ROZHODNUTIE KOMISIE (EÚ, Euratom) 2021/259

z 10. februára 2021,

ktorým sa stanovujú vykonávacie predpisy pre oblasť priemyselnej bezpečnosti v súvislosti s utajovanými grantmi

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 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 ([1]),

so zreteľom na rozhodnutie Komisie (EÚ, Euratom) 2015/443 z 13. marca 2015 o bezpečnosti v Komisii ([2]),

so zreteľom na rozhodnutie Komisie (EÚ, Euratom) 2015/444 z 13. marca 2015 o bezpečnostných predpisoch na ochranu utajovaných skutočností EÚ ([3]),

so zreteľom na rozhodnutie Komisie (EÚ, Euratom) 2017/46 z 10. januára 2017 o bezpečnosti komunikačných a informačných systémov v Európskej komisii ([4]),

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 uvedeného rozhodnutia majú stanoviť vo vykonávacích predpisoch pre oblasť priemyselnej bezpečnosti, ktorými sa bude riadiť udeľovanie utajovaných dohôd o grante, priemyselné bezpečnostné previerky, personálne bezpečnostné previerky, návštevy, prenos a preprava utajovaných skutočností EÚ (EUCI).

(2) V rozhodnutí (EÚ, Euratom) 2015/444 sa stanovuje, že utajované dohody o grante 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) ([5]).

([1]) Ú. v. EÚ L 193, 30.7.2018, s. 1.
([2]) Ú. v. EÚ L 72, 17.3.2015, s. 41.
([3]) Ú. v. EÚ L 72, 17.3.2015, s. 53.
([4]) Ú. v. EÚ L 6, 11.1.2017, s. 40.
([5]) Ú. v. EÚ C 202, 8.7.2011, s. 13.

(3) Rada, Komisia a Vysoký predstaviteľ Únie pre zahraničné veci a bezpečnostnú politiku sa dohodli na zabezpečení maximálnej konzistentnosti pri 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 ([6]) o bezpečnostných predpisoch na ochranu utajovaných skutočností EÚ.

(4) Vo vykonávacích predpisoch Komisie pre oblasť priemyselnej bezpečnosti v súvislosti s utajovanými grantmi 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.

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

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 grantmi v zmysle rozhodnutia (EÚ, Euratom) 2015/444, a najmä jeho kapitoly 6.

2. Týmto rozhodnutím sa stanovujú osobitné požiadavky na zabezpečenie ochrany utajovaných skutočností EÚ (EUCI) pri uverejňovaní výziev na predkladanie návrhov, pri udeľovaní grantov a vykonávaní utajovaných dohôd o grante, ktoré uzavrela Európska komisia.

3. Toto rozhodnutie sa týka grantov zahŕňajúcich skutočnosti s týmito stupňami utajenia:

a) RESTREINT UE/EU RESTRICTED;

b) CONFIDENTIEL UE/EU CONFIDENTIAL;

c) SECRET UE/EU SECRET.

4. Toto rozhodnutie sa uplatňuje bez toho, aby boli dotknuté osobitné pravidlá stanovené v iných právnych aktoch, ako sú pravidlá týkajúce sa Programu rozvoja európskeho obranného priemyslu.

Článok 2

Zodpovednosť v rámci Komisie

1. Súčasťou povinností povoľujúceho úradníka orgánu poskytujúceho grant podľa nariadenia Európskeho parlamentu a Rady (EÚ, Euratom) 2018/1046 je zabezpečiť, aby bol utajovaný grant v súlade s rozhodnutím (EÚ, Euratom) 2015/444 a jeho vykonávacími predpismi.

([6]) 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).

([7]) Rozhodnutie Komisie zo 4. 5. 2016 o poverení v súvislosti s bezpečnosťou [C(2016) 2797 final].

2. Na tento účel sa príslušný povoľujúci úradník vo všetkých fázach radí s bezpečnostným orgánom Komisie v otázkach spojených s bezpečnostnými prvkami utajovanej dohody o grante, programu či projektu, pričom miestneho bezpečnostného úradníka informuje o podpísaných utajovaných dohodách o grante. Rozhodnutie o stupni utajenia určitých aspektov prijíma orgán poskytujúci grant s náležitým prihliadnutím na sprievodcu stupňami utajenia.

3. Ak sa uplatňujú bezpečnostné pokyny pre program alebo projekt uvedené v článku 5 ods. 3, orgán poskytujúci grant a bezpečnostný orgán Komisie vykonávajú povinnosti, ktoré im v tých pokynoch boli pridelené.

