ROZHODNUTIE KOMISIE (EÚ, Euratom) 2019/1963

zo 17. októbra 2019,

ktorým sa stanovujú vykonávacie predpisy pre oblasť priemyselnej bezpečnosti v súvislosti s utajovanými zmluvami na verejné zákazky

EURÓPSKA KOMISIA,

so zreteľom na Zmluvu o fungovaní Európskej únie, a najmä na jej článok 249,

so zreteľom na Zmluvu o založení Európskeho spoločenstva pre atómovú energiu, a najmä na jej článok 106,

so zreteľom na rozhodnutie Komisie (EÚ, Euratom) 2015/443 z 13. marca 2015 o bezpečnosti v Komisii ([1]),

so zreteľom na rozhodnutie Komisie (EÚ, Euratom) 2015/444 z 13. marca 2015 o bezpečnostných predpisoch na ochranu utajovaných skutočností EÚ ([2]),

so zreteľom na rozhodnutie Komisie (EÚ, Euratom) 2017/46 z 10. januára 2017 o bezpečnosti komunikačných a informačných systémov v Európskej komisii ([3]),

po konzultácii so skupinou bezpečnostných expertov Komisie v súlade s článkom 41 ods. 5 rozhodnutia (EÚ, Euratom) 2015/444,

keďže:

(1) Podľa článkov 41, 42, 47 a 48 rozhodnutia (EÚ, Euratom) 2015/444 sa podrobnejšie ustanovenia na doplnenie a podporu kapitoly 6 daného rozhodnutia stanovia vo vykonávacích predpisoch pre oblasť priemyselnej bezpečnosti, ktorými sa upravia otázky ako výberové konania, uzatváranie utajovaných zmlúv, previerky bezpečnosti zariadenia, previerky personálnej bezpečnosti, návštevy, prenos a preprava utajovaných skutočností EÚ (EUCI).

(2) V rozhodnutí (EÚ, Euratom) 2015/444 sa stanovuje, že utajované zmluvy sa vykonávajú v úzkej spolupráci s národným bezpečnostným orgánom, určeným bezpečnostným orgánom alebo akýmkoľvek iným príslušným orgánom dotknutých členských štátov; Členské štáty súhlasili s tým, že zabezpečia, aby bol každý subjekt spadajúci do ich právomoci, ktorý môže dostať alebo vytvoriť utajované skutočnosti s pôvodom v Komisii, primerane bezpečnostne preverený a schopný poskytnúť vhodnú ochranu rovnocennú ochrane, ktorú poskytujú bezpečnostné predpisy Rady Európskej únie na ochranu utajovaných skutočností EÚ, so zodpovedajúcim označením stupňa utajenia, ako sa uvádza v Dohode medzi vládami členských štátov Európskej únie, ktoré sa zišli na zasadnutí Rady, o ochrane utajovaných skutočností, ktoré sa vymieňajú v záujme Európskej únie (2011/C 202/05) ([4]).

(3) Rada, Komisia a Vysoký predstaviteľ Únie pre zahraničné veci a bezpečnostnú politiku sa dohodli na zabezpečení maximálnej konzistentnosti v uplatňovaní bezpečnostných predpisov z hľadiska ich ochrany utajovaných skutočností EÚ pri súčasnom zohľadnení osobitných inštitucionálnych a organizačných potrieb v súlade s vyhláseniami pripojenými k zápisnici zo zasadnutia Rady, na ktorom bolo prijaté rozhodnutie Rady 2013/488/EÚ ([5]) o bezpečnostných predpisoch na ochranu utajovaných skutočností EÚ.

(4) Vo vykonávacích predpisoch Komisie pre oblasť priemyselnej bezpečnosti v súvislosti s utajovanými zmluvami by sa preto takisto mala zabezpečiť maximálna konzistentnosť a mali by sa zohľadniť usmernenia pre oblasť priemyselnej bezpečnosti schválené Bezpečnostným výborom Rady 13. decembra 2016, ako aj články 7 a 22 smernice Európskeho parlamentu a Rady 2009/81/ES ([6]).

(5) Komisia 4. mája 2016 prijala rozhodnutie ([7]), ktorým poverila člena Komisie zodpovedného za bezpečnosť, aby v mene Komisie a na jej zodpovednosť prijal vykonávacie predpisy uvedené v článku 60 rozhodnutia (EÚ, Euratom) 2015/444,

([1]) Ú. v. EÚ L 72, 17.3.2015, s. 41.
([2]) Ú. v. EÚ L 72, 17.3.2015, s. 53.
([3]) Ú. v. EÚ L 6, 11.1.2017, s. 40.
([4]) Ú. v. EÚ C 202, 8.7.2011, s. 13.
([5]) Rozhodnutie Rady 2013/488/EÚ z 23. septembra 2013 o bezpečnostných predpisoch na ochranu utajovaných skutočností EÚ (Ú. v. EÚ L 274, 15.10.2013, s. 1).
([6]) Smernica Európskeho parlamentu a Rady 2009/81/ES z 13. júla 2009 o koordinácii postupov pre zadávanie určitých zákaziek na práce, zákaziek na dodávku tovaru a zákaziek na služby verejnými obstarávateľmi alebo obstarávateľmi v oblastiach obrany a bezpečnosti (Ú. v. EÚ L 216, 20.8.2009, s. 76).
([7]) Rozhodnutie Komisie zo 4. mája 2016 o poverení v súvislosti s bezpečnosťou [C(2016) 2797].

PRIJALA TOTO ROZHODNUTIE:

KAPITOLA 1

VŠEOBECNÉ USTANOVENIA

Článok 1

Predmet úpravy a rozsah pôsobnosti

1. Týmto rozhodnutím sa stanovujú vykonávacie predpisy pre oblasť priemyselnej bezpečnosti v súvislosti s utajovanými zmluvami na verejné zákazky v záujme podpory vykonávania rozhodnutia (EÚ, Euratom) 2015/444, a najmä jeho kapitoly 6.

2. Týmto rozhodnutím sa stanovujú osobitné požiadavky na zaistenie ochrany utajovaných skutočností EÚ (EUCI) hospodárskymi subjektmi vo fáze pred uzavretím zmluvy, počas celého životného cyklu utajovaných zmlúv uzavretých Európskou komisiou, ako aj v subdodávateľských zmluvách uzavretých dodávateľmi Komisie.

3. Toto rozhodnutie sa týka skutočností s týmito stupňami utajenia:

a) RESTREINT UE/EU RESTRICTED;

b) CONFIDENTIEL UE/EU CONFIDENTIAL;

c) SECRET UE/EU SECRET.

Článok 2

Zodpovednosť v rámci Komisie

1. V rámci zodpovedností vymedzených v nariadení o rozpočtových pravidlách ([8]) musí každý povoľujúci úradník Komisie, ktorá je verejným obstarávateľom, zabezpečiť, aby sa v utajovanej zmluve uviedol odkaz na minimálne normy priemyselnej bezpečnosti stanovené v kapitole 6 rozhodnutia (EÚ, Euratom) 2015/444 a v týchto vykonávacích predpisoch, prípadne v oznámení o vyhlásení obstarávania alebo vo výzve na predkladanie ponúk, a aby sa tieto normy v rámci plnenia zákazky dodržiavali.

2. Na tento účel sa príslušný povoľujúci úradník vo všetkých fázach radí s bezpečnostným orgánom Komisie v otázkach spojených s bezpečnostnými prvkami utajovanej zmluvy, programu či projektu, pričom miestneho bezpečnostného úradníka informuje o uzatvorených zmluvách. Rozhodnutie o stupni utajenia konkrétnych predmetov prijíma verejný obstarávateľ s náležitým prihliadnutím na usmernenia pre určovanie stupňa utajenia.

3. Pri dodržiavaní požiadaviek týchto vykonávacích predpisov bezpečnostný orgán Komisie úzko spolupracuje s národnými bezpečnostnými orgánmi (*national security authorities* – NSA) a s určenými bezpečnostnými orgánmi (*designated security authorities* – DSA) dotknutých členských štátov, najmä pokiaľ ide o previerky bezpečnosti zariadenia (*facility security clearances* – FSC) a previerky personálnej bezpečnosti (*personnel security clearances* – PSC), postupy návštev a plány prepravy.

KAPITOLA 2

PRÁCA S VÝZVAMI NA PREDKLADANIE PONÚK V PRÍPADE UTAJOVANÝCH ZMLÚV

Článok 3

Základné zásady

1. Utajované zmluvné zákazky sa zadajú iba hospodárskym subjektom registrovaným v niektorom členskom štáte alebo hospodárskym subjektom registrovaným v tretej krajine alebo zriadeným medzinárodnou organizáciou, ak daná tretia krajina alebo medzinárodná organizácia uzavrela s Európskou úniou dohodu o bezpečnosti utajovaných skutočností, prípadne uzavrela administratívne dojednanie s Komisiou ([9]).

2. Pred spustením výzvy na predkladanie ponúk na utajovanú zmluvnú zákazku verejný obstarávateľ určí stupeň utajenia všetkých skutočností, ktoré by mohli byť poskytnuté uchádzačom. Verejný obstarávateľ takisto určí maximálny stupeň utajenia všetkých skutočností vytvorených pri plnení zmluvy, programu alebo projektu, alebo aspoň očakávaný objem a druh skutočností, ktoré sa majú vypracovať alebo s ktorými sa má manipulovať, a rozhodne o tom, či je potrebný utajený komunikačný a informačný systém (*communication and information system* – CIS).

([8]) Nariadenie Európskeho parlamentu a Rady (EÚ, Euratom) 2018/1046 z 18. júla 2018 o rozpočtových pravidlách, ktoré sa vzťahujú na všeobecný rozpočet Únie, o zmene nariadení (EÚ) č. 1296/2013, (EÚ) č. 1301/2013, (EÚ) č. 1303/2013, (EÚ) č. 1304/2013, (EÚ) č. 1309/2013, (EÚ) č. 1316/2013, (EÚ) č. 223/2014, (EÚ) č. 283/2014 a rozhodnutia č. 541/2014/EÚ a o zrušení nariadenia (EÚ, Euratom) č. 966/2012 (Ú. v. EÚ L 193, 30.7.2018, s. 1).

([9]) Zoznam dohôd, ktoré uzatvorila EÚ, ako aj administratívnych dojednaní, ktoré uzatvorila Európska komisia, podľa ktorých možno vymieňať utajované skutočnosti EÚ s tretími krajinami a medzinárodnými organizáciami, možno nájsť na webovom sídle Komisie.

3. Verejný obstarávateľ zabezpečí, aby sa v oznámeniach o vyhlásení obstarávania na utajované zmluvné zákazky poskytli informácie o osobitných bezpečnostných povinnostiach spojených s utajovanými skutočnosťami. V prílohe I je vzorový príklad informácií, ktoré sa majú uviesť v oznámení o vyhlásení obstarávania.

4. Verejný obstarávateľ zabezpečí, aby sa skutočnosti so stupňom utajenia RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL a SECRET UE/EU SECRET uchádzačom poskytli až po tom, ako podpísali dohodu o zachovaní mlčanlivosti, ktorá uchádzačov zaväzuje manipulovať s EUCI a chrániť ich v súlade s rozhodnutím (EÚ, Euratom) 2015/444 a jeho vykonávacími predpismi.

5. Všetci dodávatelia, od ktorých sa vyžaduje, aby so skutočnosťami so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo SECRET UE/EU SECRET manipulovali alebo ich uchovávali vo svojich priestoroch, či už v rámci plnenia samotnej utajovanej zmluvy alebo vo fáze pred uzavretím zmluvy, musia mať previerku FSC príslušného stupňa. Nasledujú tri možné scenáre vo fáze obstarávania utajovanej zmluvnej zákazky, ktorá zahŕňa EUCI so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo SECRET UE/EU SECRET:

a) žiaden prístup k EUCI so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo SECRET UE/EU SECRET vo fáze obstarávania:

   Ak sa oznámenie o vyhlásení obstarávania alebo výzva na predkladanie ponúk týka zmluvy, ktorá bude zahŕňať EUCI so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo SECRET UE/EU SECRET, no nevyžaduje od uchádzača, aby s takýmito informáciami manipuloval vo fáze obstarávania, nesmú byť uchádzači bez previerky FSC na príslušnom stupni vylúčení z predkladania ponúk z dôvodu, že previerku FSC nemajú.

b) prístup k EUCI so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo SECRET UE/EU SECRET vo fáze obstarávania v objekte verejného obstarávateľa:

   Prístup sa udelí zamestnancom uchádzača, ktorí majú previerku PSC na požadovanom stupni a potrebujú dané skutočnosti poznať. Pred udelením takéhoto prístupu verejný obstarávateľ prostredníctvom bezpečnostného orgánu Komisie u príslušného NSA/DSA overí, či sa podľa vnútroštátnej legislatívy v tejto fáze vyžaduje aj previerka FSC.

c) manipulácia s EUCI so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo SECRET UE/EU SECRET alebo ich uchovávanie v objekte uchádzača vo fáze obstarávania:

   Ak sa v oznámení o vyhlásení obstarávania alebo vo výzve na predkladanie ponúk od uchádzačov vyžaduje manipulácia s EUCI alebo ich uchovávanie vo vlastnom objekte, uchádzač musí mať previerku FSC na požadovanom stupni. Za týchto okolností verejný obstarávateľ získa prostredníctvom bezpečnostného orgánu Komisie od príslušného NSA/DSA uistenie, že uchádzačovi bola vydaná zodpovedajúca previerka FSC. Prístup sa udelí zamestnancom uchádzača, ktorí majú previerku PSC na požadovanom stupni a potrebujú dané skutočnosti poznať.

