

**СПОРАЗУМ
ИЗМЕЂУ
РЕПУБЛИКЕ СРБИЈЕ
И
ЧЕШКЕ РЕПУБЛИКЕ
О РАЗМЕНИ И УЗАЈАМНОЈ ЗАШТИТИ ТАЈНИХ ПОДАТАКА**

Република Србија и Чешка Република, (у даљем тексту: Стране),

у жељи да осигурају заштиту тајних података које међусобно размењују, односно које размењују правна или физичка лица у њиховој надлежности и уз узајамно поштовање националних интереса и безбедности,

споразумеле су се о следећем:

Члан 1. Предмет споразума

1. Предмет овог споразума јесте да обезбеди заштиту тајних података који се размењују или стварају у сарадњи између Страна, односно правних или физичких лица у њиховој надлежности.
2. Овај споразум се односи на сваки уговор или договор, као и на сваку другу сарадњу која укључује размену тајних података између Страна, односно правних или физичких лица у њиховој надлежности.
3. Службе безбедности Страна размењују тајне податке непосредно.

Члан 2. Дефиниције

У сврху овог споразума наведени термини имају следеће значење:

„**Тајни подаци**” су сви подаци који, независно од форме у којој се налазе, захтевају заштиту од неовлашћеног откривања, противправног присвајања или губитка, у складу с националним законодавством сваке Стране и који су означени као такви.

„**Уговор с тајним подацима**” је уговор који садржи или подразумева приступ тајним подацима.

„**Страна порекла**” је Страна, односно правно или физичко лице у њеној надлежности која уступа тајне податке.

„**Страна прималац**” је Страна, односно правно или физичко лице у њеној надлежности која прима тајне податке.

„**Трећа страна**” је свака држава, као и правно или физичко лице у њеној надлежности, односно међународна организација која није Страна у овом споразуму.

Члан 3.
Органи надлежни за заштиту тајних података

1. Органи надлежни за заштиту тајних података и примену овог споразума су:

у Републици Србији:

Канцеларија Савета за националну безбедност и заштиту тајних података.

у Чешкој Републици:

Канцеларија за националну безбедност (Narodni bezpečnostni urad).

2. Органи надлежни за заштиту тајних података доставиће један другом све службене информације за контакт и називе других државних органа који су надлежни за заштиту тајних података и примену овог споразума.

Члан 4.
Степени тајности

Еквивалентни степени тајности су:

У Републици Србији	У Чешкој Републици
ДРЖАВНА ТАЈНА/ DRŽAVNA TAJNA	PŘÍSNĚ TAJNÉ
СТРОГО ПОВЕРЉИВО/ STROGO POVERLJIVO	TAJNÉ
ПОВЕРЉИВО/ POVERLJIVO	TAJNÉ DŮVĚRNÉ
ИНТЕРНО/ INTERNO	VYHRAZENÉ

Члан 5.
Приступ тајним подацима

Приступ тајним подацима који се уступају према овом споразуму могу имати само физичка лица која су за то овлашћена, у складу с националним законодавством сваке од Страна.

Члан 6. Принципи безбедности

1. Страна порекла дужна је:

а) да обезбеди да тајни подаци буду означени одговарајућим ознакама степена тајности у складу с њеним националним законодавством,

б) да обавести Страну примаоца о свим условима под којима уступа тајне податке,

ц) да обавести Страну примаоца о свим накнадним изменама степена тајности или укидању степена тајности.

2. Страна прималац дужна је:

а) да обезбеди да сви тајни подаци буду означени еквивалентним степеном тајности у складу са чланом 4. овог споразума,

б) да омогући исти степен заштите за примљене тајне податке као за националне тајне податке еквивалентног степена тајности,

ц) да обезбеди да ознаке степена тајности примљених тајних података не могу бити укинута или промењена без претходног писменог одобрења Стране порекла,

д) да осигура да тајни подаци не могу бити уступљени трећој страни без претходног писменог одобрења Стране порекла,

е) да користи тајне податке само у сврху за коју су уступљени и у складу са захтевима за руковање тим подацима које је поставила Страна порекла.

