P.Z. br. 559

HRVATSKI SABOR

KLASA: 022-02/23-01/92
URBROJ: 65-23-2

Zagreb, 27. rujna 2023.

ZASTUPNICAMA I ZASTUPNICIMA
HRVATSKOGA SABORA

PREDSJEDNICAMA I PREDSJEDNICIMA
RADNIH TIJELA

Na temelju članaka 178. i 192., a u vezi s člankom 207.a Poslovnika Hrvatskoga sabora u prilogu upućujem ***Konačni prijedlog zakona o potvrđivanju Ugovora između Vlade Republike Hrvatske i Vlade Savezne Republike Njemačke o razmjeni i uzajamnoj zaštiti klasificiranih podataka,*** koji je predsjedniku Hrvatskoga sabora podnijela Vlada Republike Hrvatske, aktom od 27. rujna 2023. godine.

Za svoje predstavnike, koji će u njezino ime sudjelovati u radu Hrvatskoga sabora i njegovih radnih tijela, Vlada je odredila potpredsjednika Vlade Republike Hrvatske i ministra hrvatskih branitelja Tomu Medveda, državne tajnike Darka Nekića i dr. sc. Špiru Janovića, dr. med., te predstojnika Ureda Vijeća za nacionalnu sigurnost mr. sc. Valentina Franjića.

PREDSJEDNIK

Gordan Jandroković

VLADA REPUBLIKE HRVATSKE

KLASA: 022-03/22-11/02
URBROJ: 50301-29/23-23-11

Zagreb, 27. rujna 2023.

PREDSJEDNIKU HRVATSKOGA SABORA

PREDMET: Konačni prijedlog zakona o potvrđivanju Ugovora između Vlade Republike Hrvatske i Vlade Savezne Republike Njemačke o razmjeni i 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, 123/20. i 86/23. - Odluka Ustavnog suda Republike Hrvatske), Vlada Republike Hrvatske podnosi Konačni prijedlog zakona o potvrđivanju Ugovora između Vlade Republike Hrvatske i Vlade Savezne Republike Njemačke o razmjeni i uzajamnoj zaštiti klasificiranih podataka.

Za svoje predstavnike, koji će u njezino ime sudjelovati u radu Hrvatskoga sabora i njegovih radnih tijela, Vlada je odredila potpredsjednika Vlade Republike Hrvatske i ministra hrvatskih branitelja Tomu Medveda, državne tajnike Darka Nekića i dr. sc. Špiru Janovića, dr. med., te predstojnika Ureda Vijeća za nacionalnu sigurnost mr. sc. Valentina Franjića.

PREDSJEDNIK

mr. sc. Andrej Plenković

VLADA REPUBLIKE HRVATSKE

KONAČNI PRIJEDLOG ZAKONA O POTVRĐIVANJU UGOVORA IZMEĐU VLADE REPUBLIKE HRVATSKE I VLADE SAVEZNE REPUBLIKE NJEMAČKE O RAZMJENI I UZAJAMNOJ ZAŠTITI KLASIFICIRANIH PODATAKA

Zagreb, rujan 2023.

KONAČNI PRIJEDLOG ZAKONA O POTVRĐIVANJU UGOVORA IZMEĐU VLADE REPUBLIKE HRVATSKE I VLADE SAVEZNE REPUBLIKE NJEMAČKE O RAZMJENI I UZAJAMNOJ ZAŠTITI KLASIFICIRANIH PODATAKA

I. USTAVNA OSNOVA

Ustavna osnova za donošenje Zakona o potvrđivanju Ugovora između Vlade Republike Hrvatske i Vlade Savezne Republike Njemačke o razmjeni i 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 OSNOVNA PITANJA KOJA SE PREDLAŽU UREDITI ZAKONOM TE POSLJEDICE KOJE ĆE DONOŠENJEM ZAKONA PROISTEĆI

Potreba za međunarodnom razmjenom podataka ili materijala, koji su prema nacionalnom zakonodavstvu klasificirani odnosno 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 druga područja rada države (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 država i organizacija kao i u postupcima sklapanja međunarodnih ugovora kojima se razmjenjuju i štite klasificirani podaci između Republike Hrvatske i drugih država 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 Savezne Republike Njemačke 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 na to da su tijekom 2007. doneseni zakoni kojima je uređeno područje zaštite klasificiranih podataka u Republici Hrvatskoj, ocijenjeno je da postoji potreba za uređivanjem suradnje između Republike Hrvatske i Savezne Republike Njemačke u području zaštite klasificiranih podataka.

Sukladno rješenjima i standardima utvrđenim u spomenutim propisima, potpisan je 18. travnja 2023. u Zagrebu, Ugovor između Vlade Republike Hrvatske i Vlade Savezne Republike Njemačke o razmjeni i uzajamnoj zaštiti klasificiranih podataka, kojim se u odnosima Republike Hrvatske i Savezne Republike Njemačke 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 Savezne Republike Njemačke o razmjeni i 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, 123/20. i 86/23. – Odluka Ustavnog suda Republike Hrvatske), 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 Savezne Republike Njemačke o razmjeni i uzajamnoj zaštiti klasificiranih podataka značajan mehanizam za ostvarivanje zaštite u području informacijske sigurnosti te zaštite klasificiranih podataka koji se razmjenjuju između Republike Hrvatske i Savezne Republike Njemačke 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 SAVEZNE REPUBLIKE NJEMAČKE O RAZMJENI I UZAJAMNOJ ZAŠTITI KLASIFICIRANIH PODATAKA

Članak 1.

Potvrđuje se Ugovor između Vlade Republike Hrvatske i Vlade Savezne Republike Njemačke o razmjeni i uzajamnoj zaštiti klasificiranih podataka, potpisan u Zagrebu 18. travnja 2023., u izvorniku na hrvatskom, njemačkom i engleskom jeziku.

Članak 2.

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

Ugovor

između

Vlade Republike Hrvatske

i

Vlade Savezne Republike Njemačke

o

razmjeni i uzajamnoj zaštiti klasificiranih podataka

Vlada Republike Hrvatske
i
Vlada Savezne Republike Njemačke,
u daljnjem tekstu „ugovorne stranke“,

u namjeri osiguravanja zaštite klasificiranih podataka koji se razmjenjuju između nadležnih tijela Republike Hrvatske i Savezne Republike Njemačke, kao i s ugovarateljima ili između ugovaratelja dviju ugovornih stranaka,

želeći usuglasiti pravni okvir za razmjenu i uzajamnu zaštitu klasificiranih podataka koji se primjenjuje na sve instrumente o suradnji koji se sklapaju između ugovornih stranaka i na ugovore koji uključuju razmjenu klasificiranih podataka,

sporazumjele su se kako slijedi:

Članak 1.
Definicije

(1) Za potrebe ovog Ugovora

1. „klasificirani podaci“ su

   a) u Republici Hrvatskoj
   bilo koji podaci, neovisno o njihovom obliku, koje treba zaštititi i koji su klasificirani u skladu s nacionalnim zakonima i propisima ili ih je kao takve ustupila druga država, međunarodna organizacija ili institucija s kojom Republika Hrvatska surađuje;

   b) u Saveznoj Republici Njemačkoj
   činjenice, predmeti ili podaci koji, neovisno o obliku u kojem se pojavljuju, u javnom interesu trebaju ostati tajni. Klasificira ih službeno tijelo, ili se klasificiraju na njegov zahtjev, u skladu s njihovom potrebom za zaštitom;

2. „klasificirani ugovor“ je ugovor između tijela ili poduzeća iz države jedne ugovorne stranke (naručitelj) i poduzeća iz države druge ugovorne stranke (ugovaratelj); u skladu s takvim ugovorom, klasificirani podaci iz države naručitelja ustupaju se ugovaratelju, ili ih ugovaratelj stvara, ili ih treba učiniti dostupnima zaposlenicima ugovaratelja koji trebaju obavljati zadaće u objektima naručitelja.

(2) Stupnjevi tajnosti utvrđuju se kako slijedi:

1. U Republici Hrvatskoj klasificirani podaci su

   a) VRLO TAJNO ako bi neovlašteno otkrivanje i pristup neovlaštenih osoba tim podacima nanio nepopravljivu štetu nacionalnoj sigurnosti i vitalnim interesima Republike Hrvatske,

   b) TAJNO ako bi neovlašteno otkrivanje i pristup neovlaštenih osoba tim podacima teško naštetio nacionalnoj sigurnosti i vitalnim interesima Republike Hrvatske,

   c) POVJERLJIVO ako bi neovlašteno otkrivanje i pristup neovlaštenih osoba tim podacima naštetio nacionalnoj sigurnosti i vitalnim interesima Republike Hrvatske,

   d) OGRANIČENO ako bi neovlašteno otkrivanje i pristup neovlaštenih osoba tim podacima naštetio djelovanju državnih tijela.

2. U Saveznoj Republici Njemačkoj klasificirani podaci su

   a) STRENG GEHEIM ako pristup neovlaštenih osoba tim podacima može predstavljati prijetnju za postojanje ili vitalne interese Savezne Republike Njemačke ili jedne od njezinih saveznih pokrajina,

   b) GEHEIM ako pristup neovlaštenih osoba tim podacima može predstavljati prijetnju za sigurnost Savezne Republike Njemačke ili jedne od njezinih saveznih pokrajina, ili može izazvati tešku štetu njihovim interesima,

   c) VS-VERTRAULICH ako pristup neovlaštenih osoba tim podacima može biti štetan za interese Savezne Republike Njemačke ili jedne od njezinih saveznih pokrajina,

   d) VS-NUR FÜR DEN DIENSTGEBRAUCH ako pristup neovlaštenih osoba tim podacima može biti nepovoljan za interese Savezne Republike Njemačke ili jedne od njezinih saveznih pokrajina.

Članak 2.
Stupnjevi tajnosti

Ugovorne stranke utvrđuju da su sljedeći stupnjevi tajnosti istoznačni:

Republika Hrvatska	Savezna Republika Njemačka
VRLO TAJNO	STRENG GEHEIM
TAJNO	GEHEIM
POVJERLJIVO	VS-VERTRAULICH
OGRANIČENO	VS-NUR FÜR DEN DIENSTGEBRAUCH

Članak 3.
Označavanje

(1) Prenesene klasificirane podatke istoznačnim nacionalnim stupnjem tajnosti kako je navedeno u članku 2. dodatno označava nadležno sigurnosno tijelo primatelja ili se označavaju na njegov zahtjev.

(2) Klasificirani podaci koji nastanu u državi ugovorne stranke primateljice u vezi s klasificiranim ugovorima, kao i umnoženi primjerci, izvatci i prijevodi izrađeni u državi ugovorne stranke primateljice, također se označavaju na taj način.

(3) Prijevod nosi odgovarajuću napomenu na jeziku prijevoda da prijevod sadrži klasificirane podatke ugovorne stranke pošiljateljice.

(4) Odluku o promjeni ili ukidanju stupnjeva tajnosti donose isključivo nadležna sigurnosna tijela ugovorne stranke pošiljateljice. Nadležno sigurnosno tijelo ugovorne stranke pošiljateljice odmah obavješćuje nadležno sigurnosno tijelo ugovorne stranke primateljice o promjeni ili ukidanju bilo kojeg stupnja tajnosti. Nadležno sigurnosno tijelo ugovorne stranke primateljice na isti način provodi tu promjenu ili ukidanje.

Članak 4.
Mjere na nacionalnoj razini

(1) U okviru područja primjene svojih odnosnih nacionalnih zakona i propisa, ugovorne stranke poduzimaju sve odgovarajuće mjere kako bi jamčile zaštitu klasificiranih podataka koji nastaju, koji se razmjenjuju ili s kojima se postupa u skladu s odredbama ovog Ugovora. One takvim

klasificiranim podacima pružaju stupanj zaštite usporediv s onim koji ugovorna stranka primateljica zahtijeva za svoje vlastite klasificirane podatke istoznačnog stupnja tajnosti.

(2) Klasificirani podaci koriste se isključivo za određenu svrhu. Ugovorna stranka primateljica koristi ili odobrava pristup, ili dopušta korištenje ili odobravanje pristupa bilo kojim klasificiranim podacima isključivo za svrhe i u okviru bilo kojih ograničenja koja je odredila ugovorna stranka pošiljateljica ili koja su određena u njezino ime. Ugovorna stranka pošiljateljica mora dati svoj pisani pristanak za bilo koje drugačije postupanje prije ustupanja klasificiranih podataka.

(3) Pristup klasificiranim podacima može se odobriti isključivo osobama kojima je to nužno za obavljanje poslova iz djelokruga s obzirom na njihove zadaće i - osim u slučaju klasificiranih podataka stupnja tajnosti OGRANIČENO / VS-NUR FÜR DEN DIENSTGEBRAUCH - kojima je izdano uvjerenje o sigurnosnoj provjeri ili na temelju svoje dužnosti imaju pravo pristupa klasificiranim podacima istoznačnog stupnja tajnosti. Uvjerenje o sigurnosnoj provjeri izdaje se tek nakon provođenja sigurnosne provjere po standardima koji su usporedivi s onima koji se primjenjuju za pristup nacionalnim klasificiranim podacima istoznačnog stupnja tajnosti.

(4) Državljaninu države jedne ugovorne stranke pristup klasificiranim podacima stupnja tajnosti POVJERLJIVO / VS-VERTRAULICH ili višeg odobrava se bez prethodnog ovlaštenja ugovorne stranke pošiljateljice.

(5) Uvjerenja o sigurnosnoj provjeri za državljane države ugovorne stranke koji borave i imaju potrebu pristupa klasificiranim podacima u svojoj vlastitoj državi izdaju njihova nadležna sigurnosna tijela.

(6) Članci 6. i 7. ovog Ugovora ne primjenjuju se na klasificirane podatke stupnja tajnosti OGRANIČENO / VS-NUR FÜR DEN DIENSTGEBRAUCH.

(7) Ugovorne stranke, svaka unutar svoje države, osiguravaju provođenje potrebnih sigurnosnih nadzora i pridržavanje ovog Ugovora.