4. 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 priemyselné bezpečnostné previerky (facility security clearances – FSC) a personálne bezpečnostné previerky (personnel security clearances – PSC), postupy návštev a plány prepravy.

5. Ak granty spravujú výkonné agentúry EÚ alebo iné financujúce orgány a osobitné pravidlá stanovené v iných právnych aktoch uvedených v článku 1 ods. 4 sa neuplatňujú, tak potom:

a) delegujúce oddelenie Komisie uplatňuje práva pôvodcu utajovaných skutočností EÚ vytvorených v súvislosti s grantmi, ak sa tak ustanovuje v dohodách o delegovaní;

b) delegujúce oddelenie Komisie je zodpovedné za určovanie stupňa utajenia;

c) žiadosti o informácie týkajúce sa bezpečnostnej previerky a oznámenia pre NSA a/alebo DSA sa zasielajú prostredníctvom bezpečnostného orgánu Komisie.

KAPITOLA 2

MANIPULÁCIA S VÝZVAMI NA PREDKLADANIE NÁVRHOV UTAJOVANÝCH GRANTOV

Článok 3

Základné zásady

1. Utajované časti grantov vykonávajú iba prijímatelia registrovaní v členskom štáte alebo prijímatelia registrovaní v tretej krajine alebo zriadení medzinárodnou organizáciou, ak daná tretia krajina alebo medzinárodná organizácia uzavrela s Úniou dohodu o bezpečnosti utajovaných skutočností, prípadne uzavrela správne dojednanie s Komisiou ([8]).

2. Pred spustením výzvy na predkladanie návrhov utajovaného grantu orgán poskytujúci grant určí stupeň utajenia všetkých skutočností, ktoré by mohli byť poskytnuté žiadateľom. Orgán poskytujúci grant takisto určí maximálny stupeň utajenia všetkých skutočností použitých alebo vytvorených pri plnení dohody o grante, 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).

3. Orgán poskytujúci grant zabezpečí, aby sa vo výzvach na predkladanie návrhov utajovaných grantov poskytli informácie o osobitných bezpečnostných povinnostiach spojených s utajovanými skutočnosťami. Dokumentácia k výzve musí obsahovať vysvetlenia týkajúce sa harmonogramu, ktorý majú prijímatelia na získanie priemyselných bezpečnostných previerok (FSC), ak sa vyžadujú. Prílohy I a II obsahujú vzorové príklady pre informácie týkajúce sa podmienok výzvy.

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

4. Orgán poskytujúci grant zabezpečí, aby sa skutočnosti so stupňom utajenia RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL a SECRET UE/EU SECRET žiadateľom poskytli až po tom, ako podpísali dohodu o mlčanlivosti, ktorá žiadateľov zaväzuje manipulovať s EUCI a chrániť ich v súlade s rozhodnutím (EÚ, Euratom) 2015/444, jeho vykonávacími predpismi a platnými vnútroštátnymi predpismi.

5. Ak sa skutočnosti so stupňom utajenia RESTREINT UE/EU RESTRICTED poskytujú žiadateľom, minimálne požiadavky uvedené v článku 5 ods. 7 tohto rozhodnutia sa zahrnú vo výzve alebo v príslušných dohodách o zachovaní mlčanlivosti uzavretých vo fáze návrhu.

6. Všetci žiadatelia a prijímatelia, od ktorých sa vyžaduje, aby manipulovali s informáciami so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo SECRET UE/EU SECRET alebo ich uchovávali v rámci svojich zariadení buď vo fáze návrhu alebo počas plnenia samotnej utajovanej dohody o grante, musia mať FSC na požadovanom stupni, s výnimkou prípadov uvedených v odseku 9. Nasledujú tri možné scenáre vo fáze návrhu utajovaného grantu, 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 návrhu:

   Ak sa výzva na predkladanie návrhov týka grantu, ktorý bude zahŕňať EUCI so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo SECRET UE/EU SECRET, avšak od žiadateľa nevyžaduje, aby s takýmito informáciami manipuloval vo fáze návrhu, nesmie byť žiadateľ bez previerky FSC na príslušnom stupni vylúčený z predkladania ponúk z dôvodu, že previerku FSC nemá.

b) prístup k EUCI so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo SECRET UE/EU SECRET počas fázy návrhu v objekte orgánu poskytujúceho grant:

   Prístup sa udelí zamestnancom žiadateľa, ktorí majú previerku PSC na požadovanom stupni a potrebu poznať utajované skutočnosti.