Члан 7. Безбедносна сарадња

1. Да би се примењивали слични стандарди безбедности, орган надлежан за заштиту тајних података дужан је да обавести други орган надлежан за заштиту тајних података који му је упутио захтев, о свом националном законодавству које се односи на заштиту тајних података и праксама које проистичу из њихове примене.

2. Орган надлежан за заштиту тајних података дужан је да, у складу са својим националним законодавством, пружи помоћ другом органу надлежном за заштиту тајних података који му је упутио захтев током спровођења процедура за издавање безбедносних сертификата за физичка и правна лица.

3. Стране узајамно признају безбедносне сертификате за физичка и правна лица у складу са својим националним законодавством.

4. Орган надлежан за заштиту тајних података дужан је да одмах обавести други орган надлежан за заштиту тајних података о свим изменама у вези са признатим безбедносним сертификатима за физичка и правна лица, посебно ако су ти сертификати опозвани или ако су престали да важе.

5. Сарадња у складу са овим споразумом врши се на енглеском језику.

6. Орган надлежан за заштиту тајних података обавештава други орган надлежан за заштиту тајних података о безбедносним ризицима који могу угрозити размењене тајне податке.

Члан 8.

Уговори с тајним подацима

1. Орган надлежан за заштиту тајних података дужан је да другом органу за заштиту тајних података који му је упутио захтев потврди да предложени уговарачи-извршиоци посла, као и физичка лица која учествују у преговорима за закључење уговора с тајним подацима, односно у примени уговора с тајним подацима имају безбедносни сертификат за физичка, односно правна лица.

2. Орган надлежан за заштиту тајних података може да захтева да се спроведе безбедносна инспекција правног лица које се налази на територији друге Стране, да би се обезбедила стална усаглашеност са националним законодавством своје Стране којим се уређује област заштите тајних података.

3. Уговори с тајним подацима садрже безбедносни анекс и програмска безбедносна упутства у вези са применом безбедносних захтева и степеном тајности сваког елемента уговора с тајним подацима. Један примерак програмских упутства за безбедност доставља се органу надлежном за заштиту тајних података Стране у чијој надлежности је примена уговора с тајним подацима.

Члан 9.

Пренос тајних података

1. Тајни подаци се преносе у складу са националним законодавством Стране порекла дипломатским путем или другим путем о коме се договоре органи надлежни за заштиту тајних података.

2. Стране могу преносити тајне податке електронским путем у складу с безбедносним процедурама које су одобрили органи надлежни за заштиту тајних података.

Члан 10.

Умножавање, превођење и уништавање тајних података

1. Умножени примерци и преводи тајних података носе одговарајућу ознаку степена тајности и заштићени су као оригинални тајни подаци. Број умножених примерака не сме бити већи од неопходног минимума.

2. На преводе се ставља напомена на језику превода да они садрже тајне податке Стране порекла.

3. Тајни подаци са ознаком тајности ДРЖАВНА ТАЈНА/PŘÍSNĚ TAJNÉ преводе се или умножавају само уз претходно писмено одобрење Стране порекла.

4. Тајни подаци са ознаком тајности ДРЖАВНА ТАЈНА/PŘÍSNĚ TAJNÉ не уништавају се, већ се враћају Страни порекла.

Члан 11.

Посете

1. За посете које захтевају приступ тајним подацима потребно је писмено одобрење органа надлежног за заштиту тајних података, осим ако се органи надлежни за заштиту тајних података о томе другачије не договоре.

2. Најмање двадесет дана пре датума започињања посете, посетилац подноси захтев за посету свом органу надлежном за заштиту тајних података који тај захтев прослеђује органу надлежном за заштиту тајних података друге Стране. У хитним случајевима, захтев за посету може да се поднесе у краћем року, зависно од претходно постигнуте координације између органа надлежних за заштиту тајних података.

3. Захтев за посету садржи:

- а) име и презиме посетиоца, датум и место рођења, држављанство, број пасоша/личне карте;
- б) функцију посетиоца и ближи опис правног лица које тај посетилац представља;
- ц) степен тајности безбедносног сертификата посетиоца и његово важење;
- д) датум и трајање посете, а у случају учесталих посета треба навести укупан период који ће бити обухваћен тим посетама;
- е) сврху посете, укључујући највиши степен тајних података с којима ће се радити;
- ф) назив, адресу, број телефона/факса, имејл и лице за контакт правног лица које је предмет посете;
- г) датум, потпис и службени печат органа надлежног за заштиту тајних података.

