 192., a u svezi članka 207.a Poslovnika Hrvatskoga sabora u prilogu upućujem ***Konačni prijedlog zakona o potvrđivanju Ugovora između Vlade Republike Hrvatske i Vlade Kraljevine Španjolske o uzajamnoj zaštiti klasificiranih podataka,*** koji je predsjedniku Hrvatskoga sabora podnijela Vlada Republike Hrvatske, aktom od 25. veljače 2021. godine.

Za svoje predstavnike, koji će u njezino ime sudjelovati u radu Hrvatskoga sabora i njegovih radnih tijela, Vlada je odredila ministra pravosuđa i uprave dr. sc. Ivana Malenicu, državne tajnike mr. sc. Josipa Salapića, Juru Martinovića i Sanjina Rukavinu te predstojnicu Ureda Vijeća za nacionalnu sigurnost Maju Čavlović.

**PREDSJEDNIK**

**Gordan Jandroković**

**VLADA REPUBLIKE HRVATSKE**

KLASA: 022-03/20-11/44
URBROJ: 50301-29/23-21-4

Zagreb, 25. veljače 2021.

**PREDSJEDNIKU HRVATSKOGA SABORA**

PREDMET: Konačni prijedlog zakona o potvrđivanju Ugovora između Vlade Republike Hrvatske i Vlade Kraljevine Španjolske o uzajamnoj zaštiti klasificiranih podataka

Na temelju članka 85. Ustava Republike Hrvatske („Narodne novine“, br. 85/10. – pročišćeni tekst i 5/14. – Odluka Ustavnog suda Republike Hrvatske) i članka 207.a Poslovnika Hrvatskoga sabora („Narodne novine“, br. 81/13., 113/16., 69/17., 29/18., 53/20., 119/20. – Odluka Ustavnog suda Republike Hrvatske i 123/20.), Vlada Republike Hrvatske podnosi Konačni prijedlog zakona o potvrđivanju Ugovora između Vlade Republike Hrvatske i Vlade Kraljevine Španjolske o uzajamnoj zaštiti klasificiranih podataka.

Za svoje predstavnike, koji će u njezino ime sudjelovati u radu Hrvatskoga sabora i njegovih radnih tijela, Vlada je odredila ministra pravosuđa i uprave dr. sc. Ivana Malenicu, državne tajnike mr. sc. Josipa Salapića, Juru Martinovića i Sanjina Rukavinu te predstojnicu Ureda Vijeća za nacionalnu sigurnost Maju Čavlović.

PREDSJEDNIK

mr. sc. Andrej Plenković

**VLADA REPUBLIKE HRVATSKE**

# KONAČNI PRIJEDLOG ZAKONA O POTVRĐIVANJU UGOVORA IZMEĐU VLADE REPUBLIKE HRVATSKE I VLADE KRALJEVINE ŠPANJOLSKE O UZAJAMNOJ ZAŠTITI KLASIFICIRANIH PODATAKA

**Zagreb, veljača 2021.**

**KONAČNI PRIJEDLOG ZAKONA O POTVRĐIVANJU UGOVORA IZMEĐU VLADE REPUBLIKE HRVATSKE I VLADE KRALJEVINE ŠPANJOLSKE O UZAJAMNOJ ZAŠTITI KLASIFICIRANIH PODATAKA**

## I. USTAVNA OSNOVA ZA DONOŠENJE ZAKONA

Ustavna osnova za donošenje Zakona o potvrđivanju Ugovora između Vlade Republike Hrvatske i Vlade Kraljevine Španjolske o uzajamnoj zaštiti klasificiranih podataka sadržana je u odredbi članka 140. stavka 1. Ustava Republike Hrvatske („Narodne novine“, br. 85/10. – pročišćeni tekst i 5/14. – Odluka Ustavnog suda Republike Hrvatske).

## II. OCJENA STANJA I CILJ KOJI SE DONOŠENJEM ZAKONA ŽELI POSTIĆI

Potreba za međunarodnom razmjenom podataka ili materijala, koji su prema nacionalnom zakonodavstvu klasificirani ili označeni jednim od zakonom utvrđenih stupnjeva tajnosti, načelno je izraz s jedne strane bliskih vanjskopolitičkih odnosa između država, a s druge strane povećane potrebe za njihovim uzajamnim i usklađenim djelovanjem na rješavanju suvremenih, osobito sigurnosnih problema koji često svojim razmjerima i kompleksnošću nadilaze nacionalne okvire.

Također je međunarodna razmjena i zaštita klasificiranih podataka na navedeni način obuhvaćena i pojedinim zakonima koji uređuju neka područja rada državne uprave (npr. Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske i sl.).

Zakonima kojima se uređuje područje informacijske sigurnosti osigurana je primjena potrebnih mjera i standarda u razmjeni klasificiranih podataka između Republike Hrvatske i drugih zemalja i organizacija kao i u postupcima sklapanja međunarodnih ugovora kojima se razmjenjuju i štite klasificirani podaci između Republike Hrvatske i drugih zemalja i organizacija. Podzakonskim aktima donesenim na temelju zakona koji su uredili područje informacijske sigurnosti, uspostavljeni su strukovni standardi za odgovarajuće, cjelovito uređenje zaštite klasificiranih podataka, kako na unutarnjem tako i na međunarodnom planu.

Suradnja između Republike Hrvatske i Kraljevine Španjolske u području razmjene klasificiranih podataka temelji se na zajedničkim interesima i razvoju odnosa dviju država u području informacijske sigurnosti kao i u ostalim područjima međudržavne suradnje. Slijedom toga, a s obzirom da su tijekom 2007. godine doneseni zakoni kojima je uređeno područje zaštite klasificiranih podataka u Republici Hrvatskoj, ocijenjeno je da postoji potreba za uređivanjem suradnje između Republike Hrvatske i Kraljevine Španjolske u području zaštite klasificiranih podataka.

Sukladno rješenjima i standardima utvrđenim u spomenutim propisima, potpisan je 15. prosinca 2020. u Zagrebu, Ugovor između Vlade Republike Hrvatske i Vlade Kraljevine Španjolske o uzajamnoj zaštiti klasificiranih podataka, kojim se u odnosima Republike Hrvatske i Kraljevine Španjolske stvara pravni okvir te uspostavljaju pravila uzajamne zaštite klasificiranih podataka, koja će se odnositi na sve buduće ugovore o suradnji i klasificirane ugovore koje ugovorne stranke sklapaju, a koji sadrže ili uključuju klasificirane podatke.

## III. OSNOVNA PITANJA KOJA SE PREDLAŽU UREDITI ZAKONOM

Ovim Zakonom potvrđuje se Ugovor između Vlade Republike Hrvatske i Vlade Kraljevine Španjolske o uzajamnoj zaštiti klasificiranih podataka, kako bi njegove odredbe u smislu članka 141. Ustava Republike Hrvatske postale dio unutarnjeg pravnog poretka Republike Hrvatske.

Ugovorom se uspostavlja pravni okvir za osiguranje zaštite klasificiranih podataka koji zajednički nastaju ili se razmjenjuju između ugovornih stranaka, određuju se nadležna tijela za provedbu Ugovora, utvrđuju se istoznačni stupnjevi tajnosti, postupanje s klasificiranim podacima, obveze u pogledu nacionalnih mjera za zaštitu klasificiranih podataka, mehanizmi prijenosa klasificiranih podataka, sadržane su posebne odredbe o klasificiranim ugovorima, uređuje se način ostvarivanja posjeta i sastanaka stručnjaka, postupanje u slučaju povreda sigurnosti kao i pitanje troškova nastalih u provedbi Ugovora.