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

   Ak sa vo výzve na predkladanie návrhov od žiadateľov vyžaduje manipulácia s EUCI alebo ich uchovávanie vo vlastnom objekte, žiadateľ musí mať previerku FSC na požadovanom stupni. Za týchto okolností orgán poskytujúci grant získa prostredníctvom bezpečnostného orgánu Komisie od príslušného NSA alebo DSA ubezpečenie, že žiadateľovi bola udelená zodpovedajúca previerka FSC pred tým, ako mu bol poskytnutý akýkoľvek materiál EUCI. Prístup sa udelí zamestnancom žiadateľa, ktorí majú previerku PSC na požadovanom stupni a potrebu poznať utajované skutočnosti.

7. Previerka FSC alebo PSC sa v zásade nevyžaduje na prístup ku skutočnostiam so stupňom utajenia RESTREINT UE/EU RESTRICTED, a to ani počas fázy návrhu ani v rámci plnenia dohody o grante. Ak členské štáty v zmysle vnútroštátnych predpisov vyžadujú FSC alebo PSC na dohody o grante alebo subdodávateľské zmluvy so stupňom utajenia RESTREINT UE/EU RESTRICTED (podľa prílohy IV), neukladajú sa týmito vnútroštátnymi požiadavkami žiadne dodatočné povinnosti ostatným členským štátom, ani sa z príslušných dohôd o grante alebo zo subdodávateľských zmlúv či hospodárskej súťaže o ne nesmú vylúčiť žiadatelia, prijímatelia alebo subdodávatelia z členských štátov, ktoré takéto požiadavky mať previerku FSC alebo PSC na prístup ku skutočnostiam so stupňom utajenia RESTREINT UE/EU RESTRICTED nemajú. Tieto dohody o grante sa plnia v členských štátoch v súlade s ich vnútroštátnymi právnymi predpismi.

8. Ak sa pri manipulácii s výzvou na predkladanie ponúk a pri vykonávaní utajovanej dohody o grante vyžaduje FSC, orgán poskytujúci grant predloží prostredníctvom bezpečnostného orgánu Komisie žiadosť národnému bezpečnému orgánu alebo určenému bezpečnostnému orgánu prijímateľa použitím informačného listu priemyselnej bezpečnostnej previerky (facility security clearance information sheet – FSCIS) alebo akéhokoľvek zavedeného rovnocenného elektronického formulára. V dodatku D prílohy III je uvedený príklad formulára FSCIS ([9]). Na FSCIS sa podľa možnosti odpovie do desiatich pracovných dní odo dňa žiadosti.

9. Ak sa vládne zariadenia členských štátov alebo zariadenia pod kontrolou ich vlády zúčastňujú na utajovaných grantoch, ktoré si vyžadujú previerky FSC, a ak sa FSC pre tieto zariadenia nevydávajú podľa vnútroštátnych právnych predpisov, orgán poskytujúci grant overí prostredníctvom bezpečnostného orgánu Komisie u dotknutého NSA alebo DSA, či sú tieto vládne zariadenia schopné manipulovať s EUCI na požadovanom stupni.

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

10. Ak sa na plnenie utajovanej dohody o grante vyžaduje PSC a ak je podľa vnútroštátnych predpisov pred udelením PSC potrebná FSC, orgán poskytujúci grant overí prostredníctvom bezpečnostného orgánu Komisie u národného bezpečnostného orgánu alebo určeného bezpečnostného orgánu prijímateľa, použitím FSCIS, či je prijímateľ držiteľom FSC alebo či prebieha proces FSC. V tomto prípade Komisia nevydá žiadosti o PSC použitím informačného listu personálnej bezpečnostnej previerky (personnel security clearance information sheet – PSCIS).

Článok 4

Subdodávky pri utajovaných grantoch

1. Podmienky, za ktorých prijímatelia môžu na úkony zahŕňajúce EUCI využiť subdodávateľov, sa vymedzia vo výzve a v dohode o grante. Tieto podmienky zahŕňajú požiadavku, aby sa všetky FSCIS predložili prostredníctvom bezpečnostného orgánu Komisie. Využívanie subdodávateľov podlieha predchádzajúcemu písomnému súhlasu orgánu poskytujúceho grant. V prípade potreby využívanie subdodávateľov musí byť v súlade so základným aktom, ktorým sa zriaďuje program.