4. Органи надлежни за заштиту тајних података могу се договорити да утврде списак посетилаца којима су одобрене чешће посете, као и о појединостима тих посета.

5. Тајни подаци које посетилац прибави током своје посете сматраће се тајним подацима који су уступљени у складу са овим споразумом.

Члан 12. Нарушавање безбедности

1. Органи надлежни за заштиту тајних података су обавезни да одмах писмено обавесте један другог о сваком нарушавању безбедности које за последицу има губитак, противправно присвајање или неовлашћено откривање тајних података или о сумњи да је до тога дошло.

2. Надлежни безбедносни органи Стране примаоца дужни су да одмах спроведу истрагу о том инциденту. Надлежни безбедносни органи Стране порекла су дужни да, на захтев, сарађују у тој истрази.

3. Страна пријема је дужна да писменим путем обавести Страну порекла о околностима нарушавања безбедности тајних података, обиму штете, донетим мерама за њено смањење и о резултату истраге.

Члан 13. Трошкови

Свака Страна сноси свој део трошкова који настану током примене овог споразума.

Члан 14. Тумачење и спорови

Сваки спор у вези са тумачењем или применом овом споразума решава се преговорима између Страна и не упућује се на решавање домаћем или међународном суду.

Члан 15. Административни уговори

Органи надлежни за заштиту тајних података могу ради примене овог споразума да закључе административне уговоре.

Члан 16.
Завршне одредбе

1. Овај споразум се закључује на неодређено време и ступа на снагу првог дана другог месеца након датума када је примљено последње обавештење достављеног дипломатским путем у коме се наводи да су окончане унутрашње правне процедуре за ступање на снагу овог споразума.

2. Овај споразум може бити измењен и допуњен на основу узајамне сагласности Страна. Све измене и допуне ступају на снагу у складу са ставом 1. овог члана.

3. Страна има право да у сваком тренутку писменим путем откаже овај споразум и у том случају он престаје да важи шест месеци од дана када друга Страна прими писмено обавештење о отказу.

4. Без обзира на отказ споразума, тајни подаци који су уступљени или створени на основу овог споразума биће заштићени у складу са његовим одредбама, док Страна порекла не ослободи Страну примаоца те обавезе.

5. Потврђујући горе наведено, овај споразум су потписали прописно овлашћени представници својих влада.

Сачињено у Београду, дана 13. маја 2013. године у по два оригинала на српском, чешком и енглеском језику, при чему су сви текстови подједнако веродостојни. У случају различитог тумачења, меродаван је текст Споразума на енглеском језику.

За Републику Србију	За Чешку Републику
 <p style="text-align: center;">др Горан Матић директор Канцеларија Савета за националну безбедност и заштиту тајних података</p>	 <p style="text-align: center;">Душан Навратил директор Канцеларија за националну безбедност</p>

**AGREEMENT
BETWEEN
THE REPUBLIC OF SERBIA
AND
THE CZECH REPUBLIC
ON THE EXCHANGE AND MUTUAL PROTECTION
OF CLASSIFIED INFORMATION**

The Republic of Serbia and the Czech Republic, hereinafter referred to as „the Parties”,

Wishing to ensure the protection of Classified Information exchanged between them or between legal entities or individuals under their jurisdiction have, in mutual respect for national interests and security agreed upon the following:

Article 1 Scope of the Agreement

1. The objective of this Agreement is to ensure the protection of Classified Information exchanged or generated in the course of co-operation between the Parties or between legal entities or individuals under their jurisdiction.
2. This Agreement shall be applied to any contract or agreement as well as any other co-operation between the Parties or between legal entities or individuals under their jurisdiction involving Classified Information.
3. The intelligence services of the Parties shall exchange Classified Information directly.

Article 2 Definitions

For the purpose of this Agreement:

„**Classified Information**” means any information that, regardless of its form, under the national laws and regulations of either Party, requires protection against unauthorised disclosure, misappropriation or loss, and has been designated as such.

„**Classified Contract**” means a contract that contains or involves access to Classified Information.