## IV. OCJENA SREDSTAVA POTREBNIH ZA PROVEDBU ZAKONA

Za provedbu ovoga Zakona nije potrebno osigurati dodatna financijska sredstva u državnom proračunu Republike Hrvatske.

## V. ZAKONI KOJIMA SE POTVRĐUJU MEĐUNARODNI UGOVORI

Temelj za donošenje ovoga Zakona nalazi se u članku 207.a Poslovnika Hrvatskoga sabora („Narodne novine“, br. 81/13., 113/16., 69/17., 29/18., 53/20., 119/20. – Odluka Ustavnog suda Republike Hrvatske i 123/20.), prema kojem se zakoni kojima se, u skladu s Ustavom Republike Hrvatske, potvrđuju međunarodni ugovori donose u pravilu u jednom čitanju, a postupak donošenja pokreće se podnošenjem konačnog prijedloga zakona o potvrđivanju međunarodnog ugovora.

Naime, s obzirom na razloge navedene u točkama II. i III. ovoga Prijedloga, kao i činjenicu da je Ugovor između Vlade Republike Hrvatske i Vlade Kraljevine Španjolske o uzajamnoj zaštiti klasificiranih podataka značajan mehanizam za ostvarivanje zaštite u području informacijske sigurnosti te zaštite klasificiranih podataka koji se razmjenjuju između Republike Hrvatske i Kraljevnine Španjolske, ocjenjuje se da postoji interes da Republika Hrvatska što skorije okonča svoj unutarnji pravni postupak, kako bi se stvorile pretpostavke da Ugovor, u skladu sa svojim odredbama, u odnosima dviju država stupi na snagu.

S obzirom na prirodu postupka potvrđivanja međunarodnih ugovora, kojim država i formalno izražava spremnost biti vezana već sklopljenim međunarodnim ugovorom, kao i na činjenicu da se u ovoj fazi postupka, u pravilu ne može mijenjati ili dopunjavati tekst međunarodnog ugovora, predlaže se ovaj Konačni prijedlog zakona raspraviti i prihvatiti u jednom čitanju.

**KONAČNI PRIJEDLOG ZAKONA O POTVRĐIVANJU UGOVORA IZMEĐU VLADE REPUBLIKE HRVATSKE I VLADE KRALJEVINE ŠPANJOLSKE O UZAJAMNOJ ZAŠTITI KLASIFICIRANIH PODATAKA**

**Članak 1.**

Potvrđuje se Ugovor između Vlade Republike Hrvatske i Vlade Kraljevine Španjolske o uzajamnoj zaštiti klasificiranih podataka, potpisan u Zagrebu 15. prosinca 2020., u izvorniku na hrvatskom, španjolskom i engleskom jeziku.

**Članak 2.**

Tekst Ugovora iz članka 1. ovoga Zakona, u izvorniku na hrvatskom, glasi:

**UGOVOR**

**IZMEĐU**

**VLADE REPUBLIKE HRVATSKE**

**I**

**VLADE KRALJEVINE ŠPANJOLSKE**

**O UZAJAMNOJ ZAŠTITI KLASIFICIRANIH PODATAKA**

Vlada Republike Hrvatske i Vlada Kraljevine Španjolske (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 u tijeku suradnje između stranaka,

sporazumjele su se kako slijedi:

**Članak 1.**
**Predmet**

Predmet ovog Ugovora je 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 da se pristup klasificiranim podacima može odobriti samo osobama za koje je potvrđeno da imaju potrebu znati ili posjedovati takve podatke za obavljanje svojih službenih i stručnih zadaća;

(3) „**povreda sigurnosti**" označava bilo koji oblik neovlaštenog otkrivanja, zlouporabe, neovlaštene izmjene, oštećivanja ili uništavanja klasificiranih podataka, kao i bilo koje drugo činjenje ili nečinjenje, koji dovode do gubitka njihove povjerljivosti, cjelovitosti ili dostupnosti;

(4) „**stupanj tajnosti**" označava kategoriju koja, u skladu s nacionalnim zakonima i propisima, predstavlja stupanj ograničenja pristupa klasificiranim podacima i minimalni stupanj njihove zaštite koji osiguravaju stranke;

(5) „**stranka pošiljateljica**" označava stranku koja je stvorila klasificirane podatke;

(6) „**stranka primateljica**" označava stranku kojoj se prenose klasificirani podaci stranke pošiljateljice;

(7) „**nacionalno sigurnosno tijelo**" označava nacionalno tijelo odgovorno za provedbu i nadzor ovog Ugovora;

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

(9) „**ugovaratel**j" označava fizičku ili pravnu osobu koja ima pravnu sposobnost sklapanja ugovora;

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

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

(12) „**uvjerenje o sigurnosnoj provjeri pravne osobe**" označava potvrdu nadležnog 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;

(13) „**treća strana**" označava bilo koju državu, organizaciju, pravnu ili fizičku osobu koja nije stranka ovog Ugovora.

**Članak 3.**
**Stupnjevi tajnosti**

Stranke su suglasne da su sljedeći stupnjevi tajnosti istoznačni:

| Za Republiku Hrvatsku | Za Kraljevinu Španjolsku |
|---|---|
| VRLO TAJNO | SECRETO |
| TAJNO | RESERVADO |
| POVJERLJIVO | CONFIDENCIAL |
| OGRANIČENO | DIFUSIÓN LIMITADA |

**Članak 4.**
**Nacionalna sigurnosna tijela**

1. Nacionalna sigurnosna tijela stranaka su:

   Za Republiku Hrvatsku:
   - Ured Vijeća za nacionalnu sigurnost;

   Za Kraljevinu Španjolsku:
   - Nacionalni ured za sigurnost, Nacionalni obavještajni centar.

2. Stranke obavješćuju jedna drugu, diplomatskim putem, o bilo kojim promjenama svojih odnosnih nacionalnih sigurnosnih tijela.

3. Na zahtjev, nacionalna sigurnosna tijela obavješćuju jedno drugo 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. U skladu sa svojim nacionalnim zakonima i propisima, stranke poduzimaju sve odgovarajuće mjere za zaštitu klasificiranih podataka koji se razmjenjuju ili nastaju u skladu s ovim Ugovorom. Za takve klasificirane podatke osigurava se isti stupanj zaštite kakav je predviđen za nacionalne klasificirane podatke istoznačnog stupnja tajnosti, kako je određeno u članku 3. ovog Ugovora.

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

3. 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.

4. U okviru područja primjene ovog Ugovora, svaka stranka priznaje uvjerenja o sigurnosnoj provjeri osobe i uvjerenja o sigurnosnoj provjeri pravne osobe koja je izdala druga stranka.

5. Nadležna tijela, na zahtjev i u skladu s nacionalnim zakonima i propisima, pomažu jedno drugom u provođenju postupaka provjere nužnih za primjenu ovog Ugovora.

6. U okviru područja primjene ovog Ugovora, nacionalna sigurnosna tijela bez odgode obavješćuju jedno drugo o bilo kojoj izmjeni u vezi s uvjerenjima o sigurnosnoj provjeri osobe i uvjerenjima o sigurnosnoj provjeri pravne osobe, posebice o povlačenju ili promjeni stupnja tajnosti.

7. Na zahtjev nacionalnog sigurnosnog tijela stranke pošiljateljice, nacionalno sigurnosno tijelo stranke primateljice izdaje pisanu potvrdu da fizička osoba ima pravo pristupa klasificiranim podacima ili da je pravnoj osobi izdano uvjerenje o sigurnosnoj provjeri pravne osobe.

8. 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. ovog Ugovora;

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

9. Ako bilo koji drugi ugovor sklopljen između stranaka sadrži strože odredbe u vezi s razmjenom ili zaštitom klasificiranih podataka, primjenjuju se te odredbe.