6. Previerka FSC sa v zásade nevyžaduje na prístup ku skutočnostiam so stupňom utajenia RESTREINT UE/EU RESTRICTED, a to ani počas obstarávania ani v rámci plnenia zmluvy. Ak členské štáty v zmysle vnútroštátnej legislatívy vyžadujú previerku FSC na zmluvné dodávky alebo subdodávky so stupňom utajenia RESTREINT UE/EU RESTRICTED (podľa prílohy IV), neukladajú sa týmito vnútroštátnymi požiadavkami žiadne dodatočné povinnosti ostatným členským štátom, ani sa zo zmlúv na dodávky/subdodávky alebo zo súťaží o ne nesmú vylúčiť uchádzači, dodávatelia alebo subdodávatelia z členských štátov, ktoré takúto povinnosť mať previerku FSC na prístup ku skutočnostiam so stupňom utajenia RESTREINT UE/EU RESTRICTED nemajú. Tieto zmluvy sa budú plniť v členských štátoch v súlade s ich vnútroštátnymi právnymi predpismi.

7. Ak sa na plnenie utajovanej zmluvy vyžaduje previerka FSC, verejný obstarávateľ prostredníctvom bezpečnostného orgánu Komisie zašle dodávateľovmu NSA/DSA žiadosť, pričom použije informačný list previerky bezpečnosti zariadenia (*facility security clearance information sheet* – FSCIS). V dodatku D prílohy III je uvedený príklad listu FSCIS ([10]). Utajovaná zmluvná zákazka sa nezadá, kým dodávateľov NSA/DSA nepotvrdí uchádzačovu previerku FSC. Na FSCIS sa podľa možnosti odpovie do desiatich pracovných dní odo dňa žiadosti.

([10]) Môžu sa použiť aj formuláre, ktoré sa od príkladu uvedeného v týchto vykonávacích predpisoch líšia vzhľadom.

Článok 4

Subdodávky pri utajovaných zmluvách

1. Podmienky, za ktorých môže dodávateľ, ktorý získal utajovanú zmluvnú zákazku Komisie, uzatvárať subdodávateľské zmluvy, sa musia vymedziť vo výzve na predkladanie ponúk a v súťažných podkladoch. Ak utajovaná zmluva umožňuje subdodávky na niektoré jej časti, takéto subdodávky podliehajú predchádzajúcemu písomnému súhlasu verejného obstarávateľa. Verejný obstarávateľ sa pred udelením súhlasu poradí s bezpečnostným orgánom Komisie.

2. Pri utajovaných zmluvných zákazkách môžu subdodávky poskytovať iba hospodárske subjekty registrované v niektorom členskom štáte alebo hospodárske subjekty registrované v tretej krajine alebo zriadené medzinárodnou organizáciou, ak daná tretia krajina alebo medzinárodná organizácia uzavrela s EÚ dohodu o bezpečnosti utajovaných skutočností, prípadne uzavrela administratívne dojednanie s Komisiou ([11]).

KAPITOLA 3

ZADÁVANIE UTAJOVANÝCH ZMLUVNÝCH ZÁKAZIEK KOMISIE

Článok 5

Základné zásady

1. Pri zadávaní utajovanej zmluvnej zákazky sa verejný obstarávateľ spolu s bezpečnostným orgánom Komisie uistí, že neoddeliteľnou súčasťou zmluvnej zákazky sú povinnosti dodávateľa z hľadiska ochrany EUCI poskytnutých danému dodávateľovi alebo vzniknuté v rámci plnenia zmluvy. Bezpečnostné požiadavky špecifické pre danú zmluvu majú podobu bezpečnostnej doložky (*security aspects letter* – SAL). Vzor doložky SAL je uvedený v prílohe III.

2. Pred podpísaním utajovanej zmluvy verejný obstarávateľ na základe konzultácie s bezpečnostným orgánom Komisie vypracuje usmernenia pre určovanie stupňa utajenia (*security classification guide* – SCG) pre úlohy, ktoré sa majú poskytovať, a informácie, ktoré sa majú generovať v rámci plnenia zmluvy, resp. prípadne na úrovni programu alebo projektu. Usmernenia SCG sú súčasťou doložky SAL.

3. Programové alebo projektové bezpečnostné požiadavky majú formu programových (resp. projektových) bezpečnostných pokynov (*programme/project security instruction* – PSI). Pokyny PSI možno vypracovať na základe ustanovení zo vzoru doložky SAL podľa prílohy III. Pokyny PSI vypracuje oddelenie Komisie, ktoré spravuje daný program alebo projekt, v úzkej spolupráci s bezpečnostným orgánom Komisie a predloží ich na schválenie skupine bezpečnostných expertov Komisie. Ak je zmluvná zákazka súčasťou programu alebo projektu, ktorý má vlastné pokyny PSI, použije sa zjednodušená doložka SAL danej zmluvy s odkazom na bezpečnostné ustanovenia stanovené v pokynoch PSI programu, resp. projektu.

4. Verejný obstarávateľ sa považuje za pôvodcu utajovaných skutočností, ktoré vzniknú a s ktorými sa manipuluje na účely plnenia zmluvy.

5. Verejný obstarávateľ prostredníctvom bezpečnostného orgánu Komisie informuje orgány NSA/DSA všetkých dodávateľov a subdodávateľov o uzatvorení utajovaných dodávateľských alebo subdodávateľských zmlúv, ako aj o všetkých prípadných predĺženiach či predčasných ukončeniach týchto dodávateľských alebo subdodávateľských zmlúv. Zoznam požiadaviek v jednotlivých krajinách je uvedený v prílohe IV.

6. Pri zmluvných zákazkách zahŕňajúcich skutočnosti so stupňom utajenia RESTREINT UE/EU RESTRICTED musia zmluvy zahŕňať bezpečnostnú doložku, ktorou sa dodávateľ zaväzuje dodržiavať ustanovenia dodatku E prílohy III. Súčasťou týchto zmlúv musí byť doložka SAL, v ktorej sa stanovia aspoň požiadavky na manipuláciu so skutočnosťami so stupňom utajenia RESTREINT UE/EU RESTRICTED vrátane aspektov informačnej bezpečnosti a konkrétnych požiadaviek, ktoré musí dodávateľ s delegovaním od verejného obstarávateľa splniť na certifikáciu dodávateľovho CIS, v ktorom sa manipuluje so skutočnosťami so stupňom utajenia RESTREINT UE/EU RESTRICTED.

([11]) Zoznam dohôd, ktoré uzatvorila EÚ, ako aj administratívnych dojednaní, ktoré uzatvorila Európska komisia, podľa ktorých možno vymieňať utajované skutočnosti EÚ s tretími krajinami a medzinárodnými organizáciami, možno nájsť na webovom sídle Komisie.

7. Ak sa skutočnosti so stupňom utajenia RESTREINT UE/EU RESTRICTED poskytujú uchádzačom alebo potenciálnym dodávateľom, minimálne požiadavky uvedené v odseku 6 sa zahrnú v ponukách alebo príslušných dohodách o zachovaní mlčanlivosti uzavretých vo fáze obstarávania.

8. Ak to vyžadujú vnútroštátne právne predpisy členských štátov, NSA/DSA zabezpečia, že dodávatelia alebo subdodávatelia spadajúci do ich právomoci spĺňajú príslušné bezpečnostné ustanovenia na ochranu skutočností so stupňom utajenia RESTREINT UE/EU RESTRICTED, a vykonajú overovanie na mieste v priestoroch dodávateľov na svojom území. Ak NSA/DSA takúto povinnosť nemajú, verejný obstarávateľ sa uistí, že dodávateľ implementuje požadované bezpečnostné ustanovenia prílohy III.

Článok 6

Prístup zamestnancov dodávateľov a subdodávateľov k EUCI

1. Oddelenie komisie ako verejný obstarávateľ zabezpečí, aby utajované zmluvy obsahovali ustanovenia, na základe ktorých sa zamestnancom dodávateľa alebo subdodávateľa, ktorí na účely plnenia utajovanej zmluvy alebo subdodávateľskej zmluvy potrebujú prístup k EUCI, takýto prístup poskytne, len ak:

a) sa potvrdilo, že ich potrebujú poznať;

b) v prípade skutočností so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo SECRET UE/EU SECRET im príslušný NSA/DSA alebo iný príslušný bezpečnostný orgán udelil previerku PSC na zodpovedajúcom stupni;

c) boli poučení o platných bezpečnostných predpisoch a postupoch ochrany EUCI a vzali na vedomie svoje povinnosti v súvislosti s ochranou takýchto utajovaných skutočností.

2. Ak chce dodávateľ alebo subdodávateľ využiť v pozícii, ktorá si vyžaduje prístup k EUCI so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo SECRET UE/EU SECRET štátneho príslušníka krajiny mimo EÚ, je zodpovednosťou daného dodávateľa alebo subdodávateľa iniciovať postup bezpečnostnej previerky tejto osoby v súlade s vnútroštátnymi právnymi predpismi platnými v mieste, kde sa má prístup k EUCI poskytnúť.

KAPITOLA 4

NÁVŠTEVY VYKONÁVANÉ V SÚVISLOSTI S UTAJOVANÝMI ZMLUVNÝMI ZÁKAZKAMI

Článok 7

Základné zásady

1. Ak Komisia, dodávatelia alebo subdodávatelia potrebujú na účely plnenia utajovanej zmluvy prístup k utajovaným skutočnostiam so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo SECRET UE/EU SECRET v objektoch druhej strany, spoločne organizujú návštevy svojich objektov v spolupráci s NSA/DSA alebo akýmkoľvek iným dotknutým príslušným bezpečnostným orgánom.

2. Na návštevy uvedené v odseku 1 sa vzťahujú tieto požiadavky:

a) návštevy musia mať oficiálny účel spojený s utajovanou zmluvnou zákazkou zadanou Komisiou;

b) všetci návštevníci musia mať previerku PSC na požadovanom stupni a potrebu poznať príslušné EUCI poskytované alebo vzniknuté v rámci plnenia utajovanej zmluvnej zákazky zadanej Komisiou, aby k nim získali prístup.

Článok 8

Žiadosti o návštevy

1. Návštevy dodávateľov v zariadeniach iných dodávateľov alebo v objektoch Komisie, ktoré zahŕňajú prístup ku skutočnostiam so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo SECRET UE/EU SECRET, sa organizujú v súlade s týmto postupom:

a) bezpečnostný úradník zariadenia, ktoré vysiela návštevníka, vyplní všetky príslušné časti formulára žiadosti o návštevu (*request for visit* – RFV) a žiadosť predloží NSA/DSA daného zariadenia. Vzor formulára žiadosti RFV je stanovený v dodatku C prílohy III;

b) NSA/DSA vysielajúceho zariadenia musí potvrdiť previerku PSC návštevníka pred tým, než žiadosť RFV predloží NSA/DSA hostiteľského zariadenia (alebo bezpečnostnému orgánu Komisie, ak ide o návštevu objektu Komisie);

c) bezpečnostný úradník vysielajúceho zariadenia dostane od svojho NSA/DSA odpoveď NSA/DSA hostiteľského zariadenia (resp. bezpečnostného orgánu Komisie), ktorým sa žiadosť RFV buď schvaľuje, alebo zamieta;

d) Žiadosť RFV sa považuje za schválenú, ak sa do piatich pracovných dní pred dátumom návštevy nevznesú žiadne námietky.