2. Pri utajovaných častiach grantov môžu subdodávky poskytovať iba subjekty registrované v členskom štáte alebo subjekty registrované v tretej krajine alebo zriadené medzinárodnou organizáciou, ak daná tretia krajina alebo medzinárodná organizácia uzavrela s Úniou dohodu o bezpečnosti utajovaných skutočností, prípadne uzavrela správne dojednanie s Komisiou ([10]).

KAPITOLA 3

MANIPULÁCIA S UTAJOVANÝMI GRANTMI

Článok 5

Základné zásady

1. Pri udeľovaní utajovaného grantu sa orgán poskytujúci grant spolu s bezpečnostným orgánom Komisie uistí, že neoddeliteľnou súčasťou dohody o grante sú povinnosti prijímateľov z hľadiska ochrany EUCI použitých alebo vzniknutých v rámci plnenia dohody o grante. Bezpečnostné požiadavky špecifické pre daný grant majú podobu bezpečnostnej doložky (security aspects letter – SAL). Vzor doložky SAL je uvedený v prílohe III.

2. Pred podpísaním utajovaného grantu orgán poskytujúci grant schváli sprievodcu stupňami utajenia (security classification guide – SCG) pre úlohy, ktoré sa majú plniť, a informácie, ktoré sa majú generovať v rámci plnenia grantu, resp. prípadne na úrovni programu alebo projektu. Sprievodca stupňami utajenia je súčasťou doložky SAL.

3. Špecifické programové alebo projektové bezpečnostné požiadavky majú formu programových (resp. projektových) bezpečnostných pokynov (programme/project security instruction – PSI). PSI možno vypracovať na základe ustanovení zo vzoru doložky SAL podľa prílohy III. 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 dohoda o grante súčasťou programu alebo projektu, ktorý má vlastné PSI, použije sa zjednodušená doložka SAL danej dohody o grante s odkazom na bezpečnostné ustanovenia stanovené v PSI programu, resp. projektu.

4. S výnimkou prípadov spomenutých v článku 3 ods. 9 sa utajovaná dohoda o grante nepodpíše, kým NSA alebo DSA žiadateľa nepotvrdia FSC žiadateľa, alebo ak sa utajovaná dohoda o grante udelí konzorciu, kým NSA alebo DSA aspoň jedného žiadateľa (prípadne viacerých žiadateľov) v rámci konzorcia nepotvrdia FSC tohto žiadateľa.

5. Ak sa v iných príslušných predpisoch nestanovuje inak, orgán poskytujúci grant sa v zásade považuje za pôvodcu utajovaných skutočností EÚ vytvorených pri plnení dohody o grante.

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

6. Orgán poskytujúci grant prostredníctvom bezpečnostného orgánu Komisie informuje NSA a/alebo DSA všetkých prijímateľov a subdodávateľov o podpísaní utajovaných dohôd o grante alebo subdodávateľských zmlúv, ako aj o všetkých prípadných predĺženiach či predčasných vypovedaniach takýchto dohôd o grante alebo subdodávateľských zmlúv. Zoznam požiadaviek v jednotlivých krajinách je uvedený v prílohe IV.

7. Dohody o grante zahŕňajúce skutočnosti so stupňom utajenia RESTREINT UE/EU RESTRICTED musia obsahovať bezpečnostnú doložku, ktorou sa prijímatelia zaväzujú dodržiavať ustanovenia dodatku E prílohy III. Súčasťou týchto dohôd o grante 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 musia prijímatelia splniť na akreditáciu svojho CIS, v ktorom sa manipuluje so skutočnosťami so stupňom utajenia RESTREINT UE/EU RESTRICTED.

8. Ak to vyžadujú vnútroštátne právne predpisy členských štátov, NSA a/alebo DSA zabezpečia, aby prijímatelia alebo subdodávatelia spadajúci do ich právomoci spĺňali príslušné bezpečnostné ustanovenia na ochranu skutočností so stupňom utajenia RESTREINT UE/EU RESTRICTED a vykonali overovanie na mieste v priestoroch prijímateľov alebo subdodávateľov umiestnených na ich území. Ak NSA alebo DSA takúto povinnosť nemajú, orgán poskytujúci grant zabezpečí, aby prijímatelia plnili požadované bezpečnostné ustanovenia uvedené v dodatku E prílohy III.