Članak 5.
Uništavanje klasificiranih podataka

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

(2) Klasificirani podaci stupnja tajnosti VRLO TAJNO / STRENG GEHEIM se ne uništavaju. Oni se vraćaju ugovornoj stranci pošiljateljici na zahtjev ili ako određena svrha više ne postoji.

(3) Klasificirani podaci stupnja tajnosti TAJNO / GEHEIM ili POVJERLJIVO / VS-VERTRAULICH mogu se uništiti ako to pisano odobri ugovorna stranka pošiljateljica.

(4) Ugovorna stranka primateljica može uništiti klasificirane podatke stupnja tajnosti OGRANIČENO / VS-NUR FÜR DEN DIENSTGEBRAUCH ako određena svrha više ne postoji.

(5) U kriznoj situaciji u kojoj je nemoguće zaštititi ili vratiti klasificirane podatke razmijenjene ili nastale u skladu s ovim Ugovorom, klasificirani podaci se odmah uništavaju. Ugovorna stranka primateljica što je prije moguće obavješćuje nadležno sigurnosno tijelo ugovorne stranke pošiljateljice o tom uništavanju.

Članak 6.
Sklapanje klasificiranih ugovora

(1) Prije sklapanja klasificiranog ugovora naručitelj, putem svog nadležnog sigurnosnog tijela, pribavlja uvjerenje o sigurnosnoj provjeri pravne osobe od nadležnog sigurnosnog tijela ugovaratelja kako bi dobio potvrdu podliježe li potencijalni ugovaratelj sigurnosnom nadzoru nadležnog sigurnosnog tijela svoje države i je li taj ugovaratelj poduzeo sigurnosne mjere potrebne za provedbu klasificiranog ugovora. U slučaju da ugovaratelj još ne podliježe sigurnosnom nadzoru, može se podnijeti zahtjev u tu svrhu.

(2) Uvjerenje o sigurnosnoj provjeri pravne osobe pribavlja se i ako je od potencijalnog ugovaratelja zatraženo da preda ponudu i ako će klasificirane podatke stupnja tajnosti POVJERLJIVO / VS-VERTRAULICH ili višeg trebati ustupiti prije sklapanja klasificiranog ugovora tijekom natječajnog postupka.

(3) U slučajevima iz gore navedenih stavaka (1) i (2) primjenjuje se sljedeći postupak:

1. Zahtjevi za izdavanje uvjerenja o sigurnosnoj provjeri pravne osobe za ugovaratelje iz države druge ugovorne stranke sadrže podatke o projektu, kao i prirodi, opsegu i stupnju tajnosti klasificiranih podataka za koje se očekuje da će biti ustupljeni ugovaratelju ili da će ih on stvoriti.

2. Osim punog naziva ugovaratelja, njegove poštanske adrese, imena savjetnika za informacijsku sigurnost, njegovog broja telefona i telefaksa te njegove adrese elektroničke pošte, uvjerenja o sigurnosnoj provjeri pravne osobe moraju sadržavati podatke posebice o opsegu u kojem je i stupnju tajnosti do kojeg je odnosni ugovaratelj poduzeo sigurnosne mjere na temelju svojih nacionalnih zakona i propisa.

3. Nadležna sigurnosna tijela ugovornih stranaka obavješćuju jedno drugo o bilo kojim promjenama činjenica na temelju kojih su uvjerenja o sigurnosnoj provjeri pravne osobe izdana.

4. Razmjena takvih obavijesti između nadležnih sigurnosnih tijela ugovornih stranaka obavlja se na nacionalnom jeziku tijela koje se obavješćuje ili na engleskom jeziku.

5. Uvjerenja o sigurnosnoj provjeri pravne osobe i zahtjevi koji se upućuju odnosnim nadležnim sigurnosnim tijelima ugovornih stranaka za izdavanje uvjerenja o sigurnosnoj provjeri pravne osobe prenose se pisano.

Članak 7.
Provedba klasificiranih ugovora

(1) Klasificirani ugovori moraju sadržavati klauzulu o sigurnosnim zahtjevima prema kojoj je ugovaratelj obvezan osigurati uvjete potrebne za zaštitu klasificiranih podataka u skladu s nacionalnim zakonima i propisima svoje države.

(2) Osim toga, klauzula o sigurnosnim zahtjevima sadrži sljedeće odredbe:

1. definiciju pojma „klasificirani podaci“ i istoznačnice stupnjeva tajnosti država dviju ugovornih stranaka u skladu s odredbama ovog Ugovora;

2. uvjet da se klasificirani podaci ustupaju trećoj strani, ili da se takvo ustupanje trećoj strani odobrava, isključivo ako je to pisano odobrila ugovorna stranka pošiljateljica;

3. uvjet da ugovaratelj odobrava pristup klasificiranim podacima isključivo osobi kojoj je to nužno za obavljanje poslova iz djelokruga i koja je zadužena za provedbu ili doprinosi provedbi klasificiranog ugovora te joj je - osim u slučaju klasificiranih podataka stupnja tajnosti OGRANIČENO / VS-NUR FÜR DEN DIENSTGEBRAUCH - unaprijed izdano uvjerenje o sigurnosnoj provjeri za odgovarajući stupanj tajnosti;

4. nazive odnosnih nadležnih tijela ugovornih stranaka zaduženih za odobravanje ustupanja klasificiranih podataka u vezi sa sklapanjem klasificiranih ugovora ili ovlaštenih za koordinaciju zaštite takvih klasificiranih podataka;

5. načine prijenosa klasificiranih podataka između nadležnih tijela i uključenih ugovaratelja;

6. postupke i mehanizme obavješćivanja o promjenama koje mogu nastati u vezi s klasificiranim podacima, bilo zbog promjene, bilo zbog ukidanja njihovih stupnjeva tajnosti;

7. postupke odobravanja posjeta objektima, ili pristupa klasificiranim podacima, za zaposlenike ugovaratelja;

8. postupke prijenosa klasificiranih podataka ugovarateljima koji postupaju s takvim klasificiranim podacima; i

9. uvjet da ugovaratelj odmah obavješćuje svoje nadležno tijelo o bilo kojem stvarnom gubitku ili sumnji u gubitak, neovlašteno otkrivanje ili neovlašteno ustupanje klasificiranih podataka obuhvaćenih klasificiranim ugovorom.

(3) Nadležno sigurnosno tijelo naručitelja dostavlja ugovaratelju zasebni popis (naputak o klasificiranju) svih dokumenata kojima je potrebno odrediti stupanj tajnosti, određuje potrebni stupanj tajnosti i osigurava dodavanje tog naputka o klasificiranju kao priloga klasificiranom ugovoru. Također, nadležno sigurnosno tijelo naručitelja dužno je prenijeti, ili pokrenuti prijenos tog naputka o klasificiranju, nadležnom sigurnosnom tijelu ugovaratelja.

(4) Nadležno sigurnosno tijelo naručitelja osigurava da će pristup klasificiranim podacima ugovaratelju biti odobren tek nakon primitka odgovarajućeg uvjerenja o sigurnosnoj provjeri pravne osobe od nadležnog sigurnosnog tijela ugovaratelja.

Članak 8.
Prijenos klasificiranih podataka

(1) Klasificirani podaci stupnja tajnosti VRLO TAJNO / STRENG GEHEIM prenose se između ugovornih stranaka isključivo putem ovlaštenih državnih tijela, u skladu s odnosnim nacionalnim zakonima i propisima.

(2) U načelu, klasificirani podaci stupnjeva tajnosti POVJERLJIVO / VS-VERTRAULICH i TAJNO / GEHEIM prenose se iz jedne države u drugu putem službenog dostavljača. Nadležna sigurnosna tijela ugovornih stranaka mogu dogovoriti druge načine prijenosa. Klasificirani podaci dostavljaju se primatelju u skladu s nacionalnim zakonima i propisima, a primitak klasificiranih podataka potvrđuje nadležno tijelo ili se potvrđuje na njegov zahtjev.

(3) Nadležna sigurnosna tijela ugovornih stranaka mogu dogovoriti - općenito ili uz ograničenja - da se klasificirani podaci stupnjeva tajnosti POVJERLJIVO / VS-VERTRAULICH i TAJNO / GEHEIM mogu prenositi na drugi način osim službenim dostavljačem. U takvim slučajevima,

1. dostavljač mora biti ovlašten za pristup klasificiranim podacima istoznačnog stupnja tajnosti,

2. pošiljatelj mora zadržati popis klasificiranih podataka koji se prenose; primjerak tog popisa predaje se primatelju za dostavu nadležnom tijelu,

3. klasificirani podaci moraju se pakirati u skladu s propisima kojima se uređuje prijevoz unutar državnih granica,

4. klasificirani podaci moraju se dostavljati uz potvrdu primitka, i

5. dostavljač mora imati dostavljačko pismo koje je izdalo nadležno tijelo pošiljatelja.

(4) Kada treba prenositi klasificirane podatke, prijevozno sredstvo, rutu i po potrebi pratnju posebno za svaki slučaj utvrđuju nadležna sigurnosna tijela na temelju detaljnog plana prijevoza.

(5) Kao dodatno alternativno sredstvo prijenosa, klasificirani podaci do i uključujući stupanj tajnosti POVJERLJIVO / VS-VERTRAULICH mogu se prenositi putem privatnih dostavljačkih službi kojima nije izdano uvjerenje o sigurnosnoj provjeri, pod uvjetom da su ispunjeni sljedeći uvjeti:

1. Dostavljačka služba ima svoje sjedište na državnom području jedne od država ugovornih stranaka i ima uspostavljen zaštitni sigurnosni program za postupanje s vrijednim predmetima uz potpis o preuzimanju, uključujući kontinuiranu evidenciju o čuvanju, bilo na temelju evidencije potpisa i tehničkog popisa, bilo putem elektroničkog sustava za praćenje ili traženje.

2. Dostavljačka služba obavezna je na temelju potpisa voditi evidenciju o primitku i dostavi na temelju koje pošiljatelju izdaje potvrdu o dostavi ili je izdaje na temelju popratne dokumentacije koja sadrži registracijski broj pošiljke.

3. Dostavljačka služba mora jamčiti da će pošiljka biti dostavljena primatelju do točno određenog vremena i datuma unutar razdoblja od 24 sata.

4. Dostavljačka služba može angažirati vanjskog suradnika ili podugovaratelja. Međutim, dostavljačka služba odgovorna je za ispunjavanje gore navedenih uvjeta.

(6) Klasificirani podaci stupnja tajnosti VRLO TAJNO / STRENG GEHEIM ne prenose se elektroničkim putem.

(7) Elektronički prijenos klasificiranih podataka stupnjeva tajnosti POVJERLJIVO / VS-VERTRAULICH i TAJNO / GEHEIM moguć je isključivo u kriptiranom obliku. Klasificirani podaci tih stupnjeva tajnosti mogu se kriptirati isključivo sredstvima za kriptiranje koja su međusobnim dogovorom odobrila nadležna sigurnosna tijela ugovornih stranaka.

(8) Klasificirani podaci stupnja tajnosti OGRANIČENO / VS-NUR FÜR DEN DIENSTGEBRAUCH mogu se prenositi putem pošte ili drugih dostavnih službi primateljima unutar državnog područja države druge ugovorne stranke, uzimajući u obzir nacionalne zakone i propise.

(9) Klasificirani podaci stupnja tajnosti OGRANIČENO / VS-NUR FÜR DEN DIENSTGEBRAUCH mogu se prenositi elektronički ili se pristup tim podacima može omogućiti pomoću komercijalnih uređaja za kriptiranje koje je odobrilo nadležno sigurnosno tijelo ugovorne stranke pošiljatelja. Klasificirani podaci tog stupnja tajnosti mogu se prenositi u nekriptiranom obliku samo ako to nije u suprotnosti s nacionalnim zakonima i propisima, ako nisu dostupna odobrena sredstva za kriptiranje, ako se prijenos odvija samo unutar fiksnih mreža, a pošiljatelj i primatelj su se unaprijed usuglasili o predloženom prijenosu.

Članak 9.
Posjeti

(1) U načelu, posjetiteljima iz države jedne ugovorne stranke pristup klasificiranim podacima te objektima i kojima zaposlenici postupaju s klasificiranim podacima, u državi druge ugovorne stranke, bit će odobren isključivo uz prethodno odobrenje nadležnog sigurnosnog tijela ugovorne stranke čija se država posjećuje. Takvo odobrenje daje se isključivo osobama kojima je to nužno za obavljanje poslova iz djelokruga i koje su - osim u slučaju klasificiranih podataka stupnja tajnosti OGRANIČENO / VS-NUR FÜR DEN DIENSTGEBRAUCH - ovlaštene za pristup klasificiranim podacima.

(2) Zahtjevi za posjet podnose se, pravovremeno i u skladu sa zakonima i propisima države ugovorne stranke na čije državno područje ti posjetitelji žele ući, nadležnom sigurnosnom tijelu te države. Nadležna sigurnosna tijela obavješćuju jedno drugo o pojedinostima u vezi s takvim zahtjevima i osiguravaju zaštitu osobnih podataka.

(3) Zahtjevi za posjete podnose se na jeziku države koju se posjećuje ili na engleskom jeziku i sadrže sljedeće podatke:

1. ime i prezime posjetitelja, datum i mjesto rođenja te broj putovnice ili osobne iskaznice;

2. državljanstvo posjetitelja;

3. naznaku radnog mjesta posjetitelja i naziv njegovog matičnog tijela ili službe;

4. stupanj tajnosti uvjerenja o sigurnosnoj provjeri posjetitelja za pristup klasificiranim podacima;

5. svrhu posjeta i predloženi datum posjeta; te

6. naznaku službi, osoba za kontakt i objekata koji se posjećuju.

Članak 10.
Konzultacije i rješavanje sporova

(1) Ugovorne stranke uzimaju u obzir zakone i propise kojima se uređuje zaštita klasificiranih podataka koji se primjenjuju u državi druge ugovorne stranke.