2. Návštevy úradníkov Komisie v zariadeniach dodávateľov, ktoré zahŕňajú prístup ku skutočnostiam so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo SECRET UE/EU SECRET, sa organizujú v súlade s týmto postupom:

a) návštevník vyplní všetky relevantné časti formulára žiadosti RFV a predloží ho bezpečnostnému orgánu Komisie;

b) bezpečnostný orgán Komisie potvrdí previerku PSC návštevníka pred tým, než žiadosť RFV predloží NSA/DSA hostiteľského zariadenia;

c) bezpečnostný orgán Komisie dostane od NSA/DSA hostiteľského zariadenia odpoveď, ktorou sa žiadosť RFV buď schvaľuje, alebo zamieta;

d) Žiadosť RFV sa považuje za schválenú, ak sa do piatich pracovných dní pred dátumom návštevy nevznesú žiadne námietky.

3. Žiadosť RFV sa môže týkať buď jednorazovej návštevy, alebo opakovaných návštev. Pri opakovaných návštevách môže žiadosť RFV platiť najviac jeden rok od žiadaného dátumu začiatku platnosti.

4. Platnosť žiadnej žiadosti RFV nesmie presiahnuť platnosť previerky PSC návštevníka.

5. Všeobecným pravidlom je, že žiadosť RFV sa príslušnému bezpečnostnému orgánu hostiteľského zariadenia predkladá aspoň 15 pracovných dní pred dátumom návštevy.

Článok 9

Postupy pri návštevách

1. Skôr, než sa návštevníkovi umožní prístup k EUCI, bezpečnostný úrad hostiteľského zariadenia musí zabezpečiť súlad so všetkými bezpečnostnými postupmi a pravidlami súvisiacimi s návštevou, ktoré stanovil NSA/DSA.

2. Návštevníci sa pri príchode do hostiteľského zariadenia legitimujú platným preukazom totožnosti alebo pasom. Tieto identifikačné údaje musia zodpovedať informáciám, ktoré sa poskytli v žiadosti RFV.

3. Hostiteľské zariadenie zabezpečí uchovávanie záznamov o všetkých návštevníkoch vrátane ich mien, organizácie, ktorú zastupujú, konečného dátumu platnosti previerky PSC, dátumu návštevy a mien navštívených osôb. Tieto záznamy sa uchovávajú aspoň päť rokov, alebo aj dlhšie, ak si to vyžadujú vnútroštátne predpisy krajiny, kde sa hostiteľské zariadenie nachádza.

Článok 10

Návštevy usporiadané priamo

1. V kontexte osobitných projektov sa môžu príslušné NSA/DSA a bezpečnostný orgán Komisie dohodnúť na postupe, pri ktorom možno návštevy v rámci konkrétnej utajovanej zmluvnej zákazky usporiadať priamo medzi bezpečnostným úradníkom návštevníka a bezpečnostným úradníkom navštevovaného zariadenia. Vzor formulára, ktorý sa na tento účel použije, je stanovený v dodatku C prílohy III. Tento výnimočný postup sa stanoví v pokynoch PSI alebo v iných osobitných dojednaniach. V týchto prípadoch sa neuplatňuje článok 8 ani článok 9 ods. 1

2. Návštevy zahŕňajúce prístup ku skutočnostiam so stupňom utajenia RESTREINT UE/EU RESTRICTED sa usporiadajú priamo medzi vysielajúcim a prijímajúcim subjektom bez potreby dodržiavať postupy podľa článku 8 a článku 9 ods. 1

KAPITOLA 5

PRENOS A PREPRAVA EUCI V RÁMCI PLNENIA UTAJOVANÝCH ZMLÚV

Článok 11

Základné zásady

Verejný obstarávateľ zabezpečí, aby všetky rozhodnutia spojené s prenosom a prepravou EUCI boli v súlade s rozhodnutím (EÚ, Euratom) 2015/444 a jeho vykonávacími predpismi, ako aj s podmienkami utajovanej zmluvy vrátane súhlasu pôvodcu.

Článok 12

Elektronická manipulácia

1. Elektronická manipulácia s EUCI a ich prenos prebieha v súlade s kapitolami 5 a 6 rozhodnutia (EÚ, Euratom) 2015/444 a s jeho vykonávacími predpismi.

Komunikačné a informačné systémy, ktoré vlastní dodávateľ a používajú sa na manipuláciu s EUCI v rámci plnenia zmluvy (ďalej len „dodávateľov CIS“) musí certifikovať zodpovedný orgán bezpečnostnej certifikácie (*security accreditation authority* – SAA). Všetok elektronický prenos EUCI sa zabezpečí kryptografickými produktmi schválenými v súlade s článkom 36 ods. 4 rozhodnutia (EÚ, Euratom) 2015/444. Uplatnia sa opatrenia TEMPEST podľa článku 36 ods. 6 daného rozhodnutia.

2. Bezpečnostnú certifikáciu dodávateľovho CIS, v ktorom sa manipuluje s EUCI so stupňom utajenia RESTREINT UE/EU RESTRICTED, a všetkých jeho prepojení možno delegovať na bezpečnostného úradníka dodávateľa, ak to povoľujú vnútroštátne právne predpisy. Ak sa táto úloha deleguje, dodávateľ je pri manipulácii so skutočnosťami so stupňom utajenia RESTREINT UE/EU RESTRICTED vo svojom CIS zodpovedný za uplatnenie minimálnych bezpečnostných požiadaviek opísaných v doložke SAL. Príslušné NSA/DSA a SAA však majú naďalej zodpovednosť za ochranu skutočností so stupňom utajenia RESTREINT UE/EU RESTRICTED, s ktorými dodávateľ manipuluje, ako aj právo preveriť bezpečnostné opatrenia prijaté dodávateľmi. Okrem toho dodávateľ poskytne verejnému obstarávateľovi, a ak to vyžadujú vnútroštátne právne predpisy, príslušnému národnému SAA vyhlásenie o zhode, ktorým potvrdzuje, že dodávateľov CIS a súvisiace prepojenia boli certifikované na manipuláciu s EUCI so stupňom utajenia RESTREINT UE/EU RESTRICTED ([12]).

Článok 13

Preprava komerčnými kuriérmi

Preprava EUCI komerčnými kuriérmi sa riadi príslušnými ustanoveniami rozhodnutí Komisie o vykonávacích predpisoch manipulácie so skutočnosťami so stupňom utajenia RESTREINT UE/EU RESTRICTED, resp. skutočnosťami so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL.

Článok 14

Osobná (ručná) preprava

1. Osobná preprava utajovaných skutočností podlieha prísnym bezpečnostným požiadavkám.

2. Skutočnosti so stupňom utajenia RESTREINT UE/EU RESTRICTED môžu prepravovať osobne zamestnanci dodávateľa v rámci EÚ, pokiaľ sú splnené tieto požiadavky:

a) použije sa nepriehľadná obálka alebo obal, na ktorých nie je nijako vyznačená povaha obsahu;

([12]) Minimálne požiadavky na komunikačné a informačné systémy, v ktorých sa manipuluje s EUCI so stupňom utajenia RESTREINT UE/EU RESTRICTED, sú stanovené v dodatku E prílohy III.

b) utajované skutočnosti neopustia držbu prenášajúceho;

c) obálka alebo obal sa po ceste neotvorí.

3. Pri skutočnostiach so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL a SECRET UE/EU SECRET sa osobná preprava zamestnancami dodávateľa v rámci členského štátu EÚ dohodne vopred medzi odosielajúcim a prijímajúcim subjektom. Odosielateľský orgán alebo zariadenie informuje prijímajúci orgán alebo zariadenie o podrobnostiach zásielky vrátane referenčného čísla, stupňa utajenia, očakávaného času doručenia a mena kuriéra. Takáto osobná preprava je povolená, pokiaľ sú splnené tieto požiadavky:

a) utajované skutočnosti sa prepravujú v dvojitej obálke alebo obale;

b) vonkajšia obálka (obal) je zabezpečená a nie je na nej nijako vyznačená povaha obsahu, zatiaľ čo vnútorná obálka je označená stupňom utajenia;

c) EUCI neopustia držbu prenášajúceho;

d) obálka alebo obal sa po ceste neotvorí;

e) obálka alebo obal sa prepravuje v uzamknuteľnej aktovke alebo podobnej schválenej batožine takej veľkosti a hmotnosti, aby nikdy nemusela opustiť osobnú držbu prenášajúceho a aby nemusela byť odovzdaná do batožinového priestoru;

f) kuriér má pri sebe kuriérske osvedčenie vystavené jeho príslušným bezpečnostným orgánom, ktorý kuriérovi povolil prepravu takto označenej utajovanej zásielky.

4. Pri osobnej preprave skutočností so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL a SECRET UE/EU SECRET zamestnancami dodávateľa z jedného členského štátu EÚ do iného členského štátu EÚ platia tieto dodatočné pravidlá:

a) kuriér je zodpovedný za bezpečnú držbu prepravovanej utajovanej veci, kým ju neodovzdá príjemcovi;

b) v prípade narušenia bezpečnosti môže odosielateľov NSA/DSA požiadať, aby orgány v krajine, kde k narušeniu došlo, vykonali vyšetrovanie, oznámili zistenia a podľa potreby prijali právne alebo iné kroky;

c) kuriér bol poučený o všetkých bezpečnostných povinnostiach, ktoré treba dodržať pri preprave, a podpísal príslušné vyhlásenie;

d) pokyny pre kuriéra sa pripoja ku kuriérskemu osvedčeniu;

e) kuriér dostal opis zásielky a itinerár;

f) dokumenty sa po skončení cesty (ciest) vrátia vystavujúcemu NSA/DSA, alebo si ich príjemca ponechá k dispozícii na účely monitorovania;

g) ak colné orgány, imigračné orgány alebo hraničná polícia požiadajú o preskúmanie zásielky, povolí sa im otvoriť a prezrieť dostatočnú časť zásielky na to, aby sa presvedčili, že neobsahuje žiadne iné veci než tie, ktoré sa deklarujú;

h) colné orgány by mali byť vyzvané k rešpektovaniu úradnej moci prepravných dokladov a povolení, ktorými kuriér disponuje.

Ak colné orgány zásielku otvoria, mali by tak urobiť mimo dohľadu nepovolaných osôb a podľa možnosti za prítomnosti kuriéra. Kuriér požiada o opätovné zabalenie zásielky a zároveň požiada orgány, ktoré vykonali kontrolu, o opätovné zapečatenie zásielky a o písomné potvrdenie, že ju otvorili.

5. Osobná preprava skutočností so stupňom utajenia RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL a SECRET UE/EU SECRET zamestnancami dodávateľa do tretej krajiny alebo medzinárodnej organizácie podlieha ustanoveniam dohody o bezpečnosti utajovaných skutočností alebo administratívneho dojednania, ktoré Európska únia, resp. Komisia uzatvorila s danou treťou krajinou alebo medzinárodnou organizáciou.

KAPITOLA 6

PLÁNOVANIE KONTINUITY ČINNOSTÍ

Článok 15

Pohotovostné plány a nápravné opatrenia

Oddelenie Komisie ako verejný obstarávateľ zabezpečí, aby sa v utajovanej zmluve uvádzala povinnosť dodávateľa stanoviť pohotovostné plány (*business contingency plans* – BCP) na ochranu EUCI, s ktorými sa v rámci plnenia utajovanej zmluvy manipuluje, počas núdzových situácií, ako aj zaviesť preventívne a nápravné opatrenia v kontexte plánovania kontinuity činností na minimalizáciu vplyvu incidentov súvisiacich s manipuláciou s EUCI a s ich uchovávaním. Dodávateľ o svojich plánoch BCP informuje verejného obstarávateľa.

Článok 16

Nadobudnutie účinnosti

Toto rozhodnutie nadobúda účinnosť dvadsiatym dňom po jeho uverejnení v *Úradnom vestníku Európskej únie*.

V Bruseli 17. októbra 2019

Za Komisiu

v mene predsedu,

Günther OETTINGER

člen Komisie

PRÍLOHA I

ŠTANDARDNÉ INFORMÁCIE V OZNÁMENIACH O VYHLÁSENÍ OBSTARÁVANIA

(prispôsobiť použitým oznámeniam o vyhlásení obstarávania)

Pri zákazkách zahŕňajúcich skutočnosti so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo SECRET UE/EU SECRET

Ostatné osobitné podmienky (*v prípade potreby*)

Plnenie zmluvy podlieha osobitným podmienkam ● áno ○ nie

(*ak áno*) Opis osobitných podmienok

Zmluva bude zahŕňať prístup ku skutočnostiam, manipuláciu so skutočnosťami a/alebo uchovávanie skutočností so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo SECRET UE/EU SECRET, na ktoré sa vzťahujú bezpečnostné predpisy na ochranu utajovaných skutočností EÚ stanovené v rozhodnutí (EÚ, Euratom) 2015/444 a vykonávacie predpisy podľa rozhodnutia ([1]).

Bude sa vyžadovať previerka bezpečnosti zariadenia, ako aj previerky personálnej bezpečnosti zamestnancov dodávateľa, ktorí budú manipulovať s utajovanými skutočnosťami.