**Članak 6.**
**Prijenos klasificiranih podataka**

Klasificirani podaci prenose se na način koji uzajamno odobre nacionalna sigurnosna tijela. Stranka primateljica pisano potvrđuje primitak klasificiranih podataka.

**Članak 7.**
**Umnožavanje i prevođenje klasificiranih podataka**

1. Podaci označeni kao TAJNO / RESERVADO 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. Takvi umnoženi podaci štite se na isti način kao izvorni podaci. Broj umnoženih primjeraka ograničen je na broj potreban za službene svrhe.

3. Prijevod se označava izvornom oznakom stupnja tajnosti i nosi dodatnu 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 VRLO TAJNO / SECRETO se ne uništavaju. Oni se vraćaju stranci pošiljateljici.

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

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

**Članak 9.**
**Klasificirani ugovori**

1. Klasificirani ugovori sklapaju se i provode u skladu s nacionalnim zakonima i propisima svake stranke.

2. Na zahtjev, nacionalno sigurnosno tijelo stranke primateljice potvrđuje da je predloženom ugovaratelju izdano odgovarajuće uvjerenje o sigurnosnoj provjeri osobe ili uvjerenje o sigurnosnoj provjeri pravne osobe. Ako predloženi ugovaratelj nema odgovarajuće uvjerenje o sigurnosnoj provjeri, nacionalno sigurnosno tijelo stranke pošiljateljice može zatražiti od nacionalnog sigurnosnog tijela stranke primateljice da izda odgovarajuće uvjerenje o sigurnosnoj provjeri.

3. Sigurnosni prilog sastavni je dio svakog klasificiranog ugovora ili podugovora, kojim stranka pošiljateljica pobliže određuje koji se klasificirani podaci ustupaju stranci primateljici, koji je stupanj tajnosti dodijeljen tim podacima i koje su obveze ugovaratelja u vezi zaštite klasificiranih podataka.

4. Obveze ugovaratelja u vezi zaštite klasificiranih podataka odnose se najmanje na sljedeće:
   a) ustupanje klasificiranih podataka isključivo fizičkim osobama koje su, u skladu s nacionalnim zakonima i propisima, ovlaštene za pristup klasificiranim podacima istoznačnog stupnja tajnosti i kojima je to nužno za obavljanje poslova iz djelokruga;
   b) prijenos klasificiranih podataka na način koji je u skladu s ovim Ugovorom;
   c) postupke za obavješćivanje o bilo kojim promjenama koje mogu nastati u vezi s klasificiranim podacima;
   d) korištenje klasificiranih podataka iz klasificiranog ugovora samo za svrhe vezane uz predmet ugovora;
   e) strogo poštivanje odredaba ovog Ugovora u vezi s postupcima za postupanje s klasificiranim podacima;
   f) obvezu obavješćivanja nacionalnog sigurnosnog tijela ugovaratelja o bilo kojoj povredi sigurnosti u vezi s klasificiranim ugovorom;
   g) ustupanje klasificiranih podataka vezanih uz klasificirani ugovor bilo kojoj trećoj strani samo na temelju prethodnog pisanog pristanka stranke pošiljateljice.

**Članak 10.**
**Posjeti**

1. Posjeti vezani uz provedbu ili pripremu klasificiranog ugovora koji zahtijevaju pristup klasificiranim podacima podliježu prethodnom odobrenju nacionalnog sigurnosnog tijela stranke domaćina. Odobrenje se izdaje na temelju zahtjeva za posjet nacionalnog sigurnosnog tijela stranke posjetitelja.

2. Zahtjev iz stavka 1. ovog članka sadrži:
   a) ime i prezime posjetitelja, datum i mjesto rođenja, državljanstvo;
   b) broj putovnice ili broj druge identifikacijske isprave posjetitelja;
   c) radno mjesto posjetitelja i naziv organizacije koju predstavlja;

d) stupanj uvjerenja o sigurnosnoj provjeri posjetitelja;

e) svrhu, predloženi radni program i planirani datum posjeta;

f) nazive organizacija i objekata za koje se traži posjet;

g) broj posjeta i traženo razdoblje;

h) druge podatke, koje dogovore nacionalna sigurnosna tijela.

3. Svaka stranka jamči zaštitu osobnih podataka posjetitelja u skladu sa svojim nacionalnim zakonima i propisima.

**Članak 11.**
**Povreda sigurnosti**

1. U slučaju stvarne povrede sigurnosti ili sumnje u povredu sigurnosti, nacionalno sigurnosno tijelo stranke kod koje se ona dogodila bez odgode obavješćuje nacionalno sigurnosno tijelo stranke pošiljateljice te, u skladu s nacionalnim zakonima i propisima, pokreće odgovarajući postupak kako bi se utvrdile okolnosti povrede sigurnosti. Rezultati postupka prosljeđuju se nacionalnom sigurnosnom tijelu stranke pošiljateljice.

2. Kada do povrede sigurnosti dođe u trećoj državi, nacionalno sigurnosno tijelo stranke pošiljatelja bez odgode poduzima radnje iz stavka 1. ovog članka.

**Članak 12.**
**Troškovi**

1. Ne očekuje se da će provedba ovog Ugovora prouzročiti bilo kakve troškove.

2. U slučaju bilo kakvih troškova, svaka stranka snosi svoje vlastite troškove koji nastanu uslijed provedbe i nadzora nad svim aspektima ovog Ugovora u skladu sa svojim nacionalnim zakonodavstvom.

**Članak 13.**
**Rješavanje sporova**

Bilo koji spor u vezi s tumačenjem ili primjenom ovog Ugovora rješavat će se konzultacijama i pregovorima između stranaka i neće se podnositi na rješavanje bilo kojem međunarodnom sudu ili trećoj strani.

**Članak 14.**
**Završne odredbe**

1. Ovaj Ugovor stupa na snagu datumom primitka posljednje pisane obavijesti kojom stranke obavješćuju jedna drugu, diplomatskim putem, da su ispunjeni njihovi unutarnji pravni uvjeti potrebni za njegovo stupanje na snagu.

2. Ovaj Ugovor može se izmijeniti i dopuniti uzajamnim pisanim pristankom stranaka. Izmjene i dopune stupaju na snagu u skladu s odredbom stavka 1. ovog članka.

3. Ovaj Ugovor sklapa se na neodređeno vrijeme. Svaka stranka može otkazati ovaj Ugovor pisanom obaviješću drugoj stranci diplomatskim putem. U tom slučaju, ovaj Ugovor prestaje šest mjeseci od datuma na koji je druga stranka primila obavijest o otkazu.

4. U slučaju prestanka ovog Ugovora, svi klasificirani podaci razmijenjeni u skladu s ovim Ugovorom nastavljaju se štititi u skladu s ovdje utvrđenim odredbama te se, na zahtjev, vraćaju stranci pošiljateljici.

Sastavljeno u Zagrebu dana 15. prosinca 2020. u dva izvornika, svaki na hrvatskom, španjolskom i engleskom jeziku, pri čemu su svi tekstovi jednako vjerodostojni. U slučaju razlika u tumačenju, mjerodavan je engleski tekst.

| ZA VLADU<br>REPUBLIKE HRVATSKE | ZA VLADU<br>KRALJEVINE ŠPANJOLSKE |
|---|---|
| **Maja Čavlović, v. r.**<br>predstojnica Ureda<br>Vijeća za nacionalnu sigurnost | **Alonso Dezcallar de Mazarredo, v. r.**<br>izvanredni i opunomoćeni veleposlanik<br>Kraljevine Španjolske u Republici Hrvatskoj |

**Članak 3.**

Provedba ovoga Zakona u djelokrugu je tijela državne uprave nadležnog za poslove informacijske sigurnosti.