„**Originating Party**” means the Party including legal entities or individuals under its jurisdiction, which releases Classified Information.

„**Recipient Party**” means the Party including legal entities or individuals under its jurisdiction, which receives Classified Information.

„**Third Party**” means any state including legal entities or individuals under its jurisdiction or international organisation not being a party to this Agreement.

Article 3
National Security Authorities

1. The National Security Authorities responsible for the protection of Classified Information as well as the implementation of this Agreement are:

In the Republic of Serbia

Канцеларија Савета за националну безбедност и заштиту тајних података.

In the Czech Republic:

Národní bezpečnostní úřad.

2. The National Security Authorities shall provide each other with official contact details and names of other competent authorities which are also responsible for the protection of Classified Information and the implementation of this Agreement.

Article 4
Security Classification Levels

The equivalence of security classification levels is as follows:

In the Republic of Serbia	In the Czech Republic
ДРЖАВНА ТАЈНА/ DRŽAVNA TAJNA	PŘÍSNĚ TAJNÉ
СТРОГО ПОВЕРЉИВО/ STROGO POVERLJIVO	TAJNÉ
ПОВЕРЉИВО/ POVERLJIVO	DŮVĚRNÉ
ИНТЕРНО/INTERNO	VYHRAZENÉ

Article 5
Access to Classified Information

Access to Classified Information released under this Agreement shall be limited only to individuals duly authorised in accordance with the national laws and regulations of the respective Party.

Article 6 Security Principles

1. The Originating Party shall:
 - a) ensure that Classified Information is marked with appropriate security classification markings in accordance with its national laws and regulations;
 - b) inform the Recipient Party of any release conditions of Classified Information;
 - c) inform the Recipient Party of any subsequent changes in classification or declassification.
2. The Recipient Party shall:
 - a) ensure that Classified Information is marked with equivalent security classification level in accordance with Article 4 of this Agreement;
 - b) afford the same degree of protection to Classified Information as afforded to its national Classified Information of equivalent security classification level;
 - c) ensure that Classified Information is not declassified nor its classification changed without the prior written consent of the Originating Party;
 - d) ensure that Classified Information is not released to a Third Party without the prior written consent of the Originating Party;
 - e) use Classified Information only for the purpose it has been released for and in accordance with handling requirements of the Originating Party.

Article 7 Security Co-operation

1. In order to maintain comparable standards of security, the National Security Authorities shall, on request, inform each other of the national laws and regulations concerning protection of Classified Information and the practices stemming from their implementation.
2. On request, the National Security Authorities shall, in accordance with the national laws and regulations, assist each other during the personnel security clearance procedures and facility security clearance procedures.
3. The Parties shall recognise their personnel security clearances and facility security clearances in accordance with the national laws and regulations. Article 4 of this Agreement shall apply accordingly.

4. The National Security Authorities shall promptly notify each other about changes in recognised personnel security clearances and facility security clearances especially in cases of their revocation or termination.

5. The co-operation under this Agreement shall be effected in the English language.

6. The National Security Authorities shall inform each other about security risks which may endanger exchanged Classified Information.

Article 8 Classified Contracts

1. On request, the National Security Authorities shall confirm that proposed contractors as well as individuals participating in pre-contractual negotiations or in the implementation of Classified Contracts have appropriate personnel security clearance or facility security clearance.

2. The National Security Authorities may request that a security inspection is carried out at a facility located on the territory of the other Party to ensure continuing compliance with the national laws and regulations concerning protection of Classified Information.

3. Classified Contracts shall contain a security annex and programme security instructions on the security requirements and on the classification of each element of the Classified Contract. A copy of the programme security instructions shall be forwarded to the National Security Authority of the Party under whose jurisdiction the Classified Contract is to be implemented.

Article 9 Transmission of Classified Information

1. Classified Information shall be transmitted in accordance with the national laws and regulations of the Originating Party through diplomatic channels or as otherwise agreed between the National Security Authorities.

2. The Parties may transmit Classified Information by electronic means in accordance with the security procedures approved by the National Security Authorities.

Article 10

Reproduction, Translation and Destruction of Classified Information

1. Reproductions and translations of Classified Information shall bear appropriate security classification markings and shall be protected as the original Classified Information. Number of reproductions shall be limited to the minimum needed.