Súčasťou zmluvy budú osobitné bezpečnostné povinnosti (bezpečnostná doložka pripojená k zmluve). Subdodávky budú podliehať predchádzajúcemu písomnému súhlasu verejného obstarávateľa, pričom subdodávateľ a jeho zamestnanci musia dodržiavať všetky bezpečnostné predpisy.

Pri zákazkách zahŕňajúcich skutočnosti so stupňom utajenia RESTREINT UE/EU RESTRICTED

Ostatné osobitné podmienky (*v prípade potreby*)

Plnenie zmluvy podlieha osobitným podmienkam ● áno ○ nie

(*ak áno*) Opis osobitných podmienok

Zmluva bude zahŕňať prístup ku skutočnostiam, manipuláciu so skutočnosťami a/alebo uchovávanie skutočností so stupňom utajenia RESTREINT UE/EU RESTRICTED, na ktoré sa vzťahujú bezpečnostné predpisy na ochranu utajovaných skutočností EÚ stanovené v rozhodnutí (EÚ, Euratom) 2015/444 a vykonávacie predpisy podľa rozhodnutia ([2]).

Súčasťou zmluvy budú osobitné bezpečnostné povinnosti (bezpečnostná doložka pripojená k zmluve). Subdodávky budú podliehať predchádzajúcemu písomnému súhlasu verejného obstarávateľa, pričom subdodávateľ a jeho zamestnanci musia dodržiavať všetky bezpečnostné predpisy.

([1]) Verejný obstarávateľ by mal po prijatí vykonávacích predpisov doplniť odkazy.
([2]) Verejný obstarávateľ by mal po prijatí vykonávacích predpisov doplniť odkazy.

PRÍLOHA II

ŠTANDARDNÉ USTANOVENIA ZMLÚV O VEREJNEJ ZÁKAZKE

(prispôsobiť použitým zmluvám)

ČLÁNOK XX

POVINNOSTI SPOJENÉ S BEZPEČNOSŤOU

XX.1. Utajované skutočnosti EÚ

Ak sa pri plnení zmluvy používajú alebo tvoria utajované skutočnosti EÚ, s takýmito skutočnosťami treba až do zrušenia ich utajenia zaobchádzať v súlade s bezpečnostnou doložkou (SAL) a jej usmerneniami pre určovanie stupňa utajenia (SCG) v zmysle prílohy 1, ako aj v súlade s rozhodnutím (EÚ, Euratom) 2015/444 a jeho vykonávacími predpismi [1].

Všetky výstupy zahŕňajúce utajované skutočnosti sa odovzdávajú v súlade s osobitnými postupmi dohodnutými s verejným obstarávateľom.

Na úkony zahŕňajúce utajované skutočnosti nemožno využiť subdodávateľov bez predchádzajúceho výslovného písomného súhlasu verejného obstarávateľa.

Utajované skutočnosti EÚ nemožno poskytnúť žiadnej tretej strane (vrátane subdodávateľov) bez predchádzajúceho výslovného písomného súhlasu verejného obstarávateľa.

[1] Verejný obstarávateľ by mal po prijatí vykonávacích predpisov doplniť odkazy.

PRÍLOHA III

[Príloha IV (k rámcovej zmluve)]

BEZPEČNOSTNÁ DOLOŽKA (SAL)

[Vzor]

Dodatok A

BEZPEČNOSTNÉ POŽIADAVKY

Verejný obstarávateľ musí v bezpečnostnej doložke (SAL) uviesť nasledujúce bezpečnostné požiadavky. Niektoré ustanovenia sa na danú zmluvu nemusia vzťahovať. Tie sú uvedené v hranatých zátvorkách.

Zoznam ustanovení nie je vyčerpávajúci. V závislosti od povahy utajovanej zmluvy možno pridať ďalšie ustanovenia.

VŠEOBECNÉ PODMIENKY

[*Pozn.: platí pre všetky utajované zmluvy*]

1. Bezpečnostná doložka (SAL) je neoddeliteľnou súčasťou utajovanej zmluvy [alebo subdodávateľskej zmluvy] a opisujú sa v nej bezpečnostné požiadavky platné pre konkrétnu zmluvu. Nesplnenie týchto požiadaviek môže byť dostatočným dôvodom na ukončenie zmluvy.

2. Na dodávateľov sa vzťahujú všetky povinnosti stanovené v rozhodnutí (EÚ, Euratom) 2015/444 a jeho vykonávacích predpisoch ([1]).

3. Utajované skutočnosti vzniknuté pri plnení zmluvy treba označiť ako utajované skutočnosti EÚ (EUCI) so stupňom utajenia podľa usmernení pre určovanie stupňa utajenia (SCG) uvedených v dodatku B k tejto doložke. Odchýlenie sa od stupňa utajenia uvedeného v SCG je možné iba na základe písomného schválenia zo strany verejného obstarávateľa.

4. Práva pôvodcu ku všetkým EUCI, ktoré vznikli a s ktorými sa manipuluje na účely plnenia utajovanej zmluvy, si uplatňuje Komisia ako verejný obstarávateľ.

5. Bez písomného súhlasu verejného obstarávateľa nesmie dodávateľ ani subdodávateľ použiť žiadne skutočnosti či veci dodané verejným obstarávateľom alebo vytvorené v mene verejného obstarávateľa na žiaden iný účel, než je plnenie zmluvy.

6. Dodávateľ musí vyšetriť všetky narušenia bezpečnosti súvisiace s EUCI a bezodkladne ich nahlásiť verejnému obstarávateľovi. Dodávateľ alebo subdodávateľ musí bezodkladne oznámiť svojmu zodpovednému národnému bezpečnostnému orgánu (NSA) alebo určenému bezpečnostnému orgánu (DSA), a ak to umožňujú vnútroštátne právne predpisy, aj bezpečnostnému orgánu Komisie všetky prípady, keď je známe alebo existuje dôvod domnievať sa, že EUCI poskytnuté alebo vzniknuté v rámci zmluvy sa stratili alebo boli vyzradené nepovolaným osobám.

7. Po skončení zmluvy musí dodávateľ alebo subdodávateľ bezodkladne vrátiť všetky EUCI, ktoré má v držbe, verejnému obstarávateľovi. Ak je to možné, dodávateľ alebo subdodávateľ môže EUCI namiesto vrátenia zničiť. Treba tak urobiť v súlade s vnútroštátnymi právnymi predpismi krajiny, v ktorej je dodávateľ usadený, na základe predchádzajúceho súhlasu bezpečnostného orgánu Komisie a podľa jeho pokynov. EUCI treba zničiť tak, aby sa nedali vcelku ani čiastočne obnoviť.

8. Ak má dodávateľ alebo subdodávateľ povolenie ponechať si EUCI po ukončení alebo skončení zmluvy, tieto EUCI musia byť naďalej chránené v súlade s rozhodnutím (EÚ, Euratom) 2015/444 (ďalej len „RK 2015/444“) a jeho vykonávacími predpismi ([2]).

9. Každá elektronická manipulácia s EUCI, ako aj elektronické spracovanie a prenos EUCI podliehajú ustanoveniam kapitoly 5 a 6 RK 2015/444. Patrí sem okrem iného požiadavka, že komunikačné a informačné systémy vo vlastníctve dodávateľa, ktoré sa používajú na manipuláciu s EUCI na účely plnenia zmluvy (ďalej len „dodávateľove CIS“) musia byť certifikované ([3]); že všetky elektronické prenosy EUCI musia byť zabezpečené kryptografickými produktmi schválenými v súlade s článkom 36 ods. 4 RK 2015/444 a že treba prijať opatrenia TEMPEST v súlade s článkom 36 ods. 6 RK 2015/444.

([1]) Verejný obstarávateľ by mal po prijatí vykonávacích predpisov doplniť odkazy.
([2]) Verejný obstarávateľ by mal po prijatí vykonávacích predpisov doplniť odkazy.
([3]) Strana, ktorá podstupuje certifikáciu, musí poskytnúť verejnému obstarávateľovi vyhlásenie o zhode, a to prostredníctvom bezpečnostného orgánu Komisie a v koordinácii s príslušným vnútroštátnym orgánom bezpečnostnej certifikácie (SAA).

10. Dodávateľ alebo subdodávateľ musí mať zavedené pohotovostné plány (BCP) na ochranu všetkých EUCI, s ktorými sa v rámci plnenia utajovanej zmluvy manipuluje, počas núdzových situácií, a musí mať zavedené preventívne a nápravné opatrenia na minimalizáciu vplyvu incidentov súvisiacich s manipuláciou s EUCI a s ich uchovávaním. Dodávateľ alebo subdodávateľ o svojich BCP informuje verejného obstarávateľa.

ZMLUVY, KTORÉ SI VYŽADUJÚ PRÍSTUP K SKUTOČNOSTIAM SO STUPŇOM UTAJENIA RESTREINT UE/EU RESTRICTED

11. Na súlad so zmluvou sa nevyžaduje previerka personálnej bezpečnosti. Ku skutočnostiam alebo k veciam so stupňom utajenia RESTREINT UE/EU RESTRICTED však smú mať prístup iba zamestnanci dodávateľa, ktorí takéto skutočnosti potrebujú na plnenie zmluvy (*zásada potreby poznať*), ktorých dodávateľov bezpečnostný úradník poučil o ich zodpovednosti a dôsledkoch akéhokoľvek ohrozenia či narušenia zabezpečenia takýchto skutočností a ktorí písomne vzali na vedomie dôsledky zlyhania pri ochrane EUCI.

12. Bez písomného súhlasu verejného obstarávateľa nesmie dodávateľ ani subdodávateľ poskytnúť prístup ku skutočnostiam alebo k veciam so stupňom utajenia RESTREINT UE/EU RESTRICTED žiadnemu subjektu ani osobe okrem vlastných zamestnancov, ktorí takéto skutočnosti potrebujú poznať.

13. Dodávateľ alebo subdodávateľ musí zachovať označenie stupňa utajenia utajovaných skutočností vzniknutých alebo poskytnutých v rámci plnenia zmluvy a nesmie odtajniť skutočnosti bez písomného súhlasu verejného obstarávateľa.

14. Skutočnosti alebo veci so stupňom utajenia RESTREINT UE/EU RESTRICTED, ktoré sa práve nepoužívajú, musia byť uskladnené v uzamknutom kancelárskom nábytku. Pri preprave musia byť dokumenty uzavreté v nepriehľadnej obálke. Dokumenty nesmú opustiť držbu prenášajúceho a nesmú sa po ceste otvoriť.

15. Dodávateľ alebo subdodávateľ môže doručovať dokumenty so stupňom utajenia RESTREINT UE/EU RESTRICTED Komisii s využitím komerčných kuriérskych spoločností, poštových služieb, osobne alebo elektronicky. Na tento účel sa dodávateľ alebo subdodávateľ drží programových (alebo projektových) bezpečnostných pokynov (PSI), ktoré vydala Komisia, a/alebo jej vykonávacích predpisov priemyselnej bezpečnosti v súvislosti s utajovanými zmluvami na verejné zákazky ([4]).

16. Keď už dokumenty so stupňom utajenia RESTREINT UE/EU RESTRICTED nie sú potrebné, treba ich zničiť tak, aby sa nedali vcelku ani čiastočne obnoviť.

17. Bezpečnostnú certifikáciu dodávateľovho CIS, v ktorom sa manipuluje s EUCI so stupňom utajenia RESTREINT UE/EU RESTRICTED, a všetkých jeho prepojení možno delegovať na bezpečnostného úradníka dodávateľa, ak to povoľujú vnútroštátne právne predpisy. V prípade takéhoto delegovania certifikácie majú príslušné NSA/DSA a SAA naďalej zodpovednosť za ochranu skutočností so stupňom utajenia RESTREINT UE/EU RESTRICTED, s ktorými dodávateľ manipuluje, ako aj právo preveriť bezpečnostné opatrenia prijaté dodávateľom. Okrem toho dodávateľ poskytne verejnému obstarávateľovi, a ak to vyžadujú vnútroštátne právne predpisy, príslušnému národnému SAA vyhlásenie o zhode, ktorým potvrdzuje, že dodávateľov CIS a súvisiace prepojenia boli certifikované na manipuláciu s EUCI so stupňom utajenia RESTREINT UE/EU RESTRICTED.

MANIPULÁCIA SO SKUTOČNOSŤAMI SO STUPŇOM UTAJENIA RESTREINT UE/EU RESTRICTED V KOMUNIKAČNÝCH A INFORMAČNÝCH SYSTÉMOCH (CIS)

18. Minimálne požiadavky na CIS, v ktorých sa manipuluje so skutočnosťami so stupňom utajenia RESTREINT UE/EU RESTRICTED, sú stanovené v dodatku E k tejto bezpečnostnej doložke.