**Članak 4.**

Na dan stupanja na snagu ovoga Zakona, Ugovor iz članka 1. ovoga Zakona nije na snazi te će se podaci o njegovom stupanju na snagu objaviti sukladno odredbi članka 30. stavka 3. Zakona o sklapanju i izvršavanju međunarodnih ugovora („Narodne novine“, broj 28/96.).

**Članak 5.**

Ovaj Zakon stupa na snagu osmoga dana od dana objave u „Narodnim novinama“.

# O B R A Z L O Ž E N J E

**Člankom 1.** Konačnog prijedloga zakona utvrđuje se da Hrvatski sabor potvrđuje Ugovor između Vlade Republike Hrvatske i Vlade Kraljevine Španjolske o uzajamnoj zaštiti klasificiranih podataka, sukladno odredbama članka 140. stavka 1. Ustava Republike Hrvatske („Narodne novine“, br. 85/10. – pročišćeni tekst i 5/14. – Odluka Ustavnog suda Republike Hrvatske), čime se iskazuje formalni pristanak Republike Hrvatske da bude vezana ovim Ugovorom, na temelju čega će ovaj pristanak biti iskazan i u odnosima s drugom ugovornom strankom.

**Članak 2.** sadrži tekst Ugovora u izvorniku na hrvatskom jeziku.

**Člankom 3.** Konačnog prijedloga zakona utvrđuje se da je provedba Zakona u djelokrugu tijela državne uprave nadležnog za poslove informacijske sigurnosti.

**Člankom 4.** utvrđuje se da na dan stupanja na snagu Zakona, Ugovor između Vlade Republike Hrvatske i Vlade Kraljevine Španjolske o uzajamnoj zaštiti klasificiranih podataka nije na snazi te da će se podaci o njegovom stupanju na snagu objaviti sukladno odredbi članka 30. stavka 3. Zakona o sklapanju i izvršavanju međunarodnih ugovora („Narodne novine“, broj 28/96.).

**Člankom 5.** uređuje se stupanje na snagu ovoga Zakona.

**PRILOG: - Preslika teksta Ugovora u izvorniku na hrvatskom, španjolskom i engleskom jeziku**

**UGOVOR**

**IZMEĐU**

**VLADE REPUBLIKE HRVATSKE**

**I**

**VLADE KRALJEVINE ŠPANJOLSKE**

**O UZAJAMNOJ ZAŠTITI KLASIFICIRANIH PODATAKA**

Vlada Republike Hrvatske i Vlada Kraljevine Španjolske (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 u tijeku suradnje između stranaka,

sporazumjele su se kako slijedi:

**Članak 1.**
**Predmet**

Predmet ovog Ugovora je 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 da se pristup klasificiranim podacima može odobriti samo osobama za koje je potvrđeno da imaju potrebu znati ili posjedovati takve podatke za obavljanje svojih službenih i stručnih zadaća;

(3) „**povreda sigurnosti**" označava bilo koji oblik neovlaštenog otkrivanja, zlouporabe, neovlaštene izmjene, oštećivanja ili uništavanja klasificiranih podataka, kao i bilo koje drugo činjenje ili nečinjenje, koji dovode do gubitka njihove povjerljivosti, cjelovitosti ili dostupnosti;

(4) „**stupanj tajnosti**" označava kategoriju koja, u skladu s nacionalnim zakonima i propisima, predstavlja stupanj ograničenja pristupa klasificiranim podacima i minimalni stupanj njihove zaštite koji osiguravaju stranke;

(5) „**stranka pošiljateljica**" označava stranku koja je stvorila klasificirane podatke;

(6) „**stranka primateljica**" označava stranku kojoj se prenose klasificirani podaci stranke pošiljateljice;

(7) „**nacionalno sigurnosno tijelo**" označava nacionalno tijelo odgovorno za provedbu i nadzor ovog Ugovora;

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

(9) „**ugovaratelj**" označava fizičku ili pravnu osobu koja ima pravnu sposobnost sklapanja ugovora;

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

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

(12) „**uvjerenje o sigurnosnoj provjeri pravne osobe**" označava potvrdu nadležnog 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;

(13) „**treća strana**" označava bilo koju državu, organizaciju, pravnu ili fizičku osobu koja nije stranka ovog Ugovora.

**Članak 3.**
**Stupnjevi tajnosti**

Stranke su suglasne da su sljedeći stupnjevi tajnosti istoznačni:

| Za Republiku Hrvatsku | Za Kraljevinu Španjolsku |
|---|---|
| VRLO TAJNO | SECRETO |
| TAJNO | RESERVADO |
| POVJERLJIVO | CONFIDENCIAL |
| OGRANIČENO | DIFUSIÓN LIMITADA |

**Članak 4.**
**Nacionalna sigurnosna tijela**

1. Nacionalna sigurnosna tijela stranaka su:

   Za Republiku Hrvatsku:
   - Ured Vijeća za nacionalnu sigurnost;

   Za Kraljevinu Španjolsku:
   - Nacionalni ured za sigurnost, Nacionalni obavještajni centar.

2. Stranke obavješćuju jedna drugu, diplomatskim putem, o bilo kojim promjenama svojih odnosnih nacionalnih sigurnosnih tijela.

3. Na zahtjev, nacionalna sigurnosna tijela obavješćuju jedno drugo 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. U skladu sa svojim nacionalnim zakonima i propisima, stranke poduzimaju sve odgovarajuće mjere za zaštitu klasificiranih podataka koji se razmjenjuju ili nastaju u skladu s ovim Ugovorom. Za takve klasificirane podatke osigurava se isti stupanj zaštite kakav je predviđen za nacionalne klasificirane podatke istoznačnog stupnja tajnosti, kako je određeno u članku 3. ovog Ugovora.

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

3. 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.

4. U okviru područja primjene ovog Ugovora, svaka stranka priznaje uvjerenja o sigurnosnoj provjeri osobe i uvjerenja o sigurnosnoj provjeri pravne osobe koja je izdala druga stranka.

5. Nadležna tijela, na zahtjev i u skladu s nacionalnim zakonima i propisima, pomažu jedno drugom u provođenju postupaka provjere nužnih za primjenu ovog Ugovora.

6. U okviru područja primjene ovog Ugovora, nacionalna sigurnosna tijela bez odgode obavješćuju jedno drugo o bilo kojoj izmjeni u vezi s uvjerenjima o sigurnosnoj provjeri osobe i uvjerenjima o sigurnosnoj provjeri pravne osobe, posebice o povlačenju ili promjeni stupnja tajnosti.

7. Na zahtjev nacionalnog sigurnosnog tijela stranke pošiljateljice, nacionalno sigurnosno tijelo stranke primateljice izdaje pisanu potvrdu da fizička osoba ima pravo pristupa klasificiranim podacima ili da je pravnoj osobi izdano uvjerenje o sigurnosnoj provjeri pravne osobe.

8. 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. ovog Ugovora;
   c) koristi klasificirane podatke samo za svrhe za koje su dostavljeni.

9. Ako bilo koji drugi ugovor sklopljen između stranaka sadrži strože odredbe u vezi s razmjenom ili zaštitom klasificiranih podataka, primjenjuju se te odredbe.

**Članak 6.**
**Prijenos klasificiranih podataka**

Klasificirani podaci prenose se na način koji uzajamno odobre nacionalna sigurnosna tijela. Stranka primateljica pisano potvrđuje primitak klasificiranih podataka.

## Članak 7.
## Umnožavanje i prevođenje klasificiranih podataka

1. Podaci označeni kao TAJNO / RESERVADO 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. Takvi umnoženi podaci štite se na isti način kao izvorni podaci. Broj umnoženih primjeraka ograničen je na broj potreban za službene svrhe.