(2) Kako bi se osigurala bliska suradnja u provedbi ovog Ugovora, nadležna tijela ugovornih stranaka konzultiraju jedno drugo na zahtjev jednoga od tih tijela.

(3) Osim toga, svaka ugovorna stranka odobrava nadležnom sigurnosnom tijelu druge ugovorne stranke ili bilo kojem drugom tijelu određenom međusobnim dogovorom da posjećuje državno područje njezine države kako bi s nadležnim tijelima njezine države razgovaralo o postupcima i objektima za zaštitu klasificiranih podataka primljenih od druge ugovorne stranke. Svaka ugovorna stranka pomaže tom tijelu pri utvrđivanju jesu li takvi klasificirani podaci primljeni od druge ugovorne stranke odgovarajuće zaštićeni. Pojedinosti posjeta utvrđuju nadležna tijela.

(4) Bilo koji spor između ugovornih stranaka koji proizađe iz tumačenja ili primjene ovog Ugovora rješava se isključivo konzultacijama ili pregovorima između ugovornih stranaka i ne podnosi se na rješavanje bilo kojem nacionalnom ili međunarodnom sudu ili trećoj strani.

Članak 11.
Kršenje odredaba kojima se uređuje zaštita klasificiranih podataka

(1) Kada se ne može isključiti neovlašteno ustupanje klasificiranih podataka ili ako se sumnja na takvo ustupanje ili se ono utvrdi, odmah se obavješćuje druga ugovorna stranka, na nacionalnom jeziku tijela koje se obavješćuje ili na engleskom jeziku.

(2) Kršenje odredaba kojima se uređuje zaštita klasificiranih podataka istražuju i odgovarajuće pravne radnje poduzimaju nadležna tijela i nadležni sudovi u državi ugovorne stranke u čijoj je to nadležnosti, u skladu s pravom te države. Na zahtjev, druga ugovorna stranka treba pružiti potporu takvim istragama i nju se obavješćuje o rezultatu.

(3) Kada do kršenja dođe tijekom prijenosa i prije potvrde primitka, nadležno sigurnosno tijelo ugovorne stranke pošiljateljice poduzima odgovarajuće istražne radnje i primjerena pravna sredstva.

Članak 12.
Troškovi

Svaka ugovorna stranka plaća troškove koje prouzroči u provedbi odredaba ovog Ugovora

Članak 13.
Nadležna sigurnosna tijela

Ugovorne stranke pisano obavješćuju jedna drugu o pojedinostima svojih odnosnih nadležnih sigurnosnih tijela odmah nakon što Ugovor stupi na snagu, a po potrebi dostavljaju i dopune tih pojedinosti.

Članak 14.
Odnos s drugim instrumentima, sporazumima i memorandumima o suglasnosti

Ovaj Ugovor ne utječe na bilo koje postojeće instrumente, sporazume i memorandume o suglasnosti između ugovornih stranaka ili nadležnih sigurnosnih tijela o zaštiti klasificiranih podataka u mjeri u kojoj oni nisu u suprotnosti s njegovim odredbama.

Članak 15.
Završne odredbe

(1) Ovaj Ugovor stupa na snagu datumom na koji Vlada Republike Hrvatske obavijesti Vladu Savezne Republike Njemačke da su ispunjeni nacionalni uvjeti za stupanje na snagu. Mjerodavni datum je datum primitka obavijesti.

(2) Ovaj Ugovor sklapa se na neodređeno vrijeme.

(3) Ovaj Ugovor može se pisano izmijeniti i dopuniti uzajamnim dogovorom između ugovornih stranaka. Svaka ugovorna stranka može u svako doba podnijeti pisani zahtjev za izmjenu i dopunu ovog Ugovora. Ako jedna od ugovornih stranaka podnese takav zahtjev, ugovorne stranke započinju pregovore o izmjeni i dopuni Ugovora.

(4) Svaka ugovorna stranka može u svako doba, diplomatskim putem, otkazati ovaj Ugovor pisanom obaviješću šest mjeseci unaprijed. U slučaju otkaza, razmijenjeni klasificirani podaci ili podaci koje je stvorio ugovaratelj na temelju ovog Ugovora nastavljaju se štititi u skladu s odredbama gornjeg članka 4. onoliko dugo koliko je to opravdano postojanjem stupnja tajnosti.

(5) Registraciju ovog Ugovora u Tajništvu Ujedinjenih naroda, u skladu s člankom 102. Povelje Ujedinjenih naroda, pokreće ugovorna stranka u čijoj je državi Ugovor sklopljen odmah nakon njegovog stupanja na snagu. Druga ugovorna stranka obavješćuje se o registraciji i o registracijskom broju UN-a čim to potvrdi Tajništvo Ujedinjenih naroda.

(6) Sporazum između Ministarstva obrane Republike Hrvatske i Saveznog ministarstva obrane Savezne Republike Njemačke o uzajamnoj zaštiti tajnih vojnih podataka potpisan 28. travnja 2003. prestaje biti na snazi datumom stupanja na snagu ovog Ugovora. Po stupanju na snagu ovog Ugovora, razmijenjeni klasificirani vojni podaci ili podaci koje je stvorio ugovaratelj na temelju Sporazuma od 28. travnja 2003. štite se u skladu s odredbama ovog Ugovora onoliko dugo koliko je to opravdano postojanjem stupnja tajnosti.

Sastavljeno u Zagrebu dana 18. travnja 2023. u dva izvornika, na hrvatskom, njemačkom i engleskom jeziku, pri čemu su svi tekstovi vjerodostojni. U slučaju različitih tumačenja hrvatskog i njemačkog teksta, mjerodavan je engleski tekst.

Za Vladu Republike Hrvatske	Za Vladu Savezne Republike Njemačke
mr. sc. Valentino Franjić, v. r. predstojnik Ureda Vijeća za nacionalnu sigurnost	dr. Christian Hellbach, v. r. izvanredni i opunomoćeni veleposlanik Savezne Republike Njemačke u Republici Hrvatskoj

Članak 3.

Provedba ovoga Zakona u djelokrugu je središnjeg državnog tijela 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“.

OBRAZLOŽENJE

Člankom 1. Konačnog prijedloga Zakona utvrđuje se da Hrvatski sabor potvrđuje Ugovor između Vlade Republike Hrvatske i Vlade Savezne Republike Njemačke o razmjeni i 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 središnjeg državnog tijela nadležnog za poslove informacijske sigurnosti.

Člankom 4. utvrđuje se da na dan stupanja na snagu Zakona, Ugovor između Vlade Republike Hrvatske i Vlade Savezne Republike Njemačke o razmjeni i 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, njemačkom i engleskom jeziku**

Ugovor

između

Vlade Republike Hrvatske

i

Vlade Savezne Republike Njemačke

o

razmjeni i uzajamnoj zaštiti klasificiranih podataka

Vlada Republike Hrvatske
i
Vlada Savezne Republike Njemačke,
u daljnjem tekstu „ugovorne stranke“,

u namjeri osiguravanja zaštite klasificiranih podataka koji se razmjenjuju između nadležnih tijela Republike Hrvatske i Savezne Republike Njemačke, kao i s ugovarateljima ili između ugovaratelja dviju ugovornih stranaka,

želeći usuglasiti pravni okvir za razmjenu i uzajamnu zaštitu klasificiranih podataka koji se primjenjuje na sve instrumente o suradnji koji se sklapaju između ugovornih stranaka i na ugovore koji uključuju razmjenu klasificiranih podataka,

sporazumjele su se kako slijedi:

Članak 1.
Definicije

(1) Za potrebe ovog Ugovora

1. „klasificirani podaci“ su

   a) u Republici Hrvatskoj
   bilo koji podaci, neovisno o njihovom obliku, koje treba zaštititi i koji su klasificirani u skladu s nacionalnim zakonima i propisima ili ih je kao takve ustupila druga država, međunarodna organizacija ili institucija s kojom Republika Hrvatska surađuje;

   b) u Saveznoj Republici Njemačkoj
   činjenice, predmeti ili podaci koji, neovisno o obliku u kojem se pojavljuju, u javnom interesu trebaju ostati tajni. Klasificira ih službeno tijelo, ili se klasificiraju na njegov zahtjev, u skladu s njihovom potrebom za zaštitom;

2. „klasificirani ugovor“ je ugovor između tijela ili poduzeća iz države jedne ugovorne stranke (naručitelj) i poduzeća iz države druge ugovorne stranke (ugovaratelj); u skladu s takvim ugovorom, klasificirani podaci iz države naručitelja ustupaju se ugovaratelju, ili ih ugovaratelj stvara, ili ih treba učiniti dostupnima zaposlenicima ugovaratelja koji trebaju obavljati zadaće u objektima naručitelja.

(2) Stupnjevi tajnosti utvrđuju se kako slijedi:

1. U Republici Hrvatskoj klasificirani podaci su

   a) VRLO TAJNO ako bi neovlašteno otkrivanje i pristup neovlaštenih osoba tim podacima nanio nepopravljivu štetu nacionalnoj sigurnosti i vitalnim interesima Republike Hrvatske,

   b) TAJNO ako bi neovlašteno otkrivanje i pristup neovlaštenih osoba tim podacima teško naštetio nacionalnoj sigurnosti i vitalnim interesima Republike Hrvatske,

   c) POVJERLJIVO ako bi neovlašteno otkrivanje i pristup neovlaštenih osoba tim podacima naštetio nacionalnoj sigurnosti i vitalnim interesima Republike Hrvatske,

   d) OGRANIČENO ako bi neovlašteno otkrivanje i pristup neovlaštenih osoba tim podacima naštetio djelovanju državnih tijela.

2. U Saveznoj Republici Njemačkoj klasificirani podaci su

   a) STRENG GEHEIM ako pristup neovlaštenih osoba tim podacima može predstavljati prijetnju za postojanje ili vitalne interese Savezne Republike Njemačke ili jedne od njezinih saveznih pokrajina,

   b) GEHEIM ako pristup neovlaštenih osoba tim podacima može predstavljati prijetnju za sigurnost Savezne Republike Njemačke ili jedne od njezinih saveznih pokrajina, ili može izazvati tešku štetu njihovim interesima,

   c) VS-VERTRAULICH ako pristup neovlaštenih osoba tim podacima može biti štetan za interese Savezne Republike Njemačke ili jedne od njezinih saveznih pokrajina,

   d) VS-NUR FÜR DEN DIENSTGEBRAUCH ako pristup neovlaštenih osoba tim podacima može biti nepovoljan za interese Savezne Republike Njemačke ili jedne od njezinih saveznih pokrajina.

Članak 2.
Stupnjevi tajnosti

Ugovorne stranke utvrđuju da su sljedeći stupnjevi tajnosti istoznačni:

Republika Hrvatska	Savezna Republika Njemačka
VRLO TAJNO	STRENG GEHEIM
TAJNO	GEHEIM
POVJERLJIVO	VS-VERTRAULICH
OGRANIČENO	VS-NUR FÜR DEN DIENSTGEBRAUCH

Članak 3.
Označavanje

(1) Prenesene klasificirane podatke istoznačnim nacionalnim stupnjem tajnosti kako je navedeno u članku 2. dodatno označava nadležno sigurnosno tijelo primatelja ili se označavaju na njegov zahtjev.

(2) Klasificirani podaci koji nastanu u državi ugovorne stranke primateljice u vezi s klasificiranim ugovorima, kao i umnoženi primjerci, izvatci i prijevodi izrađeni u državi ugovorne stranke primateljice, također se označavaju na taj način.

(3) Prijevod nosi odgovarajuću napomenu na jeziku prijevoda da prijevod sadrži klasificirane podatke ugovorne stranke pošiljateljice.

(4) Odluku o promjeni ili ukidanju stupnjeva tajnosti donose isključivo nadležna sigurnosna tijela ugovorne stranke pošiljateljice. Nadležno sigurnosno tijelo ugovorne stranke pošiljateljice odmah obavješćuje nadležno sigurnosno tijelo ugovorne stranke primateljice o promjeni ili ukidanju bilo kojeg stupnja tajnosti. Nadležno sigurnosno tijelo ugovorne stranke primateljice na isti način provodi tu promjenu ili ukidanje.

Članak 4.
Mjere na nacionalnoj razini

(1) U okviru područja primjene svojih odnosnih nacionalnih zakona i propisa, ugovorne stranke poduzimaju sve odgovarajuće mjere kako bi jamčile zaštitu klasificiranih podataka koji nastaju, koji se razmjenjuju ili s kojima se postupa u skladu s odredbama ovog Ugovora. One takvim klasificiranim podacima pružaju stupanj zaštite usporediv s onim koji ugovorna stranka primateljica zahtijeva za svoje vlastite klasificirane podatke istoznačnog stupnja tajnosti.

(2) Klasificirani podaci koriste se isključivo za određenu svrhu. Ugovorna stranka primateljica koristi ili odobrava pristup, ili dopušta korištenje ili odobravanje pristupa bilo kojim klasificiranim podacima isključivo za svrhe i u okviru bilo kojih ograničenja koja je odredila ugovorna stranka pošiljateljica ili koja su određena u njezino ime. Ugovorna stranka pošiljateljica mora dati svoj pisani pristanak za bilo koje drugačije postupanje prije ustupanja klasificiranih podataka.

(3) Pristup klasificiranim podacima može se odobriti isključivo osobama kojima je to nužno za obavljanje poslova iz djelokruga s obzirom na njihove zadaće i - osim u slučaju klasificiranih podataka stupnja tajnosti OGRANIČENO / VS-NUR FÜR DEN DIENSTGEBRAUCH - kojima je izdano uvjerenje o sigurnosnoj provjeri ili na temelju svoje dužnosti imaju pravo pristupa klasificiranim podacima istoznačnog stupnja tajnosti. Uvjerenje o sigurnosnoj provjeri izdaje se tek nakon provođenja sigurnosne provjere po standardima koji su usporedivi s onima koji se primjenjuju za pristup nacionalnim klasificiranim podacima istoznačnog stupnja tajnosti.