PODMIENKY, ZA KTORÝCH MÔŽE DODÁVATEĽ VYUŽIŤ SUBDODÁVKY

19. Dodávateľ musí získať povolenie od príslušného oddelenia Komisie, ktorá je verejným obstarávateľom, skôr, ako zadá ktorúkoľvek časť utajovanej zmluvy subdodávateľom.

([4]) Verejný obstarávateľ by mal po prijatí vykonávacích predpisov doplniť odkazy.

20. Ako subdodávateľov nemožno využiť spoločnosti registrované v krajinách mimo EÚ ani subjekty patriace medzinárodnej organizácii, pokiaľ daná tretia krajina alebo medzinárodná organizácia nemá uzatvorenú dohodu o bezpečnosti utajovaných skutočností s EÚ alebo administratívne dojednanie s Komisiou.

21. Ak dodávateľ využil subdodávateľov, bezpečnostné ustanovenia zmluvy platia *mutatis mutandis* aj pre takýchto subdodávateľov a ich zamestnancov. V takom prípade je zodpovednosťou dodávateľa zabezpečiť, že všetci subdodávatelia uplatňujú tieto zásady na vlastné využívanie subdodávok. Na zaistenie primeraného bezpečnostného dohľadu musia byť dodávateľove a subdodávateľove orgány NSA/DSA informované o uzavretí všetkých súvisiacich utajovaných subdodávateľských zmlúv na stupni utajenia CONFIDENTIEL UE/EU CONFIDENTIAL a SECRET UE/EU SECRET. Orgánom NSA/DSA dodávateľa a subdodávateľa sa podľa potreby poskytne kópia osobitných bezpečnostných ustanovení danej subdodávateľskej zmluvy. Zoznam orgánov NSA/DSA, ktoré vyžadujú informovanie o bezpečnostných ustanoveniach utajovaných zmlúv so stupňom utajenia RESTREINT UE/EU RESTRICTED, je uvedený v prílohe k vykonávacím predpisom Komisie pre oblasť priemyselnej bezpečnosti v súvislosti s utajovanými zmluvami na verejné zákazky ([1]).

22. Dodávateľ nesmie poskytnúť žiadne EUCI subdodávateľovi bez predchádzajúceho písomného súhlasu verejného obstarávateľa. Ak sa majú EUCI subdodávateľom zasielať často alebo rutinne, verejný obstarávateľ môže udeliť súhlas na určité časové obdobie (napr. 12 mesiacov) alebo na celé trvanie subdodávateľskej zmluvy.

NÁVŠTEVY

Ak sa má štandardný postup žiadosti o návštevu (RFV) použiť pri návštevách zahŕňajúcich skutočnosti so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo SECRET UE/EU SECRET, verejný obstarávateľ musí zahrnúť body 23, 24 a 25 a vymazať bod 26. Ak sa návštevy zahŕňajúce skutočnosti so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo SECRET UE/EU SECRET organizujú priamo medzi vysielajúcim a prijímajúcim subjektom, verejný obstarávateľ musí vymazať body 24 a 25 a zahrnúť len bod 26.

23. Návštevy zahŕňajúce prístup alebo potenciálny prístup ku skutočnostiam so stupňom utajenia RESTREINT UE/EU RESTRICTED sa usporadúvajú priamo medzi vysielajúcim a prijímajúcim subjektom bez potreby dodržiavať postup opísaný ďalej v bodoch 24 až 26.

[24. Pre návštevy, ktoré zahŕňajú prístup alebo potenciálny prístup ku skutočnostiam so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo SECRET UE/EU SECRET, platí tento postup:

a) bezpečnostný úradník zariadenia, ktoré vysiela návštevníka, vyplní všetky príslušné časti formulára žiadosti RFV (dodatok C) a žiadosť predloží NSA/DSA daného zariadenia;

b) NSA/DSA vysielajúceho zariadenia musí potvrdiť previerku PSC návštevníka pred tým, než žiadosť RFV predloží NSA/DSA hostiteľského zariadenia (alebo bezpečnostnému orgánu Komisie, ak ide o návštevu objektu Komisie);

c) bezpečnostný úradník vysielajúceho zariadenia dostane od svojho NSA/DSA odpoveď NSA/DSA hostiteľského zariadenia (resp. bezpečnostného orgánu Komisie), ktorým sa žiadosť RFV buď schvaľuje, alebo zamieta;

d) žiadosť RFV sa považuje za schválenú, ak sa do piatich pracovných dní pred dátumom návštevy nevznesú žiadne námietky.]

[25. Skôr, než sa návštevníkovi/návštevníkom poskytne prístup ku skutočnostiam so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo SECRET UE/EU SECRET, musí hostiteľské zariadenie disponovať schválením od svojho NSA/DSA.]

[26. Návštevy zahŕňajúce prístup alebo potenciálny prístup ku skutočnostiam so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo SECRET UE/EU SECRET sa zorganizujú priamo medzi vysielajúcim a prijímajúcim subjektom (príklad formulára, ktorý na tento účel možno použiť, je uvedený v dodatku C).]

([1]) Verejný obstarávateľ by mal po prijatí vykonávacích predpisov doplniť odkazy.

27. Návštevníci sa pri príchode do hostiteľského zariadenia legitimujú platným preukazom totožnosti alebo pasom.

28. Navštevované hostiteľské zariadenie zabezpečí uchovanie záznamov o všetkých návštevníkoch. Tie musia zahŕňať ich mená, zastupovanú organizáciu, konečný dátum platnosti previerky PSC (ak sa uplatňuje), dátum návštevy a meno navštevovanej osoby (osôb). Bez toho, aby boli dotknuté európske pravidlá ochrany údajov, sa takéto záznamy uchovávajú aspoň päť rokov, resp. podľa potreby v súlade s vnútroštátnymi pravidlami a predpismi.

HODNOTIACE NÁVŠTEVY

29. Bezpečnostný orgán Komisie môže v spolupráci s príslušným NSA/DSA navštíviť zariadenia dodávateľov alebo subdodávateľov, aby sa presvedčil, že sú splnené bezpečnostné požiadavky na manipuláciu s EUCI.

USMERNENIA PRE URČOVANIE STUPŇA UTAJENIA

30. Zoznam všetkých prvkov zmluvy, ktoré sú tajné alebo ktoré majú byť utajované počas plnenia zmluvy, pravidlá takéhoto utajenia a vymedzenie príslušných stupňov utajenia sú zahrnuté v usmerneniach pre určovanie stupňa utajenia (SCG). Usmernenia SCG sú neoddeliteľnou súčasťou tejto zmluvy a sú uvedené v dodatku B k tejto prílohe.

Dodatok B

USMERNENIA PRE URČOVANIE STUPŇA UTAJENIA

[konkrétny text upraviť v závislosti od predmetu zákazky]

Dodatok C

ŽIADOSŤ O NÁVŠTEVU

(VZOR)

Podrobné pokyny na vyplnenie žiadosti o návštevu

(Žiadosť sa musí predložiť iba v angličtine.)

HEADING	Zaškrtnite príslušné polia podľa typu návštevy a typu skutočností a uveďte počet lokalít, ktoré sa majú navštíviť, ako aj počet návštevníkov.
4. **ADMINISTRATIVE DATA**	Vyplní žiadajúci NSA/DSA.
5. **REQUESTING ORGANISATION OR INDUSTRIAL FACILITY**	Vyplňte celý názov a poštovú adresu. Podľa okolností uveďte mesto, štát a PSČ.
6. **ORGANISATION OR INDUSTRIAL FACILITY TO BE VISITED**	Vyplňte celý názov a poštovú adresu. Uveďte mesto, štát, PSČ, číslo telexu alebo faxu (ak existuje), telefónne číslo a e-mailovú adresu. Uveďte meno a telefónne čísla/čísla faxu a e-mailové adresy vášho hlavného kontaktu alebo osoby, s ktorou ste si návštevu dohodli. Poznámky: 1. Je dôležité zadať správne poštové smerovacie číslo (PSČ), pretože jedna spoločnosť môže mať viacero rôznych zariadení. 2. Pri manuálnej žiadosti možno použiť prílohu 1, ak v súvislosti s jednou vecou treba navštíviť dve alebo viac zariadení. Ak sa použije príloha, v poli 3 treba uviesť: „SEE ANNEX 1, NUMBER OF FAC: …“ (uveďte počet zariadení).
7. **DATES OF VISIT**	Uveďte skutočný dátum alebo obdobie (dátum začiatku – dátum konca) návštevy vo formáte „deň – mesiac – rok“. V náležitých prípadoch uveďte alternatívny dátum alebo obdobie v zátvorkách.
8. **TYPE OF INITIATIVE**	Uveďte, či návštevu iniciovala žiadajúca organizácia alebo zariadenie, alebo išlo o pozvanie zo strany navštevovaného zariadenia.
9. **THE VISIT RELATES TO:**	Uveďte celý názov projektu, zmluvy alebo výzvy na predkladanie ponúk, skratky používajte, iba ak sú bežné.

10. **SUBJECT TO BE DISCUSSED/ JUSTIFICATION**	Stručne opíšte dôvody návštevy. Nepoužívajte nevysvetlené skratky. Poznámky: V prípade opakovaných návštev by sa tu na začiatku dátového prvku malo uviesť „Recurring visits“ (napr. Recurring visits to discuss_____)
11. **ANTICIPATED LEVEL OF CLASSIFIED INFORMATION TO BE INVOLVED**	Uveďte SECRET UE/EU SECRET (S-UE/EU-S) alebo CONFIDENTIEL UE/EU CONFIDENTIAL (C-UE/EU-C), podľa okolností.
12. **PARTICULARS OF VISITOR**	Poznámka: Ak návšteva zahŕňa viac ako dvoch účastníkov, treba použiť prílohu 2.
13. **THE SECURITY OFFICER OF THE REQUESTING ENTITY**	V tomto poli sa vyžaduje meno, telefónne číslo, číslo faxu a e-mailová adresa bezpečnostného úradníka žiadajúceho zariadenia.
14. **CERTIFICATION OF SECURITY CLEARANCE**	Toto pole vyplní certifikačný orgán. Poznámky pre certifikačný orgán: a) Uveďte meno, adresu, telefónne číslo, číslo faxu a e-mailovú adresu (môže byť predtlačené). b) Toto pole treba podľa potreby podpísať a opečiatkovať.
15. **REQUESTING SECURITY AUTHORITY**	Toto pole vyplní NSA/DSA. Poznámky pre NSA/DSA: a) Uveďte meno, adresu, telefónne číslo, číslo faxu a e-mailovú adresu (môže byť predtlačené). b) Toto pole treba podľa potreby podpísať a opečiatkovať.

Všetky polia musia byť vyplnené a formulár zaslaný medzivládnymi kanálmi ([2]).

([2]) Ak sa dohodlo, že návštevy zahŕňajúce prístup alebo potenciálny prístup k EUCI so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL a SECRET UE/EU SECRET možno usporiadať priamo, vyplnený formulár možno predložiť priamo bezpečnostnému úradníkovi navštevovaného zariadenia.

REQUEST FOR VISIT

(MODEL)

TO: _____

1. **TYPE OF VISIT REQUEST**	2. **TYPE OF INFORMATION**	3. **SUMMARY**
☐ Single ☐ Recurring ☐ Emergency ☐ Amendment ☐ Dates ☐ Visitors ☐ Facility For an amendment, insert the NSA/DSA original RFV Reference No_____	☐ C-UE/EU-C ☐ S-UE/EU-S	No of sites: _____ No of visitors: _____

4. **ADMINISTRATIVE DATA:**

Requester:	NSA/DSA RFV Reference No_____
To:	Date *(dd/mm/yyyy)*: _____/_____/_____

5. **REQUESTING ORGANISATION OR INDUSTRIAL FACILITY:**

NAME:

POSTAL ADDRESS:

E-MAIL ADDRESS:

FAX NO: TELEPHONE NO:

6. **ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED** *(Annex 1 to be completed)*

7. **DATE OF VISIT** *(dd/mm/yyyy)*: FROM _____/_____/_____ TO _____/_____/_____

8. **TYPE OF INITIATIVE:**

☐ Initiated by requesting organisation or facility

☐ By invitation of the facility to be visited

9. **THE VISIT RELATES TO CONTRACT:**

10. **SUBJECT TO BE DISCUSSED/REASONS/PURPOSE** *(Include details of host entity and any other relevant information. Abbreviations should be avoided):*

11. **ANTICIPATED HIGHEST CLASSIFICATION LEVEL OF INFORMATION/MATERIAL OR SITE ACCESS TO BE INVOLVED:**

12. **PARTICULARS OF VISITOR(S)** *(Annex 2 to be completed)*

13. **THE SECURITY OFFICER OF THE REQUESTING ORGANISATION OR INDUSTRIAL FACILITY:**

NAME:

TELEPHONE NO:

E-MAIL ADDRESS:

SIGNATURE:

14. **CERTIFICATION OF SECURITY CLEARANCE LEVEL:**

NAME:

ADDRESS:

TELEPHONE NO:

E-MAIL ADDRESS:

STAMP

SIGNATURE: DATE *(dd/mm/yyyy)*: _____/_____/_____

15. **REQUESTING NATIONAL SECURITY AUTHORITY/DESIGNATED SECURITY AUTHORITY:**

NAME:

ADDRESS:

TELEPHONE NO:

E-MAIL ADDRESS:

STAMP

SIGNATURE: DATE *(dd/mm/yyyy)*: _____/_____/_____

16. **REMARKS** *(Mandatory justification required in the case of an emergency visit)*:

<miesto na uvedenie odkazu na platnú legislatívu o ochrane osobných údajov a prepojenia na povinné informácie pre dotknutú osobu, napr. ako sa vykonáva článok 13 všeobecného nariadenia o ochrane údajov ([3])>

([3]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (Ú. v. EÚ L 119, 4.5.2016, s. 1).