3. Prijevod se označava izvornom oznakom stupnja tajnosti i nosi dodatnu 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 VRLO TAJNO / SECRETO se ne uništavaju. Oni se vraćaju stranci pošiljateljici.

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

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

## Članak 9.
## Klasificirani ugovori

1. Klasificirani ugovori sklapaju se i provode u skladu s nacionalnim zakonima i propisima svake stranke.

2. Na zahtjev, nacionalno sigurnosno tijelo stranke primateljice potvrđuje da je predloženom ugovaratelju izdano odgovarajuće uvjerenje o sigurnosnoj provjeri osobe ili uvjerenje o sigurnosnoj provjeri pravne osobe. Ako predloženi ugovaratelj nema odgovarajuće uvjerenje o sigurnosnoj provjeri, nacionalno sigurnosno tijelo stranke pošiljateljice može zatražiti od nacionalnog sigurnosnog tijela stranke primateljice da izda odgovarajuće uvjerenje o sigurnosnoj provjeri.

3. Sigurnosni prilog sastavni je dio svakog klasificiranog ugovora ili podugovora, kojim stranka pošiljateljica pobliže određuje koji se klasificirani podaci ustupaju stranci primateljici, koji je stupanj tajnosti dodijeljen tim podacima i koje su obveze ugovaratelja u vezi zaštite klasificiranih podataka.

4. Obveze ugovaratelja u vezi zaštite klasificiranih podataka odnose se najmanje na sljedeće:

   a) ustupanje klasificiranih podataka isključivo fizičkim osobama koje su, u skladu s nacionalnim zakonima i propisima, ovlaštene za pristup klasificiranim podacima istoznačnog stupnja tajnosti i kojima je to nužno za obavljanje poslova iz djelokruga;

b) prijenos klasificiranih podataka na način koji je u skladu s ovim Ugovorom;

c) postupke za obavješćivanje o bilo kojim promjenama koje mogu nastati u vezi s klasificiranim podacima;

d) korištenje klasificiranih podataka iz klasificiranog ugovora samo za svrhe vezane uz predmet ugovora;

e) strogo poštivanje odredaba ovog Ugovora u vezi s postupcima za postupanje s klasificiranim podacima;

f) obvezu obavješćivanja nacionalnog sigurnosnog tijela ugovaratelja o bilo kojoj povredi sigurnosti u vezi s klasificiranim ugovorom;

g) ustupanje klasificiranih podataka vezanih uz klasificirani ugovor bilo kojoj trećoj strani samo na temelju prethodnog pisanog pristanka stranke pošiljateljice.

**Članak 10.**
**Posjeti**

1. Posjeti vezani uz provedbu ili pripremu klasificiranog ugovora koji zahtijevaju pristup klasificiranim podacima podliježu prethodnom odobrenju nacionalnog sigurnosnog tijela stranke domaćina. Odobrenje se izdaje na temelju zahtjeva za posjet nacionalnog sigurnosnog tijela stranke posjetitelja.

2. Zahtjev iz stavka 1. ovog članka sadrži:

   a) ime i prezime posjetitelja, datum i mjesto rođenja, državljanstvo;

   b) broj putovnice ili broj druge identifikacijske isprave posjetitelja;

   c) radno mjesto posjetitelja i naziv organizacije koju predstavlja;

   d) stupanj uvjerenja o sigurnosnoj provjeri posjetitelja;

   e) svrhu, predloženi radni program i planirani datum posjeta;

   f) nazive organizacija i objekata za koje se traži posjet;

   g) broj posjeta i traženo razdoblje;

   h) druge podatke, koje dogovore nacionalna sigurnosna tijela.

3. Svaka stranka jamči zaštitu osobnih podataka posjetitelja u skladu sa svojim nacionalnim zakonima i propisima.

**Članak 11.**
**Povreda sigurnosti**

1. U slučaju stvarne povrede sigurnosti ili sumnje u povredu sigurnosti, nacionalno sigurnosno tijelo stranke kod koje se ona dogodila bez odgode obavješćuje nacionalno sigurnosno tijelo stranke pošiljateljice te, u skladu s nacionalnim zakonima i propisima, pokreće odgovarajući postupak kako bi se utvrdile okolnosti povrede sigurnosti. Rezultati postupka prosljeđuju se nacionalnom sigurnosnom tijelu stranke pošiljateljice.

2. Kada do povrede sigurnosti dođe u trećoj državi, nacionalno sigurnosno tijelo stranke pošiljatelja bez odgode poduzima radnje iz stavka 1. ovog članka.

**Članak 12.**
**Troškovi**

1. Ne očekuje se da će provedba ovog Ugovora prouzročiti bilo kakve troškove.

2. U slučaju bilo kakvih troškova, svaka stranka snosi svoje vlastite troškove koji nastanu uslijed provedbe i nadzora nad svim aspektima ovog Ugovora u skladu sa svojim nacionalnim zakonodavstvom.

**Članak 13.**
**Rješavanje sporova**

Bilo koji spor u vezi s tumačenjem ili primjenom ovog Ugovora rješavat će se konzultacijama i pregovorima između stranaka i neće se podnositi na rješavanje bilo kojem međunarodnom sudu ili trećoj strani.

**Članak 14.**
**Završne odredbe**

1. Ovaj Ugovor stupa na snagu datumom primitka posljednje pisane obavijesti kojom stranke obavješćuju jedna drugu, diplomatskim putem, da su ispunjeni njihovi unutarnji pravni uvjeti potrebni za njegovo stupanje na snagu.

2. Ovaj Ugovor može se izmijeniti i dopuniti uzajamnim pisanim pristankom stranaka. Izmjene i dopune stupaju na snagu u skladu s odredbom stavka 1. ovog članka.

3. Ovaj Ugovor sklapa se na neodređeno vrijeme. Svaka stranka može otkazati ovaj Ugovor pisanom obaviješću drugoj stranci diplomatskim putem. U tom slučaju, ovaj Ugovor prestaje šest mjeseci od datuma na koji je druga stranka primila obavijest o otkazu.

4. U slučaju prestanka ovog Ugovora, svi klasificirani podaci razmijenjeni u skladu s ovim Ugovorom nastavljaju se štititi u skladu s ovdje utvrđenim odredbama te se, na zahtjev, vraćaju stranci pošiljateljici.

Sastavljeno u Zagrebu dana 15. prosinca 2020. u dva izvornika, svaki na hrvatskom, španjolskom i engleskom jeziku, pri čemu su svi tekstovi jednako vjerodostojni. U slučaju razlika u tumačenju, mjerodavan je engleski tekst.

**ZA VLADU**
**REPUBLIKE HRVATSKE**

**Maja Čavlović**
predstojnica Ureda
Vijeća za nacionalnu sigurnost

**ZA VLADU**
**KRALJEVINE ŠPANJOLSKE**

**Alonso Dezcallar de Mazarredo**
izvanredni i opunomoćeni veleposlanik
Kraljevine Španjolske u Republici Hrvatskoj

**ACUERDO**

**ENTRE**

**EL GOBIERNO DE LA REPÚBLICA DE CROACIA**

**Y**

**EL GOBIERNO DEL REINO DE ESPAÑA**

**PARA LA PROTECCIÓN MUTUA DE LA INFORMACIÓN CLASIFICADA**

El Gobierno de la República de Croacia y el Gobierno del Reino de España (en lo sucesivo denominados "las Partes"),

Conscientes de que una buena cooperación puede requerir el intercambio de Información Clasificada entre las Partes,

Deseando establecer un conjunto de normas que regule la protección recíproca de la Información Clasificada que se intercambie o se genere en el curso de la cooperación entre las Partes,

Han convenido en lo siguiente:

**Artículo 1**
**Objeto**

El objeto del presente Acuerdo es asegurar la protección de la Información Clasificada que se genere o intercambie habitualmente entre las Partes.