(4) Državljaninu države jedne ugovorne stranke pristup klasificiranim podacima stupnja tajnosti POVJERLJIVO / VS-VERTRAULICH ili višeg odobrava se bez prethodnog ovlaštenja ugovorne stranke pošiljateljice.

(5) Uvjerenja o sigurnosnoj provjeri za državljane države ugovorne stranke koji borave i imaju potrebu pristupa klasificiranim podacima u svojoj vlastitoj državi izdaju njihova nadležna sigurnosna tijela.

(6) Članci 6. i 7. ovog Ugovora ne primjenjuju se na klasificirane podatke stupnja tajnosti OGRANIČENO / VS-NUR FÜR DEN DIENSTGEBRAUCH.

(7) Ugovorne stranke, svaka unutar svoje države, osiguravaju provođenje potrebnih sigurnosnih nadzora i pridržavanje ovog Ugovora.

Članak 5.
Uništavanje klasificiranih podataka

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

(2) Klasificirani podaci stupnja tajnosti VRLO TAJNO / STRENG GEHEIM se ne uništavaju. Oni se vraćaju ugovornoj stranci pošiljateljici na zahtjev ili ako određena svrha više ne postoji.

(3) Klasificirani podaci stupnja tajnosti TAJNO / GEHEIM ili POVJERLJIVO / VS-VERTRAULICH mogu se uništiti ako to pisano odobri ugovorna stranka pošiljateljica.

(4) Ugovorna stranka primateljica može uništiti klasificirane podatke stupnja tajnosti OGRANIČENO / VS-NUR FÜR DEN DIENSTGEBRAUCH ako određena svrha više ne postoji.

(5) U kriznoj situaciji u kojoj je nemoguće zaštititi ili vratiti klasificirane podatke razmijenjene ili nastale u skladu s ovim Ugovorom, klasificirani podaci se odmah uništavaju. Ugovorna stranka primateljica što je prije moguće obavješćuje nadležno sigurnosno tijelo ugovorne stranke pošiljateljice o tom uništavanju.

Članak 6.
Sklapanje klasificiranih ugovora

(1) Prije sklapanja klasificiranog ugovora naručitelj, putem svog nadležnog sigurnosnog tijela, pribavlja uvjerenje o sigurnosnoj provjeri pravne osobe od nadležnog sigurnosnog tijela ugovaratelja kako bi dobio potvrdu podliježe li potencijalni ugovaratelj sigurnosnom nadzoru nadležnog sigurnosnog tijela svoje države i je li taj ugovaratelj poduzeo sigurnosne mjere potrebne za provedbu klasificiranog ugovora. U slučaju da ugovaratelj još ne podliježe sigurnosnom nadzoru, može se podnijeti zahtjev u tu svrhu.

(2) Uvjerenje o sigurnosnoj provjeri pravne osobe pribavlja se i ako je od potencijalnog ugovaratelja zatraženo da preda ponudu i ako će klasificirane podatke stupnja tajnosti POVJERLJIVO / VS-VERTRAULICH ili višeg trebati ustupiti prije sklapanja klasificiranog ugovora tijekom natječajnog postupka.

(3) U slučajevima iz gore navedenih stavaka (1) i (2) primjenjuje se sljedeći postupak:

1. Zahtjevi za izdavanje uvjerenja o sigurnosnoj provjeri pravne osobe za ugovaratelje iz države druge ugovorne stranke sadrže podatke o projektu, kao i prirodi, opsegu i stupnju tajnosti klasificiranih podataka za koje se očekuje da će biti ustupljeni ugovaratelju ili da će ih on stvoriti.

2. Osim punog naziva ugovaratelja, njegove poštanske adrese, imena savjetnika za informacijsku sigurnost, njegovog broja telefona i telefaksa te njegove adrese elektroničke pošte, uvjerenja o sigurnosnoj provjeri pravne osobe moraju sadržavati podatke posebice o opsegu u kojem je i stupnju tajnosti do kojeg je odnosni ugovaratelj poduzeo sigurnosne mjere na temelju svojih nacionalnih zakona i propisa.

3. Nadležna sigurnosna tijela ugovornih stranaka obavješćuju jedno drugo o bilo kojim promjenama činjenica na temelju kojih su uvjerenja o sigurnosnoj provjeri pravne osobe izdana.

4. Razmjena takvih obavijesti između nadležnih sigurnosnih tijela ugovornih stranaka obavlja se na nacionalnom jeziku tijela koje se obavješćuje ili na engleskom jeziku.

5. Uvjerenja o sigurnosnoj provjeri pravne osobe i zahtjevi koji se upućuju odnosnim nadležnim sigurnosnim tijelima ugovornih stranaka za izdavanje uvjerenja o sigurnosnoj provjeri pravne osobe prenose se pisano.

Članak 7.
Provedba klasificiranih ugovora

(1) Klasificirani ugovori moraju sadržavati klauzulu o sigurnosnim zahtjevima prema kojoj je ugovaratelj obvezan osigurati uvjete potrebne za zaštitu klasificiranih podataka u skladu s nacionalnim zakonima i propisima svoje države.

(2) Osim toga, klauzula o sigurnosnim zahtjevima sadrži sljedeće odredbe:

1. definiciju pojma „klasificirani podaci" i istoznačnice stupnjeva tajnosti država dviju ugovornih stranaka u skladu s odredbama ovog Ugovora;

2. uvjet da se klasificirani podaci ustupaju trećoj strani, ili da se takvo ustupanje trećoj strani odobrava, isključivo ako je to pisano odobrila ugovorna stranka pošiljateljica;

3. uvjet da ugovaratelj odobrava pristup klasificiranim podacima isključivo osobi kojoj je to nužno za obavljanje poslova iz djelokruga i koja je zadužena za provedbu ili doprinosi provedbi klasificiranog ugovora te joj je - osim u slučaju klasificiranih podataka stupnja tajnosti OGRANIČENO / VS-NUR FÜR DEN DIENSTGEBRAUCH - unaprijed izdano uvjerenje o sigurnosnoj provjeri za odgovarajući stupanj tajnosti;

4. nazive odnosnih nadležnih tijela ugovornih stranaka zaduženih za odobravanje ustupanja klasificiranih podataka u vezi sa sklapanjem klasificiranih ugovora ili ovlaštenih za koordinaciju zaštite takvih klasificiranih podataka;

5. načine prijenosa klasificiranih podataka između nadležnih tijela i uključenih ugovaratelja;

6. postupke i mehanizme obavješćivanja o promjenama koje mogu nastati u vezi s klasificiranim podacima, bilo zbog promjene, bilo zbog ukidanja njihovih stupnjeva tajnosti;

7. postupke odobravanja posjeta objektima, ili pristupa klasificiranim podacima, za zaposlenike ugovaratelja;

8. postupke prijenosa klasificiranih podataka ugovarateljima koji postupaju s takvim klasificiranim podacima; i

9. uvjet da ugovaratelj odmah obavješćuje svoje nadležno tijelo o bilo kojem stvarnom gubitku ili sumnji u gubitak, neovlašteno otkrivanje ili neovlašteno ustupanje klasificiranih podataka obuhvaćenih klasificiranim ugovorom.

(3) Nadležno sigurnosno tijelo naručitelja dostavlja ugovaratelju zasebni popis (naputak o klasificiranju) svih dokumenata kojima je potrebno odrediti stupanj tajnosti, određuje potrebni stupanj tajnosti i osigurava dodavanje tog naputka o klasificiranju kao priloga klasificiranom ugovoru. Također, nadležno sigurnosno tijelo naručitelja dužno je prenijeti, ili pokrenuti prijenos tog naputka o klasificiranju, nadležnom sigurnosnom tijelu ugovaratelja.

(4) Nadležno sigurnosno tijelo naručitelja osigurava da će pristup klasificiranim podacima ugovaratelju biti odobren tek nakon primitka odgovarajućeg uvjerenja o sigurnosnoj provjeri pravne osobe od nadležnog sigurnosnog tijela ugovaratelja.

Članak 8.
Prijenos klasificiranih podataka

(1) Klasificirani podaci stupnja tajnosti VRLO TAJNO / STRENG GEHEIM prenose se između ugovornih stranaka isključivo putem ovlaštenih državnih tijela, u skladu s odnosnim nacionalnim zakonima i propisima.

(2) U načelu, klasificirani podaci stupnjeva tajnosti POVJERLJIVO / VS-VERTRAULICH i TAJNO / GEHEIM prenose se iz jedne države u drugu putem službenog dostavljača. Nadležna sigurnosna tijela ugovornih stranaka mogu dogovoriti druge načine prijenosa. Klasificirani podaci dostavljaju se primatelju u skladu s nacionalnim zakonima i propisima, a primitak klasificiranih podataka potvrđuje nadležno tijelo ili se potvrđuje na njegov zahtjev.

(3) Nadležna sigurnosna tijela ugovornih stranaka mogu dogovoriti - općenito ili uz ograničenja - da se klasificirani podaci stupnjeva tajnosti POVJERLJIVO / VS-VERTRAULICH i TAJNO / GEHEIM mogu prenositi na drugi način osim službenim dostavljačem. U takvim slučajevima,

1. dostavljač mora biti ovlašten za pristup klasificiranim podacima istoznačnog stupnja tajnosti,

2. pošiljatelj mora zadržati popis klasificiranih podataka koji se prenose; primjerak tog popisa predaje se primatelju za dostavu nadležnom tijelu,

3. klasificirani podaci moraju se pakirati u skladu s propisima kojima se uređuje prijevoz unutar državnih granica,

4. klasificirani podaci moraju se dostavljati uz potvrdu primitka, i

5. dostavljač mora imati dostavljačko pismo koje je izdalo nadležno tijelo pošiljatelja.

(4) Kada treba prenositi klasificirane podatke, prijevozno sredstvo, rutu i po potrebi pratnju posebno za svaki slučaj utvrđuju nadležna sigurnosna tijela na temelju detaljnog plana prijevoza.

(5) Kao dodatno alternativno sredstvo prijenosa, klasificirani podaci do i uključujući stupanj tajnosti POVJERLJIVO / VS-VERTRAULICH mogu se prenositi putem privatnih dostavljačkih službi kojima nije izdano uvjerenje o sigurnosnoj provjeri, pod uvjetom da su ispunjeni sljedeći uvjeti:

1. Dostavljačka služba ima svoje sjedište na državnom području jedne od država ugovornih stranaka i ima uspostavljen zaštitni sigurnosni program za postupanje s vrijednim predmetima uz potpis o preuzimanju, uključujući kontinuiranu evidenciju o čuvanju, bilo na temelju evidencije potpisa i tehničkog popisa, bilo putem elektroničkog sustava za praćenje ili traženje.

2. Dostavljačka služba obavezna je na temelju potpisa voditi evidenciju o primitku i dostavi na temelju koje pošiljatelju izdaje potvrdu o dostavi ili je izdaje na temelju popratne dokumentacije koja sadrži registracijski broj pošiljke.

3. Dostavljačka služba mora jamčiti da će pošiljka biti dostavljena primatelju do točno određenog vremena i datuma unutar razdoblja od 24 sata.

4. Dostavljačka služba može angažirati vanjskog suradnika ili podugovaratelja. Međutim, dostavljačka služba odgovorna je za ispunjavanje gore navedenih uvjeta.

(6) Klasificirani podaci stupnja tajnosti VRLO TAJNO / STRENG GEHEIM ne prenose se elektroničkim putem.

(7) Elektronički prijenos klasificiranih podataka stupnjeva tajnosti POVJERLJIVO / VS-VERTRAULICH i TAJNO / GEHEIM moguć je isključivo u kriptiranom obliku. Klasificirani podaci tih stupnjeva tajnosti mogu se kriptirati isključivo sredstvima za kriptiranje koja su međusobnim dogovorom odobrila nadležna sigurnosna tijela ugovornih stranaka.

(8) Klasificirani podaci stupnja tajnosti OGRANIČENO / VS-NUR FÜR DEN DIENSTGEBRAUCH mogu se prenositi putem pošte ili drugih dostavnih službi primateljima

unutar državnog područja države druge ugovorne stranke, uzimajući u obzir nacionalne zakone i propise.

(9) Klasificirani podaci stupnja tajnosti OGRANIČENO / VS-NUR FÜR DEN DIENSTGEBRAUCH mogu se prenositi elektronički ili se pristup tim podacima može omogućiti pomoću komercijalnih uređaja za kriptiranje koje je odobrilo nadležno sigurnosno tijelo ugovorne stranke pošiljatelja. Klasificirani podaci tog stupnja tajnosti mogu se prenositi u nekriptiranom obliku samo ako to nije u suprotnosti s nacionalnim zakonima i propisima, ako nisu dostupna odobrena sredstva za kriptiranje, ako se prijenos odvija samo unutar fiksnih mreža, a pošiljatelj i primatelj su se unaprijed usuglasili o predloženom prijenosu.

Članak 9.
Posjeti

(1) U načelu, posjetiteljima iz države jedne ugovorne stranke pristup klasificiranim podacima te objektima i kojima zaposlenici postupaju s klasificiranim podacima, u državi druge ugovorne stranke, bit će odobren isključivo uz prethodno odobrenje nadležnog sigurnosnog tijela ugovorne stranke čija se država posjećuje. Takvo odobrenje daje se isključivo osobama kojima je to nužno za obavljanje poslova iz djelokruga i koje su - osim u slučaju klasificiranih podataka stupnja tajnosti OGRANIČENO / VS-NUR FÜR DEN DIENSTGEBRAUCH - ovlaštene za pristup klasificiranim podacima.

(2) Zahtjevi za posjet podnose se, pravovremeno i u skladu sa zakonima i propisima države ugovorne stranke na čije državno područje ti posjetitelji žele ući, nadležnom sigurnosnom tijelu te države. Nadležna sigurnosna tijela obavješćuju jedno drugo o pojedinostima u vezi s takvim zahtjevima i osiguravaju zaštitu osobnih podataka.