Článok 6

Prístup zamestnancov prijímateľov a subdodávateľov k EUCI

1. Orgán poskytujúci grant zabezpečí, aby utajované dohody o grante obsahovali ustanovenia, na základe ktorých sa zamestnancom prijímateľov alebo subdodávateľov, ktorí na účely plnenia utajovanej dohody o grante alebo subdodávateľskej zmluvy potrebujú prístup k EUCI, takýto prístup poskytne, len ak:

a) sa potvrdilo, že majú potrebu poznať;

b) v prípade skutočností so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo SECRET UE/EU SECRET boli bezpečnostne preverení pre zodpovedajúci stupeň utajenia príslušným NSA alebo DSA alebo iným príslušným bezpečnostným orgánom;

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. V prípade potreby je prístup k EUCI aj v súlade so základným aktom, ktorým sa zriaďuje program, a zohľadňuje všetky ďalšie označenia vymedzené v sprievodcovi stupňami utajenia (SCG).

3. Ak chce prijímateľ alebo subdodávateľ zamestnať 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 prijímateľa alebo subdodávateľa iniciovať postup bezpečnostnej previerky tejto osoby v súlade s vnútroštátnymi právnymi predpismi platnými v mieste, kde sa má prístup k EUCI udeliť.

Článok 7

Prístup expertov zúčastňujúcich sa na kontrolách, preskúmaniach alebo auditoch k EUCI

1. Ak sú externé osoby (ďalej len „experti“) zapojené do kontrol, preskúmaní alebo auditov vykonávaných orgánom poskytujúcim grant alebo do preskúmaní výkonnosti prijímateľov, ktoré si vyžadujú prístup k utajovaným skutočnostiam so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo SECRET UE/EU SECRET, zmluva sa im poskytne len vtedy, ak boli pre zodpovedajúci stupeň utajenia bezpečnostne preverené príslušným NSA alebo DSA alebo akýmkoľvek iným príslušným bezpečnostným orgánom. Orgán poskytujúci grant prostredníctvom bezpečnostného orgánu Komisie skontroluje a v prípade potreby požiada NSA alebo DSA, aby začali proces preverovania expertov aspoň šesť mesiacov pred začiatkom ich príslušných zmlúv.

2. Experti sú pred podpísaním svojich zmlúv poučení o platných bezpečnostných predpisoch a postupoch ochrany EUCI a berú na vedomie svoje povinnosti v súvislosti s ochranou takýchto utajovaných skutočností.

KAPITOLA 4

NÁVŠTEVY VYKONÁVANÉ V SÚVISLOSTI S UTAJOVANÝMI DOHODAMI O GRANTE

Článok 8

Základné zásady

1. Ak orgán poskytujúci grant, experti, prijímatelia alebo subdodávatelia potrebujú v rámci plnenia utajovanej dohody o grante prístup k utajovaným skutočnostiam so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo SECRET UE/EU SECRET v objektoch druhej strany, spoločne organizujú návštevy v spolupráci s NSA alebo DSA alebo akýmikoľvek inými dotknutými príslušnými bezpečnostnými orgánmi.

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

a) návšteva má oficiálny účel súvisiaci s utajovaným grantom;

b) všetci návštevníci musia mať PSC na požadovanom stupni a potrebu poznať príslušné EUCI použité alebo vzniknuté v rámci plnenia utajovaného grantu, aby k nim získali prístup.

Článok 9

Žiadosti o návštevy

1. Návštevy prijímateľov alebo subdodávateľov v zariadeniach iných subdodávateľov alebo v objektoch orgánu poskytujúceho grant, 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 alebo DSA daného zariadenia. Vzor formulára RFV sa uvádza v dodatku C prílohy III;

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

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

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

2. Návštevy úradníkov orgánu poskytujúceho grant alebo expertov či audítorov v zariadeniach prijímateľov alebo subdodávateľov, 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 RFV a predloží ho bezpečnostnému orgánu Komisie;

b) bezpečnostný orgán Komisie potvrdí PSC návštevníka pred tým, než žiadosť o návštevu predloží NSA alebo DSA hostiteľského zariadenia;

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

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

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

4. Platnosť žiadnej žiadosti o návštevu nesmie presiahnuť platnosť PSC návštevníka.

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

Článok 10

Postupy pri návštevách

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

3. Hostiteľské zariadenie zabezpečí uchovávanie záznamov o všetkých návštevníkoch vrátane ich mien, organizácie, ktorú zastupujú, konečného dátumu platnosti 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 11

Návštevy usporiadané priamo

1. V kontexte osobitných projektov sa môžu príslušné NSA alebo DSA a bezpečnostný orgán Komisie dohodnúť na postupe, pri ktorom možno návštevy v rámci konkrétnej utajovanej dohody o grante usporiadať priamo medzi bezpečnostným úradníkom návštevníka a bezpečnostným úradníkom navštevovaného zariadenia. Vzor formulára, ktorý sa na tento účel použije, sa uvádza v dodatku C prílohy III. Tento výnimočný postup sa stanoví v PSI alebo v iných osobitných dojednaniach. V týchto prípadoch sa neuplatňuje článok 9 ani článok 10 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 9 a článku 10 ods. 1.