**Artículo 2**
**Definiciones**

A los efectos del presente Acuerdo:

(1) Por "**Información Clasificada**" se entenderá toda información, independientemente de su forma, que requiera protección contra la puesta en riesgo de su seguridad y haya sido clasificada de conformidad con las leyes y reglamentos nacionales de la Parte de Origen;

(2) Por "**Necesidad de Conocer**" se entenderá que el acceso a la Información Clasificada se concederá únicamente a las personas que tengan necesidad comprobada de conocer o disponer de dicha información a efectos del desempeño de sus funciones oficiales y profesionales;

(3) Por "**Infracción de seguridad**" se entenderá cualquier forma de divulgación no autorizada, uso indebido, alteración no autorizada, daño o destrucción de la Información Clasificada, así como cualquier otra acción u omisión que tenga como consecuencia la pérdida de su confidencialidad, integridad o disponibilidad;

(4) Por "**Grado de Clasificación de Seguridad**" se entenderá una categoría que, de conformidad con las leyes y reglamentos nacionales, indica el nivel de restricción de acceso a la Información Clasificada con indicación del nivel de protección mínimo que deben aplicar las Partes;

(5) Por "**Parte de Origen**" se entenderá la Parte que haya creado la Información Clasificada;

(6) Por "**Parte Receptora**" se entenderá la Parte a la que la Parte de Origen transmita la Información Clasificada;

(7) Por "**Autoridad Nacional de Seguridad**" se entenderá la autoridad nacional responsable de la ejecución y supervisión del presente Acuerdo;

(8) Por "**Autoridad Competente**" se entenderá la Autoridad Nacional de Seguridad u otra autoridad nacional que, de conformidad con las leyes y reglamentos nacionales aplique el presente Acuerdo;

(9) Por "**Contratista**" se entenderá toda persona física o jurídica con capacidad para celebrar contratos;

(10) Por "**Contrato Clasificado**" se entenderá todo acuerdo entre dos o más Contratistas que contenga Información Clasificada o cuya ejecución requiera acceso a ella;

(11) Por "**Habilitación Personal de Seguridad**" se entenderá la determinación positiva por la Autoridad Competente de que, de conformidad con las leyes y reglamentos nacionales, una persona reúne los requisitos para tener acceso a Información Clasificada;

(12) Por "**Habilitación de Seguridad de Establecimiento**" se entenderá la determinación positiva, emitida por la Autoridad Competente, de conformidad con las leyes y reglamentos nacionales, según la cual una persona física o jurídica cuenta con la capacidad material y organizativa para el acceso a la Información Clasificada y su manejo;

(13) Por "**Tercero**" se entenderá todo Estado o persona jurídica o física que no sea Parte en el presente Acuerdo.

## Artículo 3
## Grados de Clasificación de Seguridad

Las Partes acuerdan que los siguientes Grados de Clasificación de Seguridad son equivalentes:

| Para la República de Croacia | Para el Reino de España |
|---|---|
| VRLO TAJNO | SECRETO |
| TAJNO | RESERVADO |
| POVJERLJIVO | CONFIDENCIAL |
| OGRANIČENO | DIFUSIÓN LIMITADA |

## Artículo 4
## Autoridades Nacionales de Seguridad

1. Las Autoridades Nacionales de Seguridad de las Partes son:

   Por la República de Croacia:
   - Oficina del Consejo de Seguridad Nacional;

   Por el Reino de España:
   - Oficina Nacional de Seguridad, Centro Nacional de Inteligencia.

2. Las Partes se informarán mutuamente, por conducto diplomático, de cualquier modificación que afecte a sus respectivas Autoridades Nacionales de Seguridad.

3. Las Autoridades Nacionales de Seguridad se facilitarán mutuamente, previa petición, información sobre sus leyes y reglamentos nacionales vigentes que regulen la protección de la Información Clasificada, e intercambiarán información sobre las normas, procedimientos y prácticas de seguridad para la protección de la Información Clasificada.

**Artículo 5**
**Medidas de protección y acceso a la Información Clasificada**

1. De conformidad con sus leyes y reglamentos nacionales, las Partes adoptarán todas las medidas adecuadas para la protección de la Información Clasificada que se intercambie o genere en virtud del presente Acuerdo. Las Partes otorgarán a la Información Clasificada que se transmita el mismo nivel de protección que otorguen a su propia Información Clasificada de Grado de Clasificación de Seguridad equivalente, como se define en el artículo 3 del presente Acuerdo.

2. La Parte de Origen Parte informará a la Parte Receptora, por escrito, de cualquier cambio en los Grados de Clasificación de Seguridad de la información transmitida, con el fin de que se apliquen las medidas de seguridad adecuadas.

3. Sólo tendrán acceso a la Información Clasificada las personas que hayan sido autorizadas de conformidad con sus leyes y reglamentos nacionales para tener acceso a Información Clasificada del Grado de Clasificación de Seguridad equivalente y tengan necesidad de conocerla.

4. En el ámbito del presente Acuerdo, las Partes reconocerán las Habilitaciones Personales de Seguridad y las Habilitaciones de Seguridad de Establecimiento expedidas por la otra Parte.

5. Las Autoridades Competentes se asistirán mutuamente, previa petición y de conformidad con sus leyes y reglamentos nacionales, cuando, en aplicación del presente Acuerdo, se lleven a cabo procedimientos de habilitación.

6. En el ámbito del presente Acuerdo, las Autoridades Nacionales de Seguridad se informarán mutuamente de forma inmediata acerca de cualquier modificación relacionada con Habilitaciones Personales de Seguridad y Habilitaciones de Seguridad de Establecimiento, en especial acerca de una revocación o modificación del Grado de Clasificación de Seguridad.

7. Previa petición de la Autoridad Nacional de Seguridad de la Parte de Origen, la Autoridad Nacional de Seguridad de la Parte Receptora expedirá una confirmación por escrito de que una persona física tiene derecho de acceso a Información Clasificada o de que una persona jurídica le ha sido expedida una Habilitación de Seguridad de Establecimiento.

8. La Parte Receptora:
   a) sólo remitirá Información Clasificada a Terceros con el consentimiento previo por escrito de la Parte de Origen;
   b) marcará la Información Clasificada recibida de conformidad con el Grado de Clasificación de Seguridad equivalente establecido en el artículo 3 del presente Acuerdo;
   c) hará uso de la Información Clasificada tan sólo a los efectos para los que se facilitó.

9. Si otro acuerdo concluido entre las Partes regula de manera más estricta el intercambio o la protección de la Información Clasificada, se aplicarán dichas normas.

**Artículo 6**
**Transmisión de Información Clasificada**

La Información Clasificada se transmitirá por los conductos aprobados recíprocamente por las Autoridades Nacionales de Seguridad. La Parte Receptora acusará por escrito la recepción de la misma.

**Artículo 7**
**Reproducción y Traducción de Información Clasificada**

1. La Información Clasificada como TAJNO / RESERVADO o superior sólo se traducirá o reproducirá en casos excepcionales con el consentimiento previo por escrito de la Parte de Origen.

2. Todas las copias de Información Clasificada deberán marcarse con la marca de clasificación del original. La información reproducida deberá estar protegida de la misma forma que la información original. El número de copias se limitará a las necesarias a efectos oficiales.

3. Las traducciones llevarán la marca de la clasificación de seguridad original y en ellas figurará una anotación, en la lengua de traducción, en la que se haga constar que contienen Información Clasificada de la Parte de Origen.