2. Translations shall bear a note in the language of translation indicating that they contain Classified Information of the Originating Party.

3. Classified Information marked as ДРЖАБНА ТАЈНА/DRŽAVNA TAJNA/PŘÍSNĚ TAJNĚ shall be translated or reproduced only upon the prior written consent of the Originating Party.

4. Classified Information marked as ДРЖАБНА ТАЈНА/DRŽAVNA TAJNA/PŘÍSNĚ TAJNĚ shall not be destroyed and shall be returned to the Originating Party.

Article 11

Visits

1. Visits requiring access to Classified Information are subject to the prior written consent of the respective National Security Authority, unless otherwise agreed between the National Security Authorities.

2. The visitor shall submit the request for visit at least twenty days in advance of the starting date of the visit to his National Security Authority, which shall forward it to the National Security Authority of the other Party. In urgent cases, the request for visit may be submitted at a shorter notice, subject to prior co-ordination between the National Security Authorities.

3. Request for visit shall include:

- a) first and last name of the visitor, date and place of birth, nationality and passport/ID card number;
- b) position of the visitor and specification of the facility, which the visitor represents;
- c) visitor's personnel security clearance status and its validity;
- d) date and duration of the visit, in case of recurring visit the total period of time covered by the visits shall be stated;
- e) purpose of the visit including the highest level of Classified Information to be involved;
- f) name, address, phone/fax number, e-mail address and point of contact of the facility to be visited;
- g) date, signature and stamping of the official seal of the National Security Authority.

4. The National Security Authorities may agree on a list of visitors entitled to recurring visit. The National Security Authorities shall agree on the further details of the recurring visit.

5. Classified Information acquired by a visitor shall be considered as Classified Information released under this Agreement.

Article 12 Breaches of Security

1. The National Security Authorities shall immediately inform each other in writing of a breach of security resulting in loss, misappropriation or unauthorised disclosure of Classified Information or suspicion of such a breach.

2. The competent security authorities of the Recipient Party shall investigate the incident without delay. The competent security authorities of the Originating Party shall, if required, co-operate in the investigation.

3. In any case, the Recipient Party shall inform the Originating Party in writing about the circumstances of the breach of security, the extent of the damage, the measures adopted for its mitigation and the outcome of the investigation.

Article 13 Expenses

The Parties shall bear their own expenses incurred in the course of the implementation of this Agreement.

Article 14 Interpretation and Disputes

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

Article 15 Implementing Arrangements

Implementing arrangements may be concluded between the National Security Authorities for the implementation of this Agreement.

Article 16
Final Provisions

1. This Agreement is concluded for an indefinite period of time. This Agreement shall enter into force on the first day of the second month following the date of receipt of the last of notifications between the Parties, through diplomatic channels, stating that the internal legal procedures for this Agreement to enter into force have been fulfilled.

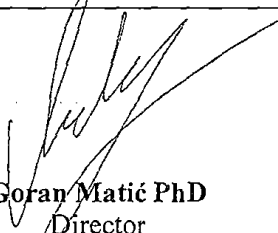
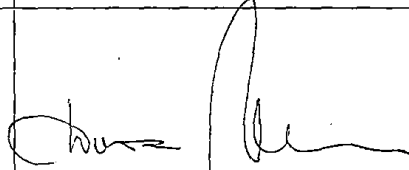
2. This Agreement may be amended on the basis of the mutual consent of the Parties. Such amendments shall enter into force in accordance with paragraph 1 of this Article.

3. Each Party is entitled to terminate this Agreement in writing at any time. In such a case, the validity of this Agreement shall expire after six months following the day on which the other Party receives the written notice of the termination.

4. Regardless of the termination of this Agreement, all Classified Information released or generated under this Agreement shall be protected in accordance with the provisions set forth herein until the Originating Party dispenses the Recipient Party from this obligation.

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

Done in Belgrade, on 13 May 2013 in two originals, in the Serbian, Czech and English languages, each text being equally authentic. In case of different interpretation the English text shall prevail.

For the Republic of Serbia	For the Czech Republic
 Goran Matic PhD Director Office of the National Security Council and Classified Information Protection	 Dušan Navrátil Director National Security Authority