(3) Zahtjevi za posjete podnose se na jeziku države koju se posjećuje ili na engleskom jeziku i sadrže sljedeće podatke:

1. ime i prezime posjetitelja, datum i mjesto rođenja te broj putovnice ili osobne iskaznice;

2. državljanstvo posjetitelja;

3. naznaku radnog mjesta posjetitelja i naziv njegovog matičnog tijela ili službe;

4. stupanj tajnosti uvjerenja o sigurnosnoj provjeri posjetitelja za pristup klasificiranim podacima;

5. svrhu posjeta i predloženi datum posjeta; te

6. naznaku službi, osoba za kontakt i objekata koji se posjećuju.

Članak 10.
Konzultacije i rješavanje sporova

(1) Ugovorne stranke uzimaju u obzir zakone i propise kojima se uređuje zaštita klasificiranih podataka koji se primjenjuju u državi druge ugovorne stranke.

(2) Kako bi se osigurala bliska suradnja u provedbi ovog Ugovora, nadležna tijela ugovornih stranaka konzultiraju jedno drugo na zahtjev jednoga od tih tijela.

(3) Osim toga, svaka ugovorna stranka odobrava nadležnom sigurnosnom tijelu druge ugovorne stranke ili bilo kojem drugom tijelu određenom međusobnim dogovorom da posjećuje državno područje njezine države kako bi s nadležnim tijelima njezine države razgovaralo o postupcima i objektima za zaštitu klasificiranih podataka primljenih od druge ugovorne stranke. Svaka ugovorna stranka pomaže tom tijelu pri utvrđivanju jesu li takvi klasificirani podaci primljeni od druge ugovorne stranke odgovarajuće zaštićeni. Pojedinosti posjeta utvrđuju nadležna tijela.

(4) Bilo koji spor između ugovornih stranaka koji proizađe iz tumačenja ili primjene ovog Ugovora rješava se isključivo konzultacijama ili pregovorima između ugovornih stranaka i ne podnosi se na rješavanje bilo kojem nacionalnom ili međunarodnom sudu ili trećoj strani.

Članak 11.
Kršenje odredaba kojima se uređuje zaštita klasificiranih podataka

(1) Kada se ne može isključiti neovlašteno ustupanje klasificiranih podataka ili ako se sumnja na takvo ustupanje ili se ono utvrdi, odmah se obavješćuje druga ugovorna stranka, na nacionalnom jeziku tijela koje se obavješćuje ili na engleskom jeziku.

(2) Kršenje odredaba kojima se uređuje zaštita klasificiranih podataka istražuju i odgovarajuće pravne radnje poduzimaju nadležna tijela i nadležni sudovi u državi ugovorne stranke u čijoj je to nadležnosti, u skladu s pravom te države. Na zahtjev, druga ugovorna stranka treba pružiti potporu takvim istragama i nju se obavješćuje o rezultatu.

(3) Kada do kršenja dođe tijekom prijenosa i prije potvrde primitka, nadležno sigurnosno tijelo ugovorne stranke pošiljateljice poduzima odgovarajuće istražne radnje i primjerena pravna sredstva.

Članak 12.
Troškovi

Svaka ugovorna stranka plaća troškove koje prouzroči u provedbi odredaba ovog Ugovora.

Članak 13.
Nadležna sigurnosna tijela

Ugovorne stranke pisano obavješćuju jedna drugu o pojedinostima svojih odnosnih nadležnih sigurnosnih tijela odmah nakon što Ugovor stupi na snagu, a po potrebi dostavljaju i dopune tih pojedinosti.

Članak 14.
Odnos s drugim instrumentima, sporazumima i memorandumima o suglasnosti

Ovaj Ugovor ne utječe na bilo koje postojeće instrumente, sporazume i memorandume o suglasnosti između ugovornih stranaka ili nadležnih sigurnosnih tijela o zaštiti klasificiranih podataka u mjeri u kojoj oni nisu u suprotnosti s njegovim odredbama.

Članak 15.
Završne odredbe

(1) Ovaj Ugovor stupa na snagu datumom na koji Vlada Republike Hrvatske obavijesti Vladu Savezne Republike Njemačke da su ispunjeni nacionalni uvjeti za stupanje na snagu. Mjerodavni datum je datum primitka obavijesti.

(2) Ovaj Ugovor sklapa se na neodređeno vrijeme.

(3) Ovaj Ugovor može se pisano izmijeniti i dopuniti uzajamnim dogovorom između ugovornih stranaka. Svaka ugovorna stranka može u svako doba podnijeti pisani zahtjev za izmjenu i dopunu ovog Ugovora. Ako jedna od ugovornih stranaka podnese takav zahtjev, ugovorne stranke započinju pregovore o izmjeni i dopuni Ugovora.

(4) Svaka ugovorna stranka može u svako doba, diplomatskim putem, otkazati ovaj Ugovor pisanom obaviješću šest mjeseci unaprijed. U slučaju otkaza, razmijenjeni klasificirani podaci ili podaci koje je stvorio ugovaratelj na temelju ovog Ugovora nastavljaju se štititi u skladu s odredbama gornjeg članka 4. onoliko dugo koliko je to opravdano postojanjem stupnja tajnosti.

(5) Registraciju ovog Ugovora u Tajništvu Ujedinjenih naroda, u skladu s člankom 102. Povelje Ujedinjenih naroda, pokreće ugovorna stranka u čijoj je državi Ugovor sklopljen odmah nakon njegovog stupanja na snagu. Druga ugovorna stranka obavješćuje se o registraciji i o registracijskom broju UN-a čim to potvrdi Tajništvo Ujedinjenih naroda.

(6) Sporazum između Ministarstva obrane Republike Hrvatske i Saveznog ministarstva obrane Savezne Republike Njemačke o uzajamnoj zaštiti tajnih vojnih podataka potpisan 28. travnja 2003. prestaje biti na snazi datumom stupanja na snagu ovog Ugovora. Po stupanju na snagu ovog Ugovora, razmijenjeni klasificirani vojni podaci ili podaci koje je stvorio ugovaratelj na temelju Sporazuma od 28. travnja 2003. štite se u skladu s odredbama ovog Ugovora onoliko dugo koliko je to opravdano postojanjem stupnja tajnosti.

Sastavljeno u Zagrebu dana 18. travnja 2023. u dva izvornika, na hrvatskom, njemačkom i engleskom jeziku, pri čemu su svi tekstovi vjerodostojni. U slučaju različitih tumačenja hrvatskog i njemačkog teksta, mjerodavan je engleski tekst.

Za Vladu
Republike Hrvatske

Za Vladu
Savezne Republike Njemačke

Abkommen

zwischen

der Regierung der Republik Kroatien

und

der Regierung der Bundesrepublik Deutschland

über

den Austausch und gegenseitigen Schutz von Verschlusssachen

Die Regierung der Republik Kroatien
und
die Regierung der Bundesrepublik Deutschland,
im Folgenden als „Vertragsparteien" bezeichnet, –

in der Absicht, den Schutz von Verschlusssachen zu gewährleisten, die zwischen den zuständigen Behörden der Republik Kroatien und der Bundesrepublik Deutschland sowie mit Auftragnehmern oder zwischen Auftragnehmern beider Vertragsparteien ausgetauscht werden,

von dem Wunsch geleitet, sich auf einen rechtlichen Rahmen für den Austausch und gegenseitigen Schutz von Verschlusssachen zu einigen, der auf alle zwischen den Vertragsparteien zu schließenden Übereinkünfte über Zusammenarbeit und auf Verträge, die einen Austausch von Verschlusssachen mit sich bringen, Anwendung findet –

sind wie folgt übereingekommen:

Artikel 1
Begriffsbestimmungen

(1) Im Sinne dieses Abkommens

1. sind „Verschlusssachen"

   a) in der Republik Kroatien
   jegliche Informationen, unabhängig von ihrer Form, die schutzbedürftig sind und in Übereinstimmung mit innerstaatlichen Gesetzen und sonstigen Vorschriften als vertraulich eingestuft sind oder die als solche durch andere Staaten, internationale Organisationen oder Institutionen, mit denen die Republik Kroatien zusammenarbeitet, überlassen wurden.

   b) in der Bundesrepublik Deutschland
   im öffentlichen Interesse geheimhaltungsbedürftige Tatsachen, Gegenstände oder Erkenntnisse, unabhängig von ihrer Darstellungsform. Sie werden entsprechend ihrer Schutzbedürftigkeit von einer amtlichen Stelle oder auf deren Veranlassung eingestuft;

2. ist ein „Verschlusssachenauftrag" ein Vertrag zwischen einer Behörde oder einem Unternehmen aus dem Staat der einen Vertragspartei (Auftraggeber) und einem Unternehmen aus dem Staat der anderen Vertragspartei (Auftragnehmer); im Rahmen eines derartigen Vertrags sind Verschlusssachen aus dem Staat des Auftraggebers dem Auftragnehmer zu überlassen, von dem Auftragnehmer zu erstellen oder Mitarbeitern des Auftragnehmers, die Arbeiten in Einrichtungen des Auftraggebers durchzuführen haben, zugänglich zu machen.

(2) Für die Geheimhaltungsgrade gelten die folgenden Begriffsbestimmungen:

1. In der Republik Kroatien sind Verschlusssachen

   a) VRLO TAJNO, wenn deren unbefugte Weitergabe und deren Kenntnisnahme durch Unbefugte einen außerordentlich schweren Schaden für die nationale Sicherheit und die lebenswichtigen Interessen der Republik Kroatien zur Folge haben würden,

   b) TAJNO, wenn deren unbefugte Weitergabe und deren Kenntnisnahme durch Unbefugte einen schweren Schaden für die nationale Sicherheit und die lebenswichtigen Interessen der Republik Kroatien zur Folge haben würden,

   c) POVJERLJIVO, wenn deren unbefugte Weitergabe und deren Kenntnisnahme durch Unbefugte für die nationale Sicherheit und die lebenswichtigen Interessen der Republik Kroatien schädlich sein würden,

   d) OGRANIČENO, wenn deren unbefugte Weitergabe und deren Kenntnisnahme durch Unbefugte schädlich für die Funktion der staatlichen Behörden sein würden.

2. In der Bundesrepublik Deutschland sind Verschlusssachen

   a) STRENG GEHEIM, wenn die Kenntnisnahme durch Unbefugte den Bestand oder lebenswichtige Interessen der Bundesrepublik Deutschland oder eines ihrer Länder gefährden kann,

   b) GEHEIM, wenn die Kenntnisnahme durch Unbefugte die Sicherheit der Bundesrepublik Deutschland oder eines ihrer Länder gefährden oder ihren Interessen schweren Schaden zufügen kann,

   c) VS-VERTRAULICH, wenn die Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder schädlich sein kann,

   d) VS-NUR FÜR DEN DIENSTGEBRAUCH, wenn die Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder nachteilig sein kann.

Artikel 2
Geheimhaltungsgrade

Die Vertragsparteien legen fest, dass folgende Geheimhaltungsgrade gleichwertig sind:

Republik Kroatien	Bundesrepublik Deutschland
VRLO TAJNO	STRENG GEHEIM
TAJNO	GEHEIM
POVJERLJIVO	VS-VERTRAULICH
OGRANIČENO	VS-NUR FÜR DEN DIENSTGEBRAUCH

Artikel 3
Kennzeichnung

(1) Die übermittelten Verschlusssachen werden von der für ihren Empfänger zuständigen Sicherheitsbehörde oder auf deren Veranlassung zusätzlich mit dem nach Artikel 2 vorgesehenen gleichwertigen innerstaatlichen Geheimhaltungsgrad gekennzeichnet.

(2) Eine entsprechende Kennzeichnungspflicht gilt auch für Verschlusssachen, die im Staat der empfangenden Vertragspartei im Zusammenhang mit Verschlusssachenaufträgen erstellt werden, sowie für im Staat der empfangenden Vertragspartei hergestellte Kopien, Auszüge und Übersetzungen.

(3) Die Übersetzung wird mit einem entsprechenden Hinweis in der Sprache, in die übersetzt wurde, versehen, dass die Übersetzung Verschlusssachen der herausgebenden Vertragspartei enthält.

(4) Die Entscheidung über die Änderung oder Aufhebung von Geheimhaltungsgraden bleibt den zuständigen Sicherheitsbehörden der herausgebenden Vertragspartei vorbehalten. Die zuständige Sicherheitsbehörde der herausgebenden Vertragspartei teilt der zuständigen Sicherheitsbehörde der empfangenden Vertragspartei unverzüglich die Änderung oder Aufhebung eines Geheimhaltungsgrads mit. Die zuständige Sicherheitsbehörde der empfangenden Vertragspartei setzt diese Änderung oder Aufhebung entsprechend um.

Artikel 4
Innerstaatliche Maßnahmen

(1) Die Vertragsparteien treffen im Rahmen ihrer jeweiligen innerstaatlichen Gesetze und sonstigen Vorschriften alle geeigneten Maßnahmen, um den Schutz von Verschlusssachen zu gewährleisten, die nach diesem Abkommen erstellt oder ausgetauscht werden oder mit denen nach diesem Abkommen umgegangen wird. Sie gewähren diesen Verschlusssachen den Schutz, der mit demjenigen vergleichbar ist, der von der empfangenden Vertragspartei für eigene Verschlusssachen des gleichwertigen Geheimhaltungsgrads gefordert wird.

(2) Die Verschlusssachen sind ausschließlich für den angegebenen Zweck zu nutzen. Die empfangende Vertragspartei darf Verschlusssachen ausschließlich für die Zwecke und mit den etwaigen Beschränkungen, die von oder im Auftrag der herausgebenden Vertragspartei festgelegt worden sind, nutzen oder den Zugang zu ihnen gewähren beziehungsweise ihre Nutzung oder die Gewährung des Zugangs zu ihnen gestatten. Einer abweichenden Regelung muss die herausgebende Vertragspartei vor der Weitergabe der Verschlusssachen schriftlich zugestimmt haben.