**Artículo 8**
**Destrucción de Información Clasificada**

1. La Información Clasificada se destruirá de tal manera que haga imposible su reconstrucción total o parcial.

2. La Información clasificada como VRLO TAJNO / SECRETO no será destruida. Deberá devolverse a la Parte de Origen.

3. La Parte de Origen podrá prohibir expresamente, mediante marcas adicionales o el subsiguiente envío de una notificación por escrito, la destrucción de Información Clasificada. Si se ha prohibido la destrucción de Información Clasificada, deberá devolverse a la Parte de Origen.

4. En caso de crisis en el que resulte imposible proteger o devolver Información Clasificada que se haya transmitido o generado con arreglo al presente Acuerdo, se procederá a su destrucción inmediata. La Parte Receptora notificará a la Autoridad Nacional de Seguridad de la Parte de Origen la destrucción de dicha información, tan pronto como sea posible.

**Artículo 9**
**Contratos Clasificados**

1. Los Contratos Clasificados se celebrarán y ejecutarán de acuerdo con las leyes y reglamentos nacionales de las Partes.

2. Previa petición, la Autoridad Nacional de Seguridad de la Parte Receptora confirmará que se ha expedido al Contratista propuesto la pertinente Habilitación Personal de Seguridad o Habilitación de Seguridad de Establecimiento. Si el Contratista propuesto no dispone de una habilitación de seguridad adecuada, la Autoridad Nacional de Seguridad de la Parte de Origen podrá solicitar a la Autoridad Nacional de Seguridad de la Parte Receptora que se le otorgue.

3. Un anexo de seguridad deberá ser parte integrante de cada Contrato Clasificado o subcontrato, para los que la Parte de Origen deberá especificar qué Información Clasificada se cederá a la Parte Receptora, qué Grado de Clasificación de Seguridad se ha asignado a dicha información y las obligaciones del Contratista a efectos de protección de la Información Clasificada.

4. La obligación del Contratista de proteger la Información Clasificada comprenderá, al menos, lo siguiente:

   a) dar acceso a la Información Clasificada únicamente a las personas que hayan sido autorizadas de conformidad con sus leyes y reglamentos nacionales a tener acceso a Información Clasificada del Grado de Clasificación de Seguridad equivalente y tengan Necesidad de Conocer;

b) la transmisión de Información Clasificada por medios de conformidad con el presente Acuerdo;

c) los procedimientos para comunicar todo cambio que pueda darse por lo que respecta a la Información Clasificada;

d) el uso de la Información Clasificada prevista en el Contrato Clasificado únicamente para los fines vinculados al objeto de este;

e) la estricta adhesión a las disposiciones del presente Acuerdo en relación con el manejo de la Información Clasificada;

f) la obligación de notificar a la Autoridad Nacional de Seguridad del Contratista de cualquier Infracción de Seguridad relacionado con el Contrato Clasificado;

g) ceder a un Tercero la Información Clasificada relacionada con el Contrato Clasificado únicamente previo consentimiento por escrito de la Parte de Origen.

**Artículo 10**
**Visitas**

1. Las visitas relacionadas con la ejecución o preparación de un Contrato Clasificado que requieran acceso a Información Clasificada deberán ser autorizadas previamente por la Autoridad Nacional de Seguridad de la Parte anfitriona. El permiso deberá concederse basándose en la solicitud de visita presentada por la Autoridad Nacional de Seguridad de la Parte visitante.

2. La solicitud mencionada en el apartado 1 del presente artículo deberá contener:
   a) nombre y apellido del visitante, fecha y lugar de nacimiento, nacionalidad;
   b) número de pasaporte o de otra tarjeta de identificación del visitante;
   c) cargo del visitante y nombre de la organización que representa;
   d) grado de Habilitación Personal de Seguridad del visitante;
   e) finalidad, programa de trabajo propuesto y fecha prevista de la visita;
   f) nombres de las entidades y de los establecimientos que se solicita visitar;
   g) número de visitas y tiempo requerido;
   h) otros datos, acordados por las Autoridades Nacionales de Seguridad.

3. Cada Parte garantizará la protección de los datos personales de los visitantes, de conformidad con sus leyes y reglamentos nacionales.

**Artículo 11**
**Infracción de Seguridad**

1. En caso de que se produzca o sospeche que se ha producido una Infracción de Seguridad, la Parte en la que se haya producido se lo notificará tan pronto como sea posible a la Autoridad Nacional de Seguridad de la Parte de Origen e iniciará los procedimientos correspondientes, con arreglo a sus leyes y reglamentos nacionales, con el fin de determinar las circunstancias de la Infracción. Los resultados de los procedimientos deberán remitirse a la Autoridad Nacional de Seguridad de la Parte de Origen.

2. Cuando la Infracción de Seguridad se haya producido en un tercer país, la Autoridad Nacional de Seguridad de la Parte de Origen adoptará sin dilación las medidas mencionadas en el apartado 1 del presente artículo.

**Artículo 12**
**Gastos**

1. No está previsto que la aplicación del presente Acuerdo genere gasto alguno.

2. En caso de producirse, cada una de las Partes sufragará sus propios gastos derivados de la aplicación y supervisión de todos los aspectos relativos al presente Acuerdo, de conformidad con su legislación nacional.

**Artículo 13**
**Resolución de conflictos**

Cualquier controversia relativa a la interpretación o aplicación del presente Acuerdo se resolverá mediante consultas y negociaciones entre las Partes y no se someterá a ningún tribunal internacional o a un Tercero para su resolución.

**Artículo 14**
**Disposiciones finales**

1. El presente Acuerdo entrará en vigor en la fecha de recepción de la última notificación escrita por la que las Partes se hayan informado recíprocamente, por conducto diplomático, de que se han completado sus trámites jurídicos internos necesarios para la entrada en vigor.

2. El presente Acuerdo podrá enmendarse por mutuo consentimiento de las Partes expresado por escrito. Las enmiendas entrarán en vigor de conformidad con lo dispuesto en el apartado 1 del presente artículo.

3. El presente Acuerdo se concluye por un periodo indefinido. Cada Parte podrá denunciar el presente Acuerdo mediante notificación previa por escrito a la otra Parte por conducto diplomático. En tal caso, el presente Acuerdo se dará por terminado seis meses después de la fecha en la que la otra Parte recibió el escrito de cancelación.

4. En caso de denuncia del presente Acuerdo, toda la Información Clasificada intercambiada conforme al mismo continuará protegida de conformidad con sus disposiciones y, previa petición, será devuelta a la Parte de Origen.

Hecho en Zagreb el 15 de diciembre de 2020 en dos ejemplares originales, ambos en croata, español e inglés, siendo todos los textos igualmente auténticos. En caso de discrepancias en la interpretación, prevalecerá el texto inglés.