PRÍLOHA 1 k formuláru RFV

ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED

1.

NAME:

ADDRESS:

TELEPHONE NO:

FAX NO:

NAME OF POINT OF CONTACT:

E-MAIL:

TELEPHONE NO:

NAME OF SECURITY OFFICER OR

SECONDARY POINT OF CONTACT:

E-MAIL:

TELEPHONE NO:

2.

NAME:

ADDRESS:

TELEPHONE NO:

FAX NO:

NAME OF POINT OF CONTACT:

E-MAIL:

TELEPHONE NO:

NAME OF SECURITY OFFICER OR

SECONDARY POINT OF CONTACT:

E-MAIL:

TELEPHONE NO:

(Continue as required)

<miesto na uvedenie odkazu na platnú legislatívu o ochrane osobných údajov a prepojenia na povinné informácie pre dotknutú osobu, napr. ako sa vykonáva článok 13 všeobecného nariadenia o ochrane údajov ([1])>

([1]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (Ú. v. EÚ L 119, 4.5.2016, s. 1).

PRÍLOHA 2 k formuláru RFV

PARTICULARS OF VISITOR(S)

1.

SURNAME:

FIRST NAMES *(as per passport)*:

DATE OF BIRTH *(dd/mm/yyyy)*: ____/____/____

PLACE OF BIRTH:

NATIONALITY:

SECURITY CLEARANCE LEVEL:

PP/ID NUMBER:

POSITION:

COMPANY/ORGANISATION:

2.

SURNAME:

FIRST NAMES *(as per passport)*:

DATE OF BIRTH *(dd/mm/yyyy)*: ____/____/____

PLACE OF BIRTH:

NATIONALITY:

SECURITY CLEARANCE LEVEL:

PP/ID NUMBER:

POSITION:

COMPANY/ORGANISATION:

(Continue as required)

<miesto na uvedenie odkazu na platnú legislatívu o ochrane osobných údajov a prepojenia na povinné informácie pre dotknutú osobu, napr. ako sa vykonáva článok 13 všeobecného nariadenia o ochrane údajov ([1])>

([1]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (Ú. v. EÚ L 119, 4.5.2016, s. 1).

Dodatok D

INFORMAČNÝ LIST PREVIERKY BEZPEČNOSTI ZARIADENIA (FSCIS)

(VZOR)

1. **Úvod**

1.1. V tejto časti je uvedený príklad informačného listu previerky bezpečnosti zariadenia (FSCIS) na rýchlu výmenu informácií o previerke bezpečnosti zariadenia (FSC), ktoré je zapojené do utajovaných výziev a dodávateľských alebo subdodávateľských zmlúv, medzi národným bezpečnostným orgánom (NSA) alebo určeným bezpečnostným orgánom (DSA), inými príslušnými vnútroštátnymi bezpečnostnými orgánmi a Komisiou (ako verejným obstarávateľom).

1.2. FSCIS je platný, iba ak je opečiatkovaný príslušným NSA/DSA alebo iným príslušným orgánom.

1.3. FSCIS sa člení na žiadosť a odpoveď a možno ho použiť na účely uvedené vyššie alebo na akékoľvek iné účely, na ktoré sa vyžaduje status FSC konkrétneho zariadenia. Žiadajúci NSA/DSA uvedie dôvod žiadosti v poli 7 prvej časti.

1.4. Údaje uvedené vo FSCIS obyčajne nie sú utajované; to znamená, že keď sa má FSCIS posielať medzi príslušnými NSA/DSA/Komisiou, prednostne by sa mal posielať elektronicky.

1.5. NSA/DSA by sa mali v maximálnej miere snažiť odpovedať na žiadosť FSCIS do desiatich pracovných dní.

1.6. Ak by sa v spojení s týmto uistením prenášali akékoľvek utajované skutočnosti alebo zadávala utajovaná zmluvná zákazka, treba o tom informovať vystavujúci NSA/DSA.

Postupy a pokyny napoužívanie informačného listu previerky bezpečnosti zariadenia (FSCIS)

Tieto podrobné pokyny sú pre NSA/DSA alebo Komisiu ako verejného obstarávateľa, ktorí FSCIS vypĺňajú. Žiadosť treba vyplniť prednostne na počítači veľkými písmenami.

ZÁHLAVIE	Žiadateľ vyplní celý názov NSA/DSA a krajiny.
1. **DRUH ŽIADOSTI**	Žiadajúci verejný obstarávateľ zvolí spomedzi možností príslušný druh žiadosti FSCIS. Uveďte požadovaný stupeň bezpečnostnej previerky. Používajte tieto skratky: SECRET UE/EU SECRET = S-UE/EU-S CONFIDENTIEL UE/EU CONFIDENTIAL = C-UE/EU-C CIS = komunikačné a informačné systémy na spracovanie utajovaných skutočností

2. **ÚDAJE O SUBJEKTE**	Polia 1 až 6 sú zrejmé. V poli 4 by sa mal použiť štandardný dvojmiestny kód krajiny. Pole 5 je nepovinné.
3. **DÔVOD ŽIADOSTI**	Uveďte konkrétny dôvod žiadosti a projektové ukazovatele, číslo zmluvy alebo výzvy na predkladanie ponúk. Uveďte potrebu možností uchovávania, stupeň utajenia v danom CIS atď. Mali by sa uviesť aj všetky prípadné dátumy konečných termínov/lehôt/udelenia zákazky, ktoré majú vplyv na dokončenie FSC.
4. **ŽIADAJÚCI NSA/DSA**	Uveďte názov skutočného žiadateľa (v mene NSA/DSA) a dátum žiadosti vo formáte dd/mm/rrrr.
5. **ODPOVEĎ**	Polia 1 – 5: zvoľte príslušné polia. Pole 2: Ak FSC prebieha, odporúča sa uviesť pre žiadateľa orientačný čas spracovania (ak je známy). Pole 6: a) Hoci sa validácia líši v závislosti od krajiny alebo dokonca zariadenia, odporúča sa uviesť konečný dátum platnosti FSC. b) Ak má uistenie o FSC časovo neobmedzenú platnosť, toto pole možno vyškrtnúť. c) V súlade s príslušnými vnútroštátnymi pravidlami a predpismi je za vyžiadanie obnovenia FSC zodpovedný buď žiadateľ, alebo dodávateľ/subdodávateľ.
6. **POZNÁMKY**	Možno použiť na dodatočné informácie o FSC, zariadení alebo uvedených položkách.
7. **VYSTAVUJÚCI NSA/DSA**	Uveďte názov poskytujúceho orgánu (v mene NSA/DSA) a dátum odpovede vo formáte dd/mm/rrrr.

INFORMAČNÝ LIST PREVIERKY BEZPEČNOSTI ZARIADENIA (FSCIS)

(VZOR)

Všetky polia musia byť vyplnené a formulár zaslaný medzivládnymi kanálmi alebo kanálmi medzi vládou a medzinárodnou organizáciou.

ŽIADOSŤ O UISTENIE O PREVIERKE BEZPEČNOSTI ZARIADENIA

Pre: _____

(názov krajiny NSA/DSA)

Vyplňte polia s odpoveďami podľa potreby:

[] Poskytnúť uistenie o FSC na stupni: [] S-UE/EU-S [] C-UE/EU-C

pre ďalej uvedené zariadenie

[] vrátane ochrany utajovaných vecí/skutočností

[] vrátane komunikačných a informačných systémov (CIS) na spracovanie utajovaných skutočností

[] Iniciovať – priamo alebo na príslušnú žiadosť dodávateľa alebo subdodávateľa – proces získania FSC po stupeň utajenia ..... vrátane ochrany na stupni ..... a CIS na stupni ....., ak zariadenie tieto možnosti na danom stupni zatiaľ neposkytuje.

Potvrdiť presnosť nasledujúcich údajov o zariadení a podľa potreby opraviť/doplniť.

1. Úplný názov zariadenia:	Opravy/doplnenia:
.....	.....
2. Úplná adresa zariadenia:	
.....	.....
3. Poštová adresa (ak sa líši od 2 vyššie)	
.....	.....
4. PSČ/mesto/krajina	
.....	.....
5. Meno bezpečnostného úradníka	
.....	.....
6. Telefón/fax/e-mail: bezpečnostného úradníka	
.....	.....

7. Žiadosť sa predkladá z týchto dôvodov: [uveďte podrobnosti o predzmluvnej fáze (výber návrhu), (sub)dodávateľskej zmluve, programe/projekte atď.]

.....

Žiadajúci NSA/DSA/verejný obstarávateľ z Komisie: Názov: ..... Dátum: (dd/mm/rrrr) .....

ODPOVEĎ (do 10 pracovných dní)

Týmto sa potvrdzuje, že:

1. [] uvedené zariadenie má previerku FSC po stupeň utajenia (vrátane) [] S-UE/EU-S

   [] C-UE/EU-C.

2. Uvedené zariadenie má možnosti na ochranu utajovaných skutočností/vecí:

   [] áno, stupeň: ..... [] nie.

3. Uvedené zariadenie má certifikovaný/povolený CIS:

   [] áno, stupeň: ..... [] nie.

4. [] Na základe žiadosti bol iniciovaný proces získania FSC. O potvrdení alebo zamietnutí previerky FSC budete informovaní.

5. [] Uvedené zariadenie nedisponuje previerkou FSC.

6. Toto uistenie o FSC je platné do: ..... (*dd/mm/rrrr*) alebo kým NSA/DSA neodporučí inak. V prípade skoršieho zrušenia platnosti alebo zmien uvedených údajov budete informovaní.

7. Poznámky:

   .....

Vystavujúci NSA/DSA Názov: ..... Dátum: *(dd/mm/rrrr)* .....

<miesto na uvedenie odkazu na platnú legislatívu o ochrane osobných údajov a prepojenia na povinné informácie pre dotknutú osobu, napr. ako sa vykonáva článok 13 všeobecného nariadenia o ochrane údajov ([2])>

([2]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (Ú. v. EÚ L 119, 4.5.2016, s. 1).

Dodatok E

Minimálne požiadavky na ochranu EUCI v elektronickom formáte so stupňom utajenia RESTREINT UE/EU RESTRICTED, s ktorými sa manipuluje v dodávateľovom CIS

Všeobecne

1. Dodávateľ musí byť zodpovedný za zaistenie, aby ochrana skutočností so stupňom utajenia RESTREINT UE/EU RESTRICTED bola v súlade s minimálnymi bezpečnostnými požiadavkami stanovenými v tejto bezpečnostnej doložke, ako aj s akýmikoľvek ďalšími požiadavkami, ktoré oznámi verejný obstarávateľ alebo prípadne národný bezpečnostný orgán (NSA) alebo určený bezpečnostný orgán (DSA).

2. Je zodpovednosťou dodávateľa splniť bezpečnostné požiadavky stanovené v tomto dokumente.

3. Na účely tohto dokumentu komunikačný a informačný systém (CIS) zahŕňa všetko vybavenie používané na manipuláciu s EUCI, ich uchovávanie a prenos vrátane pracovných staníc, tlačiarní, kopírovačiek, faxov, serverov, systémov na správu sietí, sieťových radičov a radičov komunikácie, laptopov, notebookov, tabletových počítačov, smartfónov a vymeniteľných pamäťových zariadení ako USB kľúče, CD, SD karty atď.

4. Zvláštne vybavenie, ako napríklad kryptografické produkty, musí byť chránené v súlade s osobitnými operačnými bezpečnostnými postupmi (SecOPs).