(3) Der Zugang zu Verschlusssachen darf nur Personen gewährt werden, die aufgrund ihrer Aufgaben die Bedingung „Kenntnis nur, wenn nötig" erfüllen und die – außer im Fall von Verschlusssachen des Geheimhaltungsgrads OGRANIČENO / VS-NUR FÜR DEN DIENSTGEBRAUCH – aufgrund einer Sicherheitsüberprüfung zum Zugang zu Verschlusssachen des gleichwertigen Geheimhaltungsgrads ermächtigt oder kraft Amtes dazu befugt sind. Die Ermächtigung setzt den Abschluss einer Sicherheitsüberprüfung voraus, die vergleichbar sein muss mit derjenigen, die für den Zugang zu innerstaatlichen Verschlusssachen des gleichwertigen Geheimhaltungsgrads durchgeführt wird.

(4) Der Zugang zu Verschlusssachen des Geheimhaltungsgrads POVJERLJIVO / VS-VERTRAULICH oder höher durch einen Angehörigen des Staates einer Vertragspartei wird ohne vorherige Genehmigung der herausgebenden Vertragspartei gewährt.

(5) Sicherheitsüberprüfungen bei Angehörigen des Staates einer Vertragspartei, die ihren Aufenthalt im eigenen Staat haben und dort Zugang zu Verschlusssachen benötigen, werden von deren zuständigen Sicherheitsbehörden durchgeführt.

(6) Auf Verschlusssachen des Geheimhaltungsgrads OGRANIČENO / VS-NUR FÜR DEN DIENSTGEBRAUCH finden die Artikel 6 und 7 keine Anwendung.

(7) Jede Vertragspartei stellt innerhalb ihres Staates die Durchführung der erforderlichen Sicherheitsinspektionen und die Einhaltung dieses Abkommens sicher.

Artikel 5
Vernichtung von Verschlusssachen

(1) Verschlusssachen sind so zu vernichten, dass die Möglichkeit ihrer teilweisen oder vollständigen Wiederherstellung ausgeschlossen ist.

(2) Verschlusssachen des Geheimhaltungsgrads VRLO TAJNO / STRENG GEHEIM dürfen nicht vernichtet werden. Sie werden der herausgebenden Vertragspartei auf Ersuchen zurückgegeben oder wenn der angegebene Zweck nicht mehr besteht.

(3) Verschlusssachen des Geheimhaltungsgrads TAJNO / GEHEIM oder POVJERLJIVO / VS-VERTRAULICH können vorbehaltlich der schriftlichen Genehmigung der herausgebenden Vertragspartei vernichtet werden.

(4) Verschlusssachen des Geheimhaltungsgrads OGRANIČENO / VS-NUR FÜR DEN DIENSTGEBRAUCH können durch die empfangende Vertragspartei vernichtet werden, wenn der angegebene Zweck nicht mehr besteht.

(5) Ist es in einer Krisensituation nicht möglich, nach diesem Abkommen ausgetauschte oder erstellte Verschlusssachen zu schützen oder zurückzugeben, so sind diese Verschlusssachen unverzüglich zu vernichten. Die empfangende Vertragspartei informiert die zuständige Sicherheitsbehörde der herausgebenden Vertragspartei so bald wie möglich über diese Vernichtung.

Artikel 6
Vergabe von Verschlusssachenaufträgen

(1) Vor Vergabe eines Verschlusssachenauftrags holt der Auftraggeber über die für ihn zuständige Sicherheitsbehörde bei der für den Auftragnehmer zuständigen Sicherheitsbehörde einen Sicherheitsbescheid ein, um sich vergewissern zu können, ob der in Aussicht genommene Auftragnehmer der Geheimschutzbetreuung durch die zuständige Sicherheitsbehörde seines Staates unterliegt und ob er die für die Durchführung des Verschlusssachenauftrags erforderlichen Geheimschutzvorkehrungen getroffen hat. Unterliegt ein Auftragnehmer noch nicht der Geheimschutzbetreuung, so kann dies beantragt werden.

(2) Ein Sicherheitsbescheid ist auch dann einzuholen, wenn ein möglicher Auftragnehmer zur Abgabe eines Angebots aufgefordert worden ist und im Rahmen des Ausschreibungsverfahrens bereits vor Vergabe eines Verschlusssachenauftrags Verschlusssachen des Geheimhaltungsgrads POVJERLJIVO / VS-VERTRAULICH oder höher überlassen werden müssen.

(3) In den Fällen der Absätze 1 und 2 wird das folgende Verfahren angewendet:

1. Ersuchen um Ausstellung eines Sicherheitsbescheids für Auftragnehmer aus dem Staat der anderen Vertragspartei enthalten Angaben über das Vorhaben sowie die Art, den Umfang und den Geheimhaltungsgrad der dem Auftragnehmer voraussichtlich zu überlassenden oder von ihm zu erstellenden Verschlusssachen.

2. Sicherheitsbescheide müssen neben der vollständigen Bezeichnung des Auftragnehmers, seiner Postanschrift und dem Namen seines Sicherheitsbevollmächtigten sowie dessen Telefon-, Faxverbindung und E-Mail-Adresse insbesondere Angaben darüber enthalten, in welchem Umfang und bis zu welchem Geheimhaltungsgrad von dem betreffenden Auftragnehmer Geheimschutzmaßnahmen auf der Grundlage seiner innerstaatlichen Gesetze und sonstigen Vorschriften getroffen worden sind.

3. Die zuständigen Sicherheitsbehörden der Vertragsparteien teilen es einander mit, wenn sich die den ausgestellten Sicherheitsbescheiden zugrunde liegenden Sachverhalte ändern.

4. Der Austausch dieser Mitteilungen zwischen den zuständigen Sicherheitsbehörden der Vertragsparteien erfolgt in der Landessprache der zu unterrichtenden Behörde oder in englischer Sprache.

5. Sicherheitsbescheide und an die jeweils zuständigen Sicherheitsbehörden der Vertragsparteien gerichtete Ersuchen um Ausstellung von Sicherheitsbescheiden sind schriftlich zu übermitteln.

Artikel 7
Durchführung von Verschlusssachenaufträgen

(1) Verschlusssachenaufträge müssen eine Geheimschutzklausel enthalten, der zufolge der Auftragnehmer verpflichtet ist, die zum Schutz von Verschlusssachen erforderlichen Vorkehrungen in Übereinstimmung mit den innerstaatlichen Gesetzen und sonstigen Vorschriften seines Staates zu treffen.

(2) Außerdem sind folgende Bestimmungen in die Geheimschutzklausel aufzunehmen:

1. die Bestimmung des Begriffs „Verschlusssachen" und der gleichwertigen Geheimhaltungsgrade der Staaten der beiden Vertragsparteien in Übereinstimmung mit diesem Abkommen,

2. das Erfordernis, dass eine Verschlusssache an Dritte nur weitergegeben beziehungsweise deren Weitergabe an Dritte nur gestattet werden darf, wenn die herausgebende Vertragspartei dem schriftlich zugestimmt hat,

3. das Erfordernis, dass der Auftragnehmer den Zugang zu einer Verschlusssache nur einer Person gewähren darf, welche die Bedingung „Kenntnis nur, wenn nötig" erfüllt und mit der Durchführung des Verschlusssachenauftrags beauftragt worden oder daran beteiligt ist und – außer im Fall von Verschlusssachen des Geheimhaltungsgrads OGRANIČENO / VS-NUR FÜR DEN DIENSTGEBRAUCH – zuvor bis zum entsprechenden Geheimhaltungsgrad sicherheitsüberprüft worden ist,

4. die Namen der jeweils zuständigen Behörden der Vertragsparteien, die entweder im Zusammenhang mit der Vergabe von Verschlusssachenaufträgen mit der Genehmigung zur Weitergabe von Verschlusssachen befasst sind oder zur Koordinierung des Schutzes dieser Verschlusssachen ermächtigt sind,

5. die Wege, über die Verschlusssachen zwischen den zuständigen Behörden und beteiligten Auftragnehmern weiterzugeben sind,

6. die Verfahren und Mechanismen für die Mitteilung von Änderungen, die sich möglicherweise in Bezug auf Verschlusssachen aufgrund der Änderung oder Aufhebung ihrer Geheimhaltungsgrade ergeben,

7. die Verfahren für die Genehmigung von Besuchen in Einrichtungen oder des Zugangs zu Verschlusssachen von Personal der Auftragnehmer,

8. die Verfahren für die Übermittlung von Verschlusssachen an Auftragnehmer, die mit solchen Verschlusssachen umgehen, und

9. das Erfordernis, dass der Auftragnehmer die für ihn zuständige Behörde unverzüglich über jeden erfolgten oder vermuteten Verlust, jede tatsächliche oder vermutete Indiskretion und jede tatsächliche oder vermutete unbefugte Weitergabe der unter den Verschlusssachenauftrag fallenden Verschlusssachen zu unterrichten hat.

(3) Die für den Auftraggeber zuständige Sicherheitsbehörde benennt dem Auftragnehmer in einer gesonderten Aufstellung (Einstufungsliste) sämtliche Vorgänge, die einer Verschlusssacheneinstufung bedürfen, legt den erforderlichen Geheimhaltungsgrad fest und veranlasst, dass diese Einstufungsliste dem Verschlusssachenauftrag als Anhang beigefügt wird. Die für den Auftraggeber zuständige Sicherheitsbehörde hat diese Einstufungsliste auch der für den Auftragnehmer zuständigen Sicherheitsbehörde zu übermitteln oder ihre Übermittlung zu veranlassen.

(4) Die für den Auftraggeber zuständige Sicherheitsbehörde stellt sicher, dass dem Auftragnehmer Zugang zu Verschlusssachen erst dann gewährt wird, wenn der entsprechende Sicherheitsbescheid der für den Auftragnehmer zuständigen Sicherheitsbehörde eingegangen ist.

Artikel 8
Übermittlung von Verschlusssachen

(1) Verschlusssachen des Geheimhaltungsgrads VRLO TAJNO / STRENG GEHEIM werden zwischen den Vertragsparteien nur von Regierung zu Regierung in Übereinstimmung mit den jeweiligen innerstaatlichen Gesetzen und sonstigen Vorschriften übermittelt.

(2) Verschlusssachen der Geheimhaltungsgrade POVJERLJIVO / VS-VERTRAULICH und TAJNO / GEHEIM werden von einem Staat in den anderen grundsätzlich auf dem amtlichen Kurierweg übermittelt. Die zuständigen Sicherheitsbehörden der Vertragsparteien können alternative Übermittlungswege vereinbaren. Verschlusssachen werden nach Maßgabe der innerstaatlichen Gesetze und sonstigen Vorschriften an den Empfänger weitergeleitet, und deren Empfang wird von der zuständigen Behörde oder auf deren Veranlassung bestätigt.

(3) Die zuständigen Sicherheitsbehörden der Vertragsparteien können – allgemein oder unter Festlegung von Beschränkungen – vereinbaren, dass Verschlusssachen der Geheimhaltungsgrade POVJERLJIVO / VS-VERTRAULICH und TAJNO / GEHEIM auf einem anderen als dem amtlichen Kurierweg übermittelt werden dürfen. In derartigen Fällen

1. muss der Beförderer zum Zugang zu Verschlusssachen des gleichwertigen Geheimhaltungsgrads ermächtigt sein,

2. muss beim Absender ein Verzeichnis der übermittelten Verschlusssachen verbleiben; ein Exemplar dieses Verzeichnisses ist dem Empfänger zur Weiterleitung an die zuständige Behörde zu übergeben,

3. müssen die Verschlusssachen nach den für den Inlandstransport geltenden Bestimmungen verpackt sein,

4. muss die Übergabe der Verschlusssachen gegen Empfangsbescheinigung erfolgen und

5. muss der Beförderer einen Kurierausweis mit sich führen, den die für den Absender zuständige Behörde ausgestellt hat.

(4) Für die Übermittlung von Verschlusssachen werden Transportmittel, Transportweg und erforderlichenfalls Begleitschutz in jedem Einzelfall durch die zuständigen Sicherheitsbehörden auf der Grundlage eines detaillierten Transportplans festgelegt.

(5) Als zusätzliche alternative Übermittlungsform können Verschlusssachen bis einschließlich Geheimhaltungsgrad POVJERLJIVO / VS-VERTRAULICH durch nicht sicherheitsüberprüfte private Kurierdienste übermittelt werden, sofern die folgenden Bedingungen erfüllt sind:

1. Der Kurierdienst ist im Hoheitsgebiet eines der Staaten der Vertragsparteien ansässig und hat für die Beförderung von Wertgegenständen ein Sicherheitssystem mit Unterschriftenleistung und lückenlosem Nachweis der Verantwortlichkeit für den Gewahrsam mittels eines Quittungs- und Nachweisbuchs oder eines elektronischen Ermittlungs- oder Nachforschungssystems eingerichtet.

2. Der Kurierdienst muss über Annahme und Auslieferung einer Sendung ein Quittungs- und Nachweisbuch führen, anhand dessen er dem Absender einen Auslieferungsbeleg vorlegt, oder der Kurierdienst muss auf einem Frachtbeleg mit Registriernummer den Empfangsnachweis führen.

3. Der Kurierdienst muss gewährleisten, dass die Sendung dem Empfänger innerhalb einer Frist von 24 Stunden bis zu einem bestimmten Datum und Zeitpunkt überbracht wird.

4. Der Kurierdienst kann einen Beauftragten oder Subunternehmer beauftragen. Die Verantwortung für die Einhaltung der genannten Voraussetzungen muss jedoch beim Kurierdienst verbleiben.

(6) Verschlusssachen des Geheimhaltungsgrads VRLO TAJNO / STRENG GEHEIM dürfen nicht auf elektronischem Wege übermittelt werden.

(7) Verschlusssachen der Geheimhaltungsgrade POVJERLJIVO / VS-VERTRAULICH und TAJNO / GEHEIM dürfen auf elektronischem Wege nur verschlüsselt übermittelt werden. Für die Verschlüsselung von Verschlusssachen dieser Geheimhaltungsgrade dürfen nur Verschlüsselungssysteme eingesetzt werden, die von den zuständigen Sicherheitsbehörden der Vertragsparteien in gegenseitigem Einvernehmen zugelassen worden sind.