**POR EL GOBIERNO DE LA REPÚBLICA DE CROACIA**

**Maja Čavlović**
Directora de la Oficina del Consejo de Seguridad Nacional

**POR EL GOBIERNO DEL REINO DE ESPAÑA**

**Alonso Dezcallar de Mazarredo**
Embajador Extraordinario y Plenipotenciario del Reino de España en la República de Croacia

# AGREEMENT
# BETWEEN
# THE GOVERNMENT OF THE REPUBLIC OF CROATIA
# AND
# THE GOVERNMENT OF THE KINGDOM OF SPAIN
# ON MUTUAL PROTECTION OF CLASSIFIED INFORMATION

The Government of the Republic of Croatia and the Government of the Kingdom of Spain (hereinafter referred to as "the Parties"),

Realizing that good co-operation 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
## Objective

The objective of this Agreement is 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 compromise and has been classified in accordance with national laws and regulations of the Originating Party;

(2) "**Need-to-Know**" means that access to Classified Information may only be granted to persons who have a verified requirement for knowledge or possession of such information in order to perform their official and professional duties;

(3) "**Security Breach**" means any form of unauthorized disclosure, misuse, unauthorized 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) "**Security Classification Level**" means a category which, in accordance with national laws and regulations, characterises the level of restriction of access to Classified Information and the minimum level of its protection by the Parties;

(5) "**Originating Party**" means the Party that has created the Classified Information;

(6) "**Receiving Party**" means the Party to which Classified Information of the Originating Party is transmitted;

(7) "**National Security Authority**" means the national authority responsible for the implementation and supervision of this Agreement;

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

(9) "**Contractor**" means an individual or a legal entity possessing the legal capacity to conclude contracts;

(10) "**Classified Contract**" means an agreement between two or more Contractors, which contains or the execution of which requires access to Classified Information;

(11) "**Personnel Security Clearance**" means the determination by the Competent Authority confirming, in accordance with national laws and regulations, that the individual is eligible to have access to Classified Information;

(12) "**Facility Security Clearance**" means the determination by the Competent 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;

(13) "**Third Party**" means any state, organization, legal entity or individual, which 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 Republic of Croatia | For the Kingdom of Spain |
|---|---|
| VRLO TAJNO | SECRETO |
| TAJNO | RESERVADO |
| POVJERLJIVO | CONFIDENCIAL |
| OGRANIČENO | DIFUSIÓN LIMITADA |

## Article 4
## National Security Authorities

1. The National Security Authorities of the Parties are:

   For the Republic of Croatia:
   - Office of the National Security Council;

   For the Kingdom of Spain:
   - National Office of Security, National Intelligence Centre.

2. The Parties shall inform each other through diplomatic channels of any changes to their respective National Security Authorities.

3. 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. The same level of protection shall be ensured for such 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.

2. 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.

3. 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.

4. Within the scope of this Agreement, each Party shall recognize the Personnel Security Clearances and Facility Security Clearances issued by the other Party.

5. The Competent 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.

6. Within the scope of this Agreement, the National Security Authorities shall inform each other without delay about any alteration with regard to Personnel Security Clearances and Facility Security Clearances, in particular about the revocation or the alteration of the Security Classification Level.

7. Upon 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 or a legal entity has been issued a Facility Security Clearance.

8. 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 of this Agreement;
   c) use Classified Information only for the purposes that it has been provided for.

9. If any other agreement concluded between the Parties contains stricter regulations regarding the exchange or protection of Classified Information, these regulations shall apply.

## Article 6
## Transmission of Classified Information

Classified Information shall be transmitted through channels mutually approved by the National Security Authorities. The Receiving Party shall confirm the receipt of Classified Information in writing.

**Article 7**
**Reproduction and Translation of Classified Information**

1. Information classified as TAJNO / RESERVADO 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 classification marking. Such reproduced information shall be protected in the same way as the original information. The number of copies shall be limited to that required for official purposes.

3. The translation shall be marked with the original classification marking and shall bear an additional 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 such a manner as to eliminate the possibility of its partial or total reconstruction.

2. Information classified as VRLO TAJNO / SECRETO shall not be destroyed. It shall be returned to the Originating Party.

3. The Originating Party may, by additional marking or sending subsequent written notice, expressly prohibit destruction of Classified Information. If 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. The Receiving Party shall notify the National Security Authority of the Originating Party about this destruction as soon as possible.

**Article 9**
**Classified Contracts**

1. Classified Contracts shall be concluded and implemented in accordance with national laws and regulations of each Party.

2. Upon request the National Security Authority of the Receiving Party shall confirm that a proposed Contractor has been issued an appropriate Personnel Security Clearance or Facility Security Clearance. If the proposed Contractor does not hold an appropriate security clearance, the National Security Authority of the Originating Party may request the National Security Authority of the Receiving Party to issue the appropriate security clearance.

3. A security annex shall be an integral part of each Classified Contract or sub-contract by which the Originating Party shall specify which Classified Information is to be released to the Receiving Party, which Security Classification Level has been assigned to that information and the Contractor's obligations to protect the Classified Information.

4. The Contractor's obligations to protect the Classified Information shall refer, at least, to the following:

   a) disclosure of Classified Information exclusively 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;

b) transmission of Classified Information by the means in accordance with this Agreement;

c) the procedures for communicating any changes that may arise in respect of Classified Information;

d) usage of Classified Information under the Classified Contract only for the purposes related to the subject of the contract;

e) strict adherence to the provisions of this Agreement related to the procedures for handling of Classified Information;

f) the obligation to notify the Contractor's National Security Authority of any Security Breach related to the Classified Contract;

g) release of Classified Information related to the Classified Contract to any Third Party only upon prior written consent of the Originating Party.

**Article 10**
**Visits**

1. Visits related to the execution or preparation of a Classified Contract requiring access to Classified Information are subject to prior permission by the National Security Authority of the host Party. The permission shall be granted on the basis of a visit request by the National Security Authority of the visiting Party.

2. The request referred to in paragraph 1 of this Article shall contain:
   a) visitor's name and surname, date and place of birth, citizenship;
   b) passport number or another identification card number of the visitor;
   c) position of the visitor and name of the organization represented;
   d) level of the Personnel Security Clearance of the visitor;
   e) purpose, proposed working program and planned date of the visit;
   f) names of organizations and facilities requested to be visited;
   g) number of visits and period required;
   h) other data, agreed upon by the National Security Authorities.

3. Each Party shall guarantee the protection of personal data of the visitors in accordance with its national laws and regulations.

**Article 11**
**Security Breach**

1. In case of actual or suspected Security Breach, the National Security Authority of the Party where it has occurred shall, without delay, inform the National Security Authority of the Originating Party and, in accordance with national laws and regulations, initiate appropriate proceedings, in order to determine the circumstances of the Security Breach. The results of the proceedings shall be forwarded to the National Security Authority of the Originating Party.

2. When the Security Breach has occurred in a third state, the National Security Authority of the sending Party shall take the actions referred to in paragraph 1 of this Article without delay.

**Article 12**
**Expenses**

1. The implementation of this Agreement is not expected to incur any cost.

2. In case of any cost, each Party shall bear its own expenses incurred by the implementation and supervision of all aspects of this Agreement in accordance with its national legislation.

**Article 13**
**Settlement of Disputes**

Any dispute regarding the interpretation or application of this Agreement shall be settled by consultations and negotiations between the Parties and shall not be referred to any international tribunal or Third Party for settlement.

**Article 14**
**Final Provisions**

1. This Agreement shall enter into force on the date of receipt of the last written notification by which the Parties have informed each other, through diplomatic channels, that their internal legal requirements necessary for its entry into force have been fulfilled.

2. This Agreement may be amended by mutual written consent of the Parties. Amendments shall enter into force in accordance with the provision of paragraph 1 of this Article.

3. This Agreement is concluded for an indefinite period of time. Either Party may denounce this Agreement by giving the other Party written notice through diplomatic channels. In that case, this Agreement shall terminate six months from the date on which the other Party has received the denunciation notice.

4. In case of termination of this Agreement, all Classified Information exchanged pursuant to this Agreement shall continue to be protected in accordance with the provisions set forth herein and, upon request, returned to the Originating Party.

Done at Zagreb on 15 December 2020 in two originals, each in the Croatian, Spanish and English languages, all texts being equally authentic. In case of any divergence of interpretation, the English text shall prevail.

**FOR THE GOVERNMENT OF THE REPUBLIC OF CROATIA**

**Maja Čavlović**
Director of the Office of the National Security Council

**FOR THE GOVERNMENT OF THE KINGDOM OF SPAIN**

**Alonso Dezcallar de Mazarredo**
Ambassador Extraordinary and Plenipotentiary of the Kingdom of Spain to the Republic of Croatia