5. Dodávatelia musia zaviesť štruktúru zodpovednú za riadenie bezpečnosti CIS, v ktorom sa manipuluje so skutočnosťami so stupňom utajenia RESTREINT UE/EU RESTRICTED a vymenovať bezpečnostného úradníka zodpovedného za príslušné zariadenie.

6. Využitie IT riešení (hardvéru, softvéru alebo služieb) v súkromnom vlastníctve zamestnancov dodávateľa na uchovávanie alebo spracovanie skutočností so stupňom utajenia RESTREINT UE/EU RESTRICTED nie je povolené.

7. Certifikáciu dodávateľovho CIS, v ktorom sa manipuluje so skutočnosťami so stupňom utajenia RESTREINT UE/EU RESTRICTED, musí schváliť orgán bezpečnostnej certifikácie (SAA) dotknutého členského štátu alebo sa deleguje na dodávateľovho bezpečnostného úradníka, ak to povoľujú vnútroštátne právne predpisy.

8. Manipulovať so skutočnosťami so stupňom utajenia RESTREINT UE/EU RESTRICTED, uchovávať alebo prenášať ich (pevným alebo bezdrôtovým pripojením) ako v prípade všetkých ostatných neutajených skutočností podľa zmluvy je možné, iba ak sú zašifrované schválenými kryptografickými produktmi. Tieto kryptografické produkty musí schváliť EÚ alebo členský štát.

9. Externé zariadenia zapojené do údržby/opráv musia byť zmluvne viazané dodržiavať príslušné ustanovenia o manipulácii so skutočnosťami so stupňom utajenia RESTREINT UE/EU RESTRICTED podľa tohto dokumentu.

10. Na žiadosť verejného obstarávateľa alebo príslušného NSA/DSA/SAA musí dodávateľ doložiť súlad so zmluvnou bezpečnostnou doložkou. Ak sa vyžiada aj audit a kontrola procesov a zariadení dodávateľa na zaistenie súladu s týmito požiadavkami, dodávatelia musia povoliť zástupcom verejného obstarávateľa, NSA/DSA/SAA alebo príslušného bezpečnostného orgánu EÚ výkon takéhoto auditu a kontroly.

Fyzická bezpečnosť

11. Priestory, v ktorých sa používajú CIS na zobrazenie, uchovávanie, spracovanie alebo prenos skutočností so stupňom utajenia RESTREINT UE/EU RESTRICTED, alebo priestory, v ktorých sú umiestnené servery, systémy na správu sietí, sieťové radiče a radiče komunikácie takýchto CIS, by mali byť zriadené ako oddelené a kontrolované priestory vybavené vhodným systémom kontroly prístupu. Prístup do týchto oddelených a kontrolovaných priestorov by mal byť vyhradený pre jednotlivcov s osobitným povolením. Bez toho, aby bol dotknutý bod 8, vybavenie opísané v bode 3 musí byť umiestnené v takýchto oddelených a kontrolovaných priestoroch.

12. Musia byť zavedené bezpečnostné mechanizmy a/alebo postupy na reguláciu zavádzania alebo pripájania vymeniteľných počítačových pamäťových médií (ako sú USB kľúče, ukladacie zariadenia alebo CD-RW) ku komponentom daného CIS.

Prístup k CIS

13. Prístup k dodávateľovmu CIS, v ktorom sa manipuluje s EUCI, sa povolí striktne na základe potreby poznať a iba oprávneným zamestnancom.

14. Pri všetkých CIS sa vedie aktualizovaný zoznam oprávnených používateľov. Všetci používatelia sa musia na začiatku každého spracovania autentifikovať.

15. Heslá, ktoré sú súčasťou väčšiny bezpečnostných opatrení na identifikáciu a autentifikáciu, musia mať aspoň deväť znakov, zahŕňať číslice a „zvláštne“ znaky (ak to systém umožňuje), ako aj písmená. Heslá sa musia meniť aspoň raz za 180 dní. Musia sa čo najskôr zmeniť, ak boli narušené alebo vyzradené neoprávnenej osobe alebo ak existuje podozrenie z takéhoto narušenia alebo vyzradenia.

16. Všetky CIS musia zahŕňať interné riadenie prístupu, ktoré neoprávneným používateľom zabráni v prístupe ku skutočnostiam so stupňom utajenia RESTREINT UE/EU RESTRICTED alebo v zásahu do nich, alebo v zmene systémových a bezpečnostných nastavení. Používatelia musia byť automaticky odhlásení z CIS, ak ich zariadenie nie je obsluhované určitý vopred stanovený časový interval, alebo musí CIS po 15 minútach aktivovať heslom chránený šetrič obrazovky.

17. Každému používateľovi CIS sa priradí jedinečné používateľské konto a používateľské ID. Používateľské kontá sa musia automaticky zablokovať, ak došlo aspoň k piatim neúspešným pokusom o prihlásenie za sebou.

18. Všetci používatelia CIS musia byť oboznámení so svojimi zodpovednosťami a s postupmi, ktoré treba dodržať na ochranu skutočností so stupňom utajenia RESTREINT UE/EU RESTRICTED v danom CIS. Zodpovednosti a postupy, ktoré sa majú dodržať, sa zdokumentujú a používatelia ich písomne potvrdia.

19. Používatelia a správcovia musia mať k dispozícii postupy SecOPs, ktoré zahŕňajú opis bezpečnostných rolí a súvisiaci zoznam úloh, pokynov a plánov.

Záznamy, audit a reakcia na incidenty

20. Všetky prístupy do CIS sa musia zaznamenávať.

21. Musia sa zaznamenávať tieto udalosti:

    a) všetky pokusy o prihlásenie bez ohľadu na úspešnosť;

    b) odhlásenie (vrátane automatického po intervale nečinnosti, ak k nemu dôjde);

    c) priradenie, odobratie alebo zmena prístupových práv a oprávnení;

    d) vytvorenie, vymazanie alebo zmena hesiel.

22. Pri všetkých udalostiach uvedených vyššie sa musia uviesť aspoň tieto informácie:

    a) typ udalosti;

    b) používateľské ID;

    c) dátum a čas;

    d) ID zariadenia.

23. Uvedené záznamy by mali bezpečnostnému úradníkovi pomôcť preskúmať potenciálne bezpečnostné incidenty. Takisto sa môžu použiť v prípadných súdnych vyšetrovaniach bezpečnostných incidentov. Všetky bezpečnostné záznamy by sa mali pravidelne kontrolovať s cieľom identifikovať možné bezpečnostné incidenty. Záznamy musia byť chránené proti neoprávnenému vymazaniu alebo úpravám.

24. Dodávateľ musí mať zavedenú stratégiu riešenia bezpečnostných incidentov. Používateľom a správcom sa musí vysvetliť, ako reagovať na incidenty, ako ich nahlasovať a čo robiť v stave núdze.

25. Vyzradenie skutočností so stupňom utajenia RESTREINT UE/EU RESTRICTED alebo podozrenie z ich vyzradenia sa musí oznámiť verejnému obstarávateľovi. Oznámenie musí zahŕňať opis dotknutých skutočností a opis okolností vyzradenia alebo podozrenia z vyzradenia. Všetkých používateľov CIS treba oboznámiť s postupom nahlasovania skutočných alebo domnelých bezpečnostných incidentov bezpečnostnému úradníkovi.

Siete a prepojenia

26. Ak je dodávateľov CIS, v ktorom sa manipuluje so skutočnosťami so stupňom utajenia RESTREINT UE/EU RESTRICTED, prepojený s CIS, ktorý nie je certifikovaný, výrazne to zvyšuje ohrozenie bezpečnosti samotného CIS, ako aj skutočností so stupňom utajenia RESTREINT UE/EU RESTRICTED, s ktorými sa v ňom manipuluje. Týka sa to internetu, ako aj iných verejných alebo súkromných CIS, ako napríklad CIS vo vlastníctve dodávateľa alebo subdodávateľa. V takom prípade musí dodávateľ vykonať vyhodnotenie rizika s cieľom identifikovať dodatočné bezpečnostné požiadavky, ktoré treba implementovať v rámci procesu bezpečnostnej certifikácie. Dodávateľ poskytne verejnému obstarávateľovi, a ak to vyžadujú vnútroštátne právne predpisy, príslušnému SAA vyhlásenie o zhode, ktorým potvrdzuje, že dodávateľov CIS a súvisiace prepojenia boli certifikované na manipuláciu s EUCI so stupňom utajenia RESTREINT UE/EU RESTRICTED.

27. Vzdialený prístup z iných systémov k službám LAN (napr. vzdialený prístup k e-mailom a vzdialená systémová podpora) je zakázaný, pokiaľ nie sú zavedené osobitné bezpečnostné opatrenia, s ktorými súhlasil verejný obstarávateľ, a ak to vyžadujú vnútroštátne právne predpisy, ktoré schválil príslušný SAA.

Správa konfigurácie

28. Musí byť k dispozícii a pravidelne sa udržiavať podrobná hardvérová a softvérová konfigurácia, ktorá zodpovedá certifikačnej/schvaľovacej dokumentácii (vrátane systémových a sieťových schém).

29. Dodávateľov bezpečnostný úradník musí vykonať kontroly konfigurácie hardvéru a softvéru s cieľom uistiť sa, že nebol zavedený nepovolený hardvér ani softvér.

30. Zmeny konfigurácie dodávateľovho CIS treba posúdiť z hľadiska dôsledkov pre zabezpečenie a musí ich schváliť bezpečnostný úradník, a ak to vyžadujú vnútroštátne právne predpisy, SAA.

31. Systém sa musí preskúmať z hľadiska bezpečnostnej zraniteľnosti aspoň raz za štvrťrok. Musí byť nainštalovaný a aktualizovaný softvér na detekciu malvéru. Ak je to možné, mal by byť takýto softvér schválený na štátnej alebo medzinárodnej úrovni, v opačnom prípade by malo ísť o všeobecne akceptovaný odvetvový štandard.

32. Dodávateľ musí vypracovať plán na zabezpečenie kontinuity činností. Musia sa stanoviť záložné postupy na riešenie týchto aspektov:

a) frekvencia zálohovania;

b) požiadavky na uchovávanie na mieste (ohňovzdorné schránky) alebo mimo neho;

c) kontrola oprávnenosti prístupu k záložným kópiám.

Sanitácia a zničenie

33. Pri CIS alebo dátových pamäťových médiách, v/na ktorých boli v ktoromkoľvek okamihu uložené skutočnosti so stupňom utajenia RESTREINT UE/EU RESTRICTED, sa musia pred likvidáciou vykonať na celom systéme alebo pamäťovom médiu tieto sanitačné opatrenia:

a) pamäť typu flash (napr. USB kľúče, SD karty, jednotky SSD, hybridné pevné disky) sa musí prepísať aspoň trikrát a následne sa overí, že pôvodný obsah nemožno zrekonštruovať, alebo sa musí vymazať s použitím schváleného vymazávacieho softvéru;

b) magnetické médiá (napr. pevné disky) sa musia prepísať alebo demagnetizovať;

c) optické médiá (napr. CD a DVD) sa musia skartovať alebo rozdrviť;

d) pri všetkých ostatných typoch pamäťových médií treba príslušné bezpečnostné požiadavky konzultovať s verejným obstarávateľom alebo v náležitých prípadoch s NSA/DSA/SAA.

34. Skutočnosti so stupňom utajenia RESTREINT UE/EU na akomkoľvek pamäťovom médiu treba sanitovať pred tým, než sa poskytne subjektu, ktorý nemá oprávnenie na prístup k skutočnostiam so stupňom utajenia RESTREINT UE/EU RESTRICTED (napr. na účely údržby).

PRÍLOHA IV

Previerka bezpečnosti zariadenia a previerka personálnej bezpečnosti dodávateľov, ktorých práca zahŕňa skutočnosti so stupňom utajenia RESTREINT UE/EU RESTRICTED, a NSA/DSA vyžadujúci oznamovanie utajovaných zmlúv so stupňom utajenia RESTREINT UE/EU RESTRICTED [1]

Členský štát	FSC		Oznamovanie dodávateľskej alebo subdodávateľskej zmluvy zahŕňajúcej skutočnosti so stupňom utajenia R-UE/EU-R orgánu NSA/DSA		PSC	
	ÁNO	NIE	ÁNO	NIE	ÁNO	NIE
Belgicko		X		X		X
Bulharsko		X		X		X
Česko		X		X		X
Dánsko	X		X		X	
Nemecko		X		X		X
Estónsko	X		X			X
Írsko		X		X		X
Grécko	X			X	X	
Španielsko		X	X			X
Francúzsko		X		X		X
Chorvátsko		X	X			X
Taliansko		X	X			X
Cyprus		X	X			X
Lotyšsko		X		X		X

[1] Týmito vnútroštátnymi požiadavkami na FSC/PSC a oznamovanie pri zmluvách zahŕňajúcich skutočnosti so stupňom utajenia RESTREINT UE/EU RESTRICTED sa nesmú ukladať žiadne dodatočné povinnosti iným členským štátom alebo dodávateľom spadajúcim do ich právomoci.
Pozn.: Oznamovanie zmlúv zahŕňajúcich skutočnosti so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL a SECRET UE/EU SECRET je povinné.