(8) Verschlusssachen des Geheimhaltungsgrads OGRANIČENO / VS-NUR FÜR DEN DIENSTGEBRAUCH können unter Berücksichtigung der innerstaatlichen Gesetze und sonstigen Vorschriften an Empfänger im Hoheitsgebiet des Staates der anderen Vertragspartei mit der Post oder anderen Zustelldiensten übermittelt werden.

(9) Verschlusssachen des Geheimhaltungsgrads OGRANIČENO / VS-NUR FÜR DEN DIENSTGEBRAUCH können mittels handelsüblicher Verschlüsselungsgeräte, die von einer zuständigen Sicherheitsbehörde der herausgebenden Vertragspartei zugelassen worden sind, elektronisch übermittelt oder zugänglich gemacht werden. Eine unverschlüsselte Übermittlung von Verschlusssachen dieses Geheimhaltungsgrads ist nur zulässig, wenn innerstaatliche Gesetze und sonstige Vorschriften dem nicht entgegenstehen, ein zugelassenes Verschlüsselungssystem nicht verfügbar ist, die Übermittlung ausschließlich innerhalb von Festnetzen erfolgt und Absender und Empfänger sich zuvor über die beabsichtigte Übermittlung geeinigt haben.

Artikel 9
Besuche

(1) Besuchern aus dem Staat einer Vertragspartei wird im Staat der anderen Vertragspartei Zugang zu Verschlusssachen sowie zu Einrichtungen, deren Personal mit Verschlusssachen umgeht, grundsätzlich nur mit vorheriger Erlaubnis der zuständigen Sicherheitsbehörde des Staates, der besucht werden soll, gewährt. Diese Erlaubnis wird nur Personen erteilt, welche die Bedingung „Kenntnis nur, wenn nötig" erfüllen und – außer im Fall von Verschlusssachen des Geheimhaltungsgrads OGRANIČENO / VS-NUR FÜR DEN DIENSTGEBRAUCH – zum Zugang zu Verschlusssachen ermächtigt sind.

(2) Besuchsanmeldungen sind rechtzeitig und in Übereinstimmung mit den Gesetzen und sonstigen Vorschriften des Staates der Vertragspartei, in dessen Hoheitsgebiet die Besucher einzureisen wünschen, der zuständigen Sicherheitsbehörde dieses Staates vorzulegen. Die zuständigen Sicherheitsbehörden teilen einander die Einzelheiten der Anmeldungen mit und stellen den Schutz personenbezogener Daten sicher.

(3) Besuchsanmeldungen sind in der Sprache des zu besuchenden Staates oder in englischer Sprache und mit folgenden Angaben versehen vorzulegen:

1. Vor- und Zuname, Geburtsdatum und -ort sowie die Pass- oder Personalausweisnummer des Besuchers,

2. Staatsangehörigkeit des Besuchers,

3. Dienstbezeichnung des Besuchers und Name der Behörde oder Stelle, die er vertritt,

4. Grad der Ermächtigung des Besuchers für den Zugang zu Verschlusssachen,

5. Besuchszweck sowie vorgesehenes Besuchsdatum und

6. Angabe der Stellen, Ansprechpartner und Einrichtungen, die besucht werden sollen.

Artikel 10
Konsultationen und Beilegung von Streitigkeiten

(1) Die Vertragsparteien nehmen von den im Staat der jeweils anderen Vertragspartei geltenden Gesetzen und sonstigen Vorschriften über den Schutz von Verschlusssachen Kenntnis.

(2) Um eine enge Zusammenarbeit bei der Durchführung dieses Abkommens zu gewährleisten, konsultieren die zuständigen Behörden der Vertragsparteien einander auf Ersuchen einer dieser Behörden.

(3) Jede Vertragspartei gestattet darüber hinaus der zuständigen Sicherheitsbehörde der jeweils anderen Vertragspartei oder jeder im gegenseitigen Einvernehmen bezeichneten anderen Behörde, Besuche im Hoheitsgebiet ihres Staates zu machen, um mit den zuständigen Behörden ihres Staates die Verfahren und Einrichtungen zum Schutz von Verschlusssachen, die ihr von der anderen Vertragspartei zur Verfügung gestellt wurden, zu erörtern. Jede Vertragspartei unterstützt diese Behörde bei der Feststellung, ob die Verschlusssachen, die ihr von der anderen Vertragspartei zur Verfügung gestellt wurden, ausreichend geschützt werden. Die Einzelheiten der Besuche werden von den zuständigen Behörden festgelegt.

(4) Streitigkeiten zwischen den Vertragsparteien, die sich aus der Auslegung oder Anwendung dieses Abkommens ergeben, werden ausschließlich durch Konsultationen oder Verhandlungen zwischen den Vertragsparteien beigelegt und nicht an nationale oder internationale Gerichte oder Dritte zur Beilegung verwiesen.

Artikel 11
Verletzung der Bestimmungen über den Schutz von Verschlusssachen

(1) Wenn eine unbefugte Weitergabe von Verschlusssachen nicht auszuschließen ist, vermutet oder festgestellt wird, ist dies der anderen Vertragspartei unverzüglich entweder in der Landessprache der zu unterrichtenden Behörde oder in englischer Sprache mitzuteilen.

(2) Verletzungen der Bestimmungen über den Schutz von Verschlusssachen werden von den zuständigen Behörden und Gerichten im Staat der Vertragspartei, deren Zuständigkeit gegeben ist, nach dem Recht dieses Staates untersucht und verfolgt. Die andere Vertragspartei soll diese Ermittlungen auf Ersuchen unterstützen und ist über das Ergebnis zu unterrichten.

(3) Ist eine Verletzung während der Übermittlung und vor Bestätigung der Auslieferung eingetreten, so ergreift die zuständige Sicherheitsbehörde der herausgebenden Vertragspartei die zur Untersuchung und Verfolgung geeigneten Maßnahmen.

Artikel 12
Kosten

Jede Vertragspartei trägt die ihr bei der Durchführung dieses Abkommens entstehenden Kosten.

Artikel 13
Zuständige Sicherheitsbehörden

Die Vertragsparteien teilen einander unverzüglich nach Inkrafttreten des Abkommens Einzelheiten ihrer jeweils zuständigen Sicherheitsbehörden schriftlich mit und aktualisieren diese Angaben bei Bedarf.

Artikel 14
Verhältnis zu anderen Übereinkünften, Vereinbarungen und Absprachen

Alle bestehenden Übereinkünfte, Vereinbarungen und Absprachen zwischen den Vertragsparteien oder den zuständigen Sicherheitsbehörden über den Schutz von Verschlusssachen bleiben von diesem Abkommen unberührt, soweit sie ihm nicht entgegenstehen.

Artikel 15
Schlussbestimmungen

(1) Dieses Abkommen tritt an dem Tag in Kraft, an dem die Regierung der Republik Kroatien der Regierung der Bundesrepublik Deutschland notifiziert hat, dass die innerstaatlichen Voraussetzungen für das Inkrafttreten erfüllt sind. Maßgebend ist der Tag des Eingangs der Notifikation.

(2) Dieses Abkommen wird auf unbestimmte Zeit geschlossen.

(3) Dieses Abkommen kann einvernehmlich in Schriftform von den Vertragsparteien geändert werden. Jede Vertragspartei kann jederzeit schriftlich eine Änderung dieses Abkommens beantragen. Stellt eine Vertragspartei einen entsprechenden Antrag, so nehmen die Vertragsparteien Verhandlungen über die Änderung des Abkommens auf.

(4) Jede Vertragspartei kann dieses Abkommen jederzeit unter Einhaltung einer Frist von sechs Monaten auf diplomatischem Wege schriftlich kündigen. Im Fall der Kündigung sind die aufgrund dieses Abkommens übermittelten oder vom Auftragnehmer erstellten Verschlusssachen weiterhin nach Artikel 4 zu behandeln, solange das Bestehen der Verschlusssacheneinstufung dies rechtfertigt.

(5) Die Registrierung dieses Abkommens beim Sekretariat der Vereinten Nationen nach Artikel 102 der Charta der Vereinten Nationen wird unverzüglich nach seinem Inkrafttreten von der Vertragspartei veranlasst, in deren Staat das Abkommen geschlossen wird. Die andere Vertragspartei wird unter Angabe der VN-Registrierungsnummer von der erfolgten Registrierung unterrichtet, sobald diese vom Sekretariat der Vereinten Nationen bestätigt worden ist.

(6) Mit dem Tag des Inkrafttretens dieses Abkommens tritt das am 28. April 2003 unterzeichnete Abkommen zwischen dem Verteidigungsministerium der Republik Kroatien und dem Bundesministerium der Verteidigung der Bundesrepublik Deutschland über den gegenseitigen Schutz von militärischen Verschlusssachen außer Kraft. Mit Inkrafttreten dieses Abkommens sind die aufgrund des Abkommens vom 28. April 2003 übermittelten oder vom Auftragnehmer erstellten militärischen Verschlusssachen in Übereinstimmung mit diesem Abkommen zu behandeln, solange das Bestehen der Verschlusssacheneinstufung dies rechtfertigt.

Geschehen zu Zagreb am 18. April 2023 in zwei Urschriften, jede in kroatischer, deutscher und englischer Sprache, wobei jeder Wortlaut verbindlich ist. Bei unterschiedlicher Auslegung des kroatischen und des deutschen Wortlauts ist der englische Wortlaut maßgebend.

Für die Regierung
der Republik Kroatien

Für die Regierung
der Bundesrepublik Deutschland

Agreement

between

the Government of the Republic of Croatia

and

the Government of the Federal Republic of Germany

on the

Exchange and Mutual Protection of Classified Information

The Government of the Republic of Croatia
and
the Government of the Federal Republic of Germany,
hereinafter referred to as "the Contracting Parties",

Intending to ensure the protection of classified information that is exchanged between the competent authorities of the Republic of Croatia and of the Federal Republic of Germany as well as with contractors or between contractors of the two Contracting Parties,

Desirous of agreeing on a legal framework for the exchange and mutual protection of classified information that shall apply to all instruments on cooperation to be concluded between the Contracting Parties and to contracts involving an exchange of classified information,

Have agreed as follows:

Article 1
Definitions

(1) For the purposes of this Agreement

1. "classified information" is

   a) in the Republic of Croatia
   any information, regardless of its form, which requires protection and has been classified in accordance with national laws and regulations or released as such by another state, international organization or institution that the Republic of Croatia cooperates with;

   b) in the Federal Republic of Germany
   facts, items or intelligence which, regardless of how they are presented, are to be kept secret in the public interest. They shall be classified by, or at the instance of, an official agency in accordance with their need for protection;

2. a "classified contract" is a contract between an authority or an enterprise from the state of one Contracting Party (contract owner) and an enterprise from the state of the other Contracting Party (contractor); under such contract, classified information from the state of the contract owner is to be released to the contractor or is to be generated by the contractor or is to be made accessible to members of the contractor's staff who are to perform tasks in facilities of the contract owner.

(2) The classification levels are defined as follows:

1. In the Republic of Croatia, classified information is

   a) VRLO TAJNO if its unauthorised disclosure and knowledge of it by unauthorised persons would result in exceptionally grave damage to national security and vital interests of the Republic of Croatia,

   b) TAJNO if its unauthorised disclosure and knowledge of it by unauthorised persons would result in grave damage to national security and vital interests of the Republic of Croatia,

   c) POVJERLJIVO if its unauthorised disclosure and knowledge of it by unauthorised persons would be damaging to national security and vital interests of the Republic of Croatia,

   d) OGRANIČENO if its unauthorised disclosure and knowledge of it by unauthorised persons would be damaging to the functioning of state authorities.

2. In the Federal Republic of Germany, classified information is

   a) STRENG GEHEIM if knowledge of it by unauthorised persons may pose a threat to the existence or vital interests of the Federal Republic of Germany or one of its *Länder* (federal states),

   b) GEHEIM if knowledge of it by unauthorised persons may pose a threat to the security of the Federal Republic of Germany or one of its *Länder* (federal states), or may cause severe damage to their interests,

   c) VS-VERTRAULICH if knowledge of it by unauthorised persons may be damaging to the interests of the Federal Republic of Germany or one of its *Länder* (federal states),

   d) VS-NUR FÜR DEN DIENSTGEBRAUCH if knowledge of it by unauthorised persons may be disadvantageous to the interests of the Federal Republic of Germany or one of its *Länder* (federal states).

Article 2
Classification Levels

The Contracting Parties stipulate that the following classification levels are equivalent:

Republic of Croatia	Federal Republic of Germany
VRLO TAJNO	STRENG GEHEIM
TAJNO	GEHEIM
POVJERLJIVO	VS-VERTRAULICH
OGRANIČENO	VS-NUR FÜR DEN DIENSTGEBRAUCH

Article 3
Marking

(1) Transmitted classified information shall be marked additionally with the equivalent national classification level as provided under Article 2 by, or at the instance of, the competent security authority of the recipient.

(2) Classified information which is generated in the state of the receiving Contracting Party in connection with classified contracts as well as copies, excerpts and translations made in the state of the receiving Contracting Party shall also be marked accordingly.

(3) The translation shall bear an appropriate note in the language into which it is translated that the translation contains classified information of the originating Contracting Party.

(4) The decision on the amendment or revocation of classification levels shall be taken only by the competent security authorities of the originating Contracting Party. The competent security authority of the originating Contracting Party shall inform the competent security authority of the receiving Contracting Party immediately of the amendment or revocation of any classification level. The competent security authority of the receiving Contracting Party shall implement this amendment or revocation accordingly.

Article 4
Measures at the National Level

(1) Within the scope of their respective national laws and regulations, the Contracting Parties shall take all appropriate measures to guarantee the protection of classified information generated, exchanged or handled under the terms of this Agreement. They shall afford such classified information a degree of protection comparable to that required by the receiving Contracting Party for its own classified information of the equivalent classification level.

(2) The classified information shall be used solely for the designated purpose. The receiving Contracting Party shall use or grant access, or shall permit the use or granting of access of any classified information only for the purposes and within any limitations stated by or on behalf of the originating Contracting Party. The originating Contracting Party must have given its written consent to any alternative arrangement prior to disclosure of the classified information.