Členský štát	FSC		Oznamovanie dodávateľskej alebo subdodávateľskej zmluvy zahŕňajúcej skutočnosti so stupňom utajenia R-UE/EU-R orgánu NSA/DSA		PSC	
	ÁNO	NIE	ÁNO	NIE	ÁNO	NIE
Litva	X		X			X
Luxembursko	X		X		X	
Maďarsko		X		X		X
Malta		X		X		X
Holandsko	X (iba pri zmluvách v rezorte obrany)		X (iba pri zmluvách v rezorte obrany)			X
Rakúsko		X		X		X
Poľsko		X		X		X
Portugalsko		X		X		X
Rumunsko		X		X		X
Slovinsko	X		X			X
Slovensko	X		X			X
Fínsko		X		X		X
Švédsko	X (iba pri zmluvách v rezorte obrany)		X (iba pri zmluvách v rezorte obrany)		X (iba pri zmluvách v rezorte obrany)	
Spojené kráľovstvo		X		X		X

PRÍLOHA V

ZOZNAM ÚTVAROV NÁRODNÝCH BEZPEČNOSTNÝCH ORGÁNOV/URČENÝCH BEZPEČNOSTNÝCH ORGÁNOV ZODPOVEDNÝCH ZA SPRAVOVANIE POSTUPOV SÚVISIACICH S PRIEMYSELNOU BEZPEČNOSŤOU

BELGICKO

National Security Authority
FPS Foreign Affairs
Rue des Petits Carmes 15
1000 Brussels
Tel.: +32 25014542 (Secretariat)
Fax: +32 25014596
E-mail: nvo-ans@diplobel.fed.be

BULHARSKO

1. State Commission on Information Security – National Security Authority
   4 Kozloduy Street
   1202 Sofia
   Tel.: +359 29835775
   Fax: +359 29873750
   E-mail: dksi@government.bg

2. Defence Information Service at the Ministry of Defence (security service)
   3 Dyakon Ignatiy Street
   1092 Sofia
   Tel.: +359 29227002
   Fax: +359 29885211
   E-mail: office@iksbg.org

3. State Intelligence Agency (security service)
   12 Hajdushka Polyana Street
   1612 Sofia
   Tel.: +359 29813221
   Fax: +359 29862706
   E-mail: office@dar.bg

4. State Agency for Technical Operations (security service)
   29 Shesti Septemvri Street
   1000 Sofia
   Tel.: +359 29824971
   Fax: +359 29461339
   E-mail: dato@dato.bg

   (Uvedené príslušné orgány vykonávajú schvaľovacie postupy na vystavenie FSC pre právne subjekty, ktoré sa uchádzajú o uzatvorenie utajovanej zmluvy, a PSC pre osoby plniace utajovanú zmluvu pre potreby týchto orgánov.)

5. State Agency National Security (security service)
   45 Cherni Vrah Blvd.
   1407 Sofia
   Tel.: +359 28147109
   Fax: +359 29632188, +359 28147441
   E-mail: dans@dans.bg

   (Uvedená bezpečnostná služba vykonáva schvaľovacie postupy na vystavenie FSC a PSC všetkým ostatným právnym subjektom a osobám v krajine, ktoré sa uchádzajú o uzatvorenie utajovanej zmluvy alebo plnia utajovanú zmluvu.)

ČESKO

National Security Authority
Industrial Security Department
PO BOX 49
150 06 Praha 56
Tel.: +420 257283129
E-mail: sbr@nbu.cz

DÁNSKO

1. Politiets Efterretningstjeneste
(Danish Security Intelligence Service)
Klausdalsbrovej 1
2860 Søborg
Tel.: +45 33148888
Fax: +45 33430190

2. Forsvarets Efterretningstjeneste
(Danish Defence Intelligence Service)
Kastellet 30
2100 Copenhagen Ø
Tel.: +45 33325566
Fax: +45 33931320

NEMECKO

1. V otázkach politiky priemyselnej bezpečnosti, FSC, plánov dopravy (okrem kryptografie/CCI):
Federal Ministry of Economic Affairs and Energy
Industrial Security Division – ZB3
Villemombler Str. 76
53123 Bonn
Tel.: +49 228996154028
Fax: +49 228996152676
E-mail: dsagermany-zb3@bmwi.bund.de (office e-mail: address)

2. Štandardné žiadosti o návštevy od nemeckých spoločností a v nemeckých spoločnostiach:
Federal Ministry of Economic Affairs and Energy
Industrial Security Division – ZB2
Villemombler Str. 76
53123 Bonn
Tel.: +49 228996152401
Fax: +49 228996152603
E-mail: zb2-international@bmwi.bund.de (office e-mail: address)

3. Plány prepravy kryptografického materiálu:
Federal Office for Information Security (BSI)
National Distribution Agency/NDA-EU DEU
Mainzer Str. 84
53179 Bonn
Tel.: +49 2289995826052
Fax: +49 228991095826052
E-mail: NDAEU@bsi.bund.de

ESTÓNSKO

National Security Authority Department
Estonian Foreign Intelligence Service
Rahumäe tee 4B
11316 Tallinn
Tel.: +372 6939211
Fax: +372 6935001
E-mail: nsa@fis.gov.ee

ÍRSKO

National Security Authority Ireland
Department of Foreign Affairs and Trade
76-78 Harcourt Street
Dublin 2
D02 DX45
Tel.: +353 14082724
E-mail: nsa@dfa.ie

GRÉCKO

Hellenic National Defence General Staff
E' Division (Security INTEL, CI BRANCH)
E3 Directorate
Industrial Security Office
227-231 Mesogeion Avenue
15561 Holargos, Athens
Tel.: +30 2106572022, +30 2106572178
Fax: +30 2106527612
E-mail: daa.industrial@hndgs.mil.gr

ŠPANIELSKO

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Calle Argentona 30
28023 Madrid
Tel.: +34 913725000
Fax: +34 913725808
E-mail: nsa-sp@areatec.com
V otázkach previerok personálnej bezpečnosti: asip@areatec.com
V otázkach plánov prepravy a medzinárodných návštev: sp-ivtco@areatec.com

FRANCÚZSKO

National Security Authority (NSA) (v otázkach politiky a implementácie mimo rezortu obrany)
Secrétariat général de la défense et de la sécurité nationale
Sous-direction Protection du secret (SGDSN/PSD)
51 boulevard de la Tour-Maubourg
75700 Paris 07 SP
Tel.: +33 171758193
Fax: +33 171758200
E-mail: ANSFrance@sgdsn.gouv.fr

Designated Security Authority (implementácia v rezorte obrany)
Direction Générale de l'Armement
Service de la Sécurité de Défense et des systèmes d'Information (DGA/SSDI)
60 boulevard du général Martial Valin
CS 21623
75509 Paris Cedex 15
Tel.: +33 988670421
E-mail: v prípade formulárov a odosielaných žiadostí RFV: dga-ssdi.ai.fct@intradef.gouv.fr
v prípade prichádzajúcich žiadostí RFV: dga-ssdi.visit.fct@intradef.gouv.fr

CHORVÁTSKO

Office of the National Security Council
Croatian NSA
Jurjevska 34
10000 Zagreb
Tel.: +385 14681222
Fax: +385 14686049
E-mail: NSACroatia@uvns.hr

TALIANSKO

Presidenza del Consiglio dei Ministri
D.I.S. – U.C.Se.
Via di Santa Susanna 15
00187 Roma
Tel.: +39 0661174266
Fax: +39 064885273

CYPRUS

ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Λεωφόρος Στροβόλου, 172-174
Στρόβολος, 2048, Λευκωσία
Τηλέφωνα: +357 22807569, +357 22807764
Τηλεομοιότυπο: +357 22302351
E-mail: cynsa@mod.gov.cy

Ministry of Defence
National Security Authority (NSA)
172-174, Strovolos Avenue
2048 Strovolos, Nicosia
Tel.: +357 22807569, +357 22807764
Fax: +357 22302351
E-mail: cynsa@mod.gov.cy

LOTYŠSKO

National Security Authority
Constitution Protection Bureau of the Republic of Latvia
P.O. Box 286
Riga LV-1001
Tel.: +371 67025418, +371 67025463
Fax: +371 67025454
E-mail: ndi@sab.gov.lt, ndi@zd.gov.lv

LITVA

Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija
(The Commission for Secrets Protection Coordination of the Republic of Lithuania)
National Security Authority
Gedimino 40/1
LT-01110 Vilnius
Tel.: +370 70666703, +370 70666701
Fax: +370 70666700
E-mail: nsa@vsd.lt

LUXEMBURSKO

Autorité Nationale de Sécurité
207, route d'Esch
L-1471 Luxembourg
Tel.: +352 24782210
E-mail: ans@me.etat.lu

MAĎARSKO

National Security Authority of Hungary
H-1399 Budapest P.O. Box 710/50
H-1024 Budapest, Szilágyi Erzsébet fasor 11/B
Tel.: +36 13911862
Fax: +36 13911889
E-mail: nbf@nbf.hu

MALTA

Director of Standardisation
Designated Security Authority for Industrial Security
Standards & Metrology Institute
Malta Competition and Consumer Affairs Authority
Mizzi House
National Road
Blata I-Bajda HMR9010
Tel.: +356 23952000
Fax: +356 21242406
E-mail: certification@mccaa.org.mt

HOLANDSKO

1. Ministry of the Interior and Kingdom Relations
PO Box 20010
2500 EA The Hague
Tel.: +31 703204400
Fax: +31 703200733
E-mail: nsa-nl-industry@minbzk.nl

2. Ministry of Defence
Industrial Security Department
PO Box 20701
2500 ES The Hague
Tel.: +31 704419407
Fax: +31 703459189
E-mail: indussec@mindef.nl

RAKÚSKO

1. Federal Chancellery of Austria
Department I/12, Office for Information Security
Ballhausplatz 2
1014 Vienna
Tel.: +43 153115202594
E-mail: isk@bka.gv.at

2. DSA in the military sphere:
BMLVS/Abwehramt
Postfach 2000
1030 Vienna
E-mail: abwa@bmlvs.gv.at

POĽSKO

Internal Security Agency
Department for the Protection of Classified Information
Rakowiecka 2A
00-993 Warsaw
Tel.: +48 225857944
Fax: +48 225857443
E-mail: nsa@abw.gov.pl

PORTUGALSKO

Gabinete Nacional de Segurança
Serviço de Segurança Industrial
Rua da Junqueira nº 69
1300-342 Lisbon
Tel.: +351 213031710
Fax: +351 213031711
E-mail: sind@gns.gov.pt, franco@gns.gov.pt

RUMUNSKO

Oficiul Registrului Național al Informațiilor Secrete de Stat – ORNISS
Romanian NSA – ORNISS – National Registry Office for Classified Information
4th Mures Street
012275 Bucharest
Tel.: +40 212075115
Fax: +40 212245830
E-mail: relatii.publice@orniss.ro, nsa.romania@nsa.ro

SLOVINSKO

Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
1000 Ljubljana
Tel.: +386 14781390
Fax: +386 14781399
E-mail: gp.uvtp@gov.si

SLOVENSKO

Národný bezpečnostný úrad
(National Security Authority)
Security Clearance Department
Budatínska 30
851 06 Bratislava
Tel.: +421 268691111
Fax: +421 268691700
E-mail: podatelna@nbu.gov.sk

FÍNSKO

National Security Authority
Ministry for Foreign Affairs
P.O. Box 453
FI-00023 Government
E-mail: NSA@formin.fi

ŠVÉDSKO

1. National Security Authority
   Utrikesdepartementet (Ministry for Foreign Affairs)
   UD SÄK/NSA
   SE-103 39 Stockholm
   Tel.: +46 84051000
   Fax: +46 87231176
   E-mail: ud-nsa@gov.se

2. DSA
   Försvarets Materielverk (Swedish Defence Materiel Administration)
   FMV Säkerhetsskydd
   SE-115 88 Stockholm
   Tel.: +46 87824000
   Fax: +46 87826900
   E-mail: security@fmv.se

UNITED KINGDOM

UK National Security Authority
Room 335, 3rd Floor
70 Whitehall
London
SW1A 2AS
Tel.: +44 2072765497, +44 2072765645
E-mail: UK-NSA@cabinet-office.x.gsi.gov.uk