(3) Access to classified information may be granted only to persons having a need-to-know on account of their duties and – except in the case of classified information at the OGRANIČENO / VS-NUR FÜR DEN DIENSTGEBRAUCH level – having been security-cleared or by virtue of their function being entitled to have access to classified information of the equivalent classification level. A security clearance shall be granted only after completion of a security screening under standards comparable to those applied for access to national classified information of the equivalent classification level.

(4) Access to classified information at the POVJERLJIVO / VS-VERTRAULICH level or higher by a national of the state of one Contracting Party shall be granted without the prior authorisation of the originating Contracting Party.

(5) Personnel Security Clearances for nationals of the state of a Contracting Party who reside and require access to classified information in their own state shall be conducted by their competent security authorities.

(6) Articles 6 and 7 of this Agreement shall not apply to classified information at the OGRANIČENO / VS-NUR FÜR DEN DIENSTGEBRAUCH level.

(7) The Contracting Parties shall, each within their state, ensure that the necessary security inspections are carried out and that this Agreement is complied with.

Article 5
Destruction of Classified Information

(1) Classified information shall be destroyed in a way which eliminates the possibility of its partial or total reconstruction.

(2) Classified information at the VRLO TAJNO / STRENG GEHEIM level shall not be destroyed. It shall be returned to the originating Contracting Party upon request or if the designated purpose has ceased to exist.

(3) Classified information at the TAJNO / GEHEIM or POVJERLJIVO / VS-VERTRAULICH level may be destroyed subject to the approval of the originating Contracting Party in writing.

(4) Classified information at the OGRANIČENO / VS-NUR FÜR DEN DIENSTGEBRAUCH level may be destroyed by the receiving Contracting Party if the designated purpose has ceased to exist.

(5) 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 Contracting Party shall inform the competent security authority of the originating Contracting Party about this destruction as soon as possible.

Article 6
Award of Classified Contracts

(1) Prior to the award of a classified contract, the contract owner shall, through its competent security authority, obtain a Facility Security Clearance from the competent security authority of the contractor in order to obtain assurance as to whether the prospective contractor is subject to security oversight by the competent security authority of its state and whether such contractor has taken the security precautions required for discharging the performance of the classified contract. Where a contractor is not yet subject to security oversight, an application may be made to that end.

(2) A Facility Security Clearance shall also be obtained if a potential contractor has been requested to submit a bid and if classified information of the POVJERLJIVO / VS-VERTRAULICH level or higher will have to be released prior to the award of a classified contract under the bid procedure.

(3) In the cases referred to in paragraphs (1) and (2) above, the following procedure shall be applied:

1. Requests for the issuance of a Facility Security Clearance for contractors from the state of the other Contracting Party shall contain information on the project as well as the nature, the scope and the classification level of the classified information expected to be released to the contractor or to be generated by it.

2. In addition to the full name of the contractor, its postal address, the name of its security official, his telephone and fax number and his e-mail address, Facility Security Clearances must include information in particular on the extent to which, and the classification level up to which security measures have been taken by the respective contractor on the basis of its national laws and regulations.

3. The competent security authorities of the Contracting Parties shall inform each other of any changes in the facts on the basis of which Facility Security Clearances have been issued.

4. The exchange of such information between the competent security authorities of the Contracting Parties shall be effected either in the national language of the authority to be informed or in English.

5. Facility Security Clearances and requests addressed to the respective competent security authorities of the Contracting Parties for the issuance of Facility Security Clearances shall be transmitted in writing.

Article 7
Performance of Classified Contracts

(1) Classified contracts must contain a security requirements clause under which the contractor is under an obligation to make the arrangements required for the protection of classified information pursuant to the national laws and regulations of its state.

(2) In addition, the security requirements clause shall contain the following provisions:

1. the definition of the term "classified information" and of the equivalent classification levels of the states of the two Contracting Parties in accordance with the provisions of this Agreement;

2. the requirement that classified information shall only be disclosed to a third party, or that such disclosure to a third party shall only be permitted, if this has been approved by the originating Contracting Party in writing;

3. the requirement that the contractor shall grant access to classified information only to a person who has a need-to-know and has been charged with, or contributes to, the performance of the classified contract and – except in the case of classified information at the OGRANIČENO / VS-NUR FÜR DEN DIENSTGEBRAUCH level – has been security-cleared to the appropriate classification level in advance;

4. the names of the respective competent authorities of the Contracting Parties in charge of authorising the release of classified information in connection with the award of classified contracts or entitled to coordinate the safeguarding of such classified information;

5. the channels to be used for the transfer of classified information between the competent authorities and contractors involved;

6. the procedures and mechanisms for communicating changes that may arise in respect of classified information either because of the amendment or revocation of its classification levels;

7. the procedures for the approval of visits to facilities, or access to classified information, by personnel of the contractors;

8. the procedures for transmitting classified information to contractors handling such classified information; and

9. the requirement that the contractor shall immediately notify its competent authority of any actual or suspected loss, leak or unauthorised disclosure of the classified information covered by the classified contract.

(3) The competent security authority of the contract owner shall provide the contractor with a separate list (classification guide) of all documentary records requiring security classification, shall determine the required classification level and shall arrange for this classification guide to be enclosed as an appendix to the classified contract. The competent security authority of the contract owner shall also transmit, or arrange for the transmission of, this classification guide to the competent security authority of the contractor.

(4) The competent security authority of the contract owner shall ensure that the contractor will be granted access to classified information only after the pertinent Facility Security Clearance has been received from the competent security authority of the contractor.

Article 8
Transmission of Classified Information

(1) Classified information at the VRLO TAJNO / STRENG GEHEIM level shall only be transmitted between the Contracting Parties through Government-to-Government channels in accordance with the respective national laws and regulations.

(2) As a matter of principle, classified information at the POVJERLJIVO / VS-VERTRAULICH and TAJNO / GEHEIM levels shall be transmitted from one state to another by official courier. The competent security authorities of the Contracting Parties may agree on alternative channels of transmission. Classified information shall be forwarded to the recipient in accordance with national laws and regulations, and receipt of classified information shall be confirmed by, or at the instance of, the competent authority.

(3) The competent security authorities of the Contracting Parties may agree – generally or subject to restrictions – that classified information at the POVJERLJIVO / VS-VERTRAULICH and TAJNO / GEHEIM levels may be transmitted through channels other than official courier. In such cases,

1. the bearer must be authorised to have access to classified information of the equivalent classification level,

2. a list of the items of classified information transmitted must be retained by the sender; a copy of this list shall be handed over to the recipient for forwarding to the competent authority,

3. items of classified information must be packed in accordance with the regulations governing transportation within national boundaries,

4. items of classified information must be delivered against receipt, and

5. the bearer must carry a courier certificate issued by the competent authority of the sender.

(4) Where classified information has to be transmitted, the means of transportation, the route, and in case of need an escort shall be determined on a case-by-case basis by the competent security authorities on the basis of a detailed transport plan.

(5) As an additional alternative means of transmission, classified information up to and including the POVJERLJIVO / VS-VERTRAULICH level can be transmitted through non-cleared private courier services provided that the following conditions are met:

1. The courier service is located within the territory of one of the states of the Contracting Parties and has established a protective security programme for handling valuable items with a signature service, including a record of continuous accountability on custody through either a signature and tally record, or an electronic tracking or tracing system.

2. The courier service must obtain and provide proof of delivery on the signature and tally record to the sender, or it must obtain receipts against package numbers.

3. The courier service must guarantee that the consignment will be delivered to the recipient by a specific time and date within a 24-hour period.

4. The courier service may charge a commissioner or sub-contractor. However, the responsibility for fulfilling the above requirements must remain with the courier service.

(6) Classified information at the VRLO TAJNO / STRENG GEHEIM level shall not be transmitted electronically.

(7) Classified information at the POVJERLJIVO / VS-VERTRAULICH and TAJNO / GEHEIM levels may be transmitted electronically in encrypted form only. Classified information of these classification levels may only be encrypted by encryption means approved by mutual agreement by the competent security authorities of the Contracting Parties.

(8) Classified information at the OGRANIČENO / VS-NUR FÜR DEN DIENSTGEBRAUCH level may be transmitted by post or other delivery services to recipients within the territory of the state of the other Contracting Party, taking into account national laws and regulations.

(9) Classified information at the OGRANIČENO / VS-NUR FÜR DEN DIENSTGEBRAUCH level may be transmitted electronically or made accessible by means of commercial encryption devices approved by a competent security authority of the originating Contracting Party. Classified information of this classification level may only be transmitted in an unencrypted form if this is not contrary to national laws and regulations, no approved encryption means are available, transmission is effected within fixed networks only and the sender and the recipient have reached agreement on the proposed transmission in advance.

Article 9
Visits

(1) As a matter of principle, it is only with the prior permission of the competent security authority of the Contracting Party whose state is to be visited that visitors from the state of one Contracting Party will, in the state of the other Contracting Party, be granted access to classified information and to facilities whose personnel handles classified information. Such permission shall be given only to persons having a need-to-know and – except in the case of classified information at the OGRANIČENO / VS-NUR FÜR DEN DIENSTGEBRAUCH level – having been authorised to have access to classified information.

(2) Requests for visits shall be submitted, on a timely basis and in accordance with the laws and regulations of the Contracting Party's state whose territory such visitors wish to enter, to the competent security authority of that state. The competent security authorities shall inform each other of the details regarding such requests and shall ensure that personal data are protected.

(3) Requests for visits shall be submitted in the language of the state to be visited or in English and shall contain the following information:

1. the visitor's first name and surname, date and place of birth, and his passport or identity card number;

2. the visitor's citizenship;

3. the visitor's service designation, and the name of his parent authority or agency;

4. the level of the visitor's security clearance for access to classified information;

5. the purpose of the visit, and the proposed date of the visit; and

6. the designation of the agencies, the contact persons and the facilities to be visited.

Article 10
Consultations and Settlement of Disputes

(1) The Contracting Parties shall take note of the laws and regulations governing the protection of classified information that apply within the state of the other Contracting Party.

(2) To ensure close cooperation in the implementation of this Agreement, the competent authorities of the Contracting Parties shall consult each other at the request of one of these authorities.

(3) Each Contracting Party shall, in addition, allow the competent security authority of the other Contracting Party or any other authority designated by mutual agreement to visit the territory of its state in order to discuss, with the competent authorities of its state, the procedures and facilities for the protection of classified information received from the other Contracting Party. Each Contracting Party shall assist that authority in ascertaining whether such classified information received from the other Contracting Party is adequately protected. The details of the visits shall be laid down by the competent authorities.

(4) Any dispute between the Contracting Parties arising from the interpretation or application of this Agreement shall be resolved solely by consultations or negotiations between the Contracting Parties and shall not be referred to any national or international tribunal or third party for settlement.

Article 11
Violation of Provisions Governing the Protection of Classified Information

(1) Whenever unauthorised disclosure of classified information cannot be ruled out or if such disclosure is suspected or ascertained, the other Contracting Party shall immediately be informed either in the national language of the authority to be informed or in English.

(2) Violations of provisions governing the protection of classified information shall be investigated, and pertinent legal action shall be taken, by the competent authorities and courts in the state of the Contracting Party having jurisdiction, according to the law of that state. The other Contracting Party should, if so requested, support such investigations and shall be informed of the outcome.

(3) When a violation has occurred during transmission and before the delivery has been confirmed, the competent security authority of the originating Contracting Party shall take the appropriate actions to investigate and take pertinent legal action.

Article 12
Costs

Each Contracting Party shall pay the expenses incurred by it in implementing the provisions of this Agreement.

Article 13
Competent Security Authorities

The Contracting Parties shall inform each other in writing about the details of their respective competent security authorities immediately after the Agreement has entered into force and shall also provide updates to these details as necessary.

Article 14
Relationship with Other Instruments, Agreements and Memoranda of Understanding

Any existing instruments, agreements and memoranda of understanding between the Contracting Parties or the competent security authorities on the protection of classified information shall be unaffected by this Agreement in so far as they do not conflict with its provisions.

Article 15
Final Provisions

(1) This Agreement shall enter into force on the date on which the Government of the Republic of Croatia has notified the Government of the Federal Republic of Germany that the national requirements for the entry into force have been fulfilled. The relevant date shall be the date of receipt of the notification.

(2) This Agreement is concluded for an indefinite period of time.

(3) This Agreement may be amended in writing by mutual agreement between the Contracting Parties. Either Contracting Party may at any time submit a written request for the amendment of this Agreement. If such a request is submitted by one of the Contracting Parties, the Contracting Parties shall initiate negotiations on the amendment of the Agreement.

(4) Either Contracting Party may at any time, through diplomatic channels, denounce this Agreement by giving six months' written notice. In the event of denunciation, classified information transmitted, or generated by the contractor, on the basis of this Agreement shall continue to be treated in accordance with the provisions of Article 4 above for as long as is justified by the existence of the security classification.

(5) Registration of this Agreement with the Secretariat of the United Nations, in accordance with Article 102 of the Charter of the United Nations, shall be initiated by the Contracting Party in the state of which the Agreement is concluded immediately following its entry into force. The other Contracting Party shall be informed of registration, and of the UN registration number, as soon as this has been confirmed by the Secretariat of the United Nations.

(6) The Agreement between the Ministry of Defence of the Republic of Croatia and the Federal Ministry of Defence of the Federal Republic of Germany concerning the Mutual Protection of Classified Military Information signed on 28 April 2003 shall cease to have effect upon the date of entry into force of this Agreement. Upon the entry into force of this Agreement, classified military information transmitted, or generated by the contractor, on the basis of the Agreement of 28 April 2003 shall be treated in accordance with the provisions of this Agreement for as long as is justified by the existence of the security classification.

Done at Zagreb on 18th April 2023 in two originals in the Croatian, German and English languages, all texts being authentic. In case of divergent interpretations of the Croatian and German texts, the English text shall prevail.

For the Government of
the Republic of Croatia

For the Government of
the Federal Republic of Germany