KAPITOLA 5

PRENOS A PREPRAVA EUCI V RÁMCI PLNENIA UTAJOVANÝCH DOHÔD O GRANTE

Článok 12

Základné zásady

Orgán poskytujúci grant 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 dohody o grante vrátane súhlasu pôvodcu.

Článok 13

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 prijímateľ a ktoré sa používajú na manipuláciu s EUCI v rámci plnenia dohody o grante (ďalej len „prijímateľov CIS“) musí akreditovať zodpovedný bezpečnostný akreditačný orgán (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 bezpečnostné opatrenia TEMPEST podľa článku 36 ods. 6 uvedeného rozhodnutia.

2. Bezpečnostnú akreditáciu prijímateľovho CIS, v ktorom sa manipuluje s EUCI so stupňom utajenia RESTREINT UE/EU RESTRICTED, a všetkých jeho prepojení možno delegovať na bezpečnostného úradníka prijímateľa, ak to povoľujú vnútroštátne právne predpisy. Ak sa táto úloha deleguje, prijímateľ 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 alebo DSA a SAA však majú naďalej zodpovednosť za ochranu skutočností so stupňom utajenia RESTREINT UE/EU RESTRICTED, s ktorými prijímateľ manipuluje, ako aj právo preveriť bezpečnostné opatrenia prijaté prijímateľom. Okrem toho prijímateľ poskytne orgánu poskytujúcemu grant, a ak to vyžadujú vnútroštátne právne predpisy, príslušnému národnému SAA, vyhlásenie o zhode, ktorým potvrdzuje, že prijímateľov CIS a súvisiace prepojenia boli akreditované na manipuláciu s EUCI so stupňom utajenia RESTREINT UE/EU RESTRICTED ([11]).

Článok 14

Preprava komerčnými kuriérmi

Pri preprave utajovaných skutočností EÚ komerčnými kuriérmi sa dodržiavajú príslušné ustanovenia rozhodnutia Komisie (EÚ, Euratom) 2019/1962 ([12]) o vykonávacích predpisoch manipulácie so skutočnosťami so stupňom utajenia RESTREINT UE/EU RESTRICTED a rozhodnutia Komisie (EÚ, Euratom) 2019/1961 ([13]) o vykonávacích predpisoch manipulácie so skutočnosťami so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL a SECRET UE/EU SECRET.

Článok 15

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 prijímateľa v rámci EÚ, pokiaľ sú splnené tieto požiadavky:

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

b) utajované skutočnosti neopustia držbu prepravujúceho;

c) obálka alebo obal sa počas cesty neotvorí.

3. Pri skutočnostiach so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL a SECRET UE/EU SECRET sa osobná preprava zamestnancami prijímateľa 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 referenčnej značky, 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 prepravujúceho;

d) obálka alebo obal sa počas cesty neotvorí;

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

f) kuriér má pri sebe kuriérske osvedčenie vystavené jeho príslušným bezpečnostným orgánom, ktoré ho oprávňuje na prepravu takto označenej utajovanej zásielky.

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

([12]) Rozhodnutie Komisie (EÚ, Euratom) 2019/1962 zo 17. októbra 2019 o vykonávacích predpisoch manipulácie so skutočnosťami so stupňom utajenia RESTREINT UE/EU RESTRICTED (Ú. v. EÚ L 311, 2.12.2019, s. 21).

([13]) Rozhodnutie Komisie (EÚ, Euratom) 2019/1961 zo 17. októbra 2019 o vykonávacích predpisoch manipulácie so skutočnosťami so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL a SECRET UE/EU SECRET (Ú. v. EÚ L 311, 2.12.2019, s. 1).

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

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

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

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

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 alebo DSA, alebo si ich príjemca ponechá k dispozícii na účely monitorovania;

g) ak colné orgány, imigračné orgány alebo hraničná polícia požiadajú o preskúmanie a kontrolu zásielky, povolí sa im otvoriť a prezrieť dostatočnú časť zásielky na to, aby sa presvedčili, že neobsahuje žiaden iný materiál než ten, ktorý sa deklaruje;

h) colné orgány by mali byť vyzvané k rešpektovaniu úradnej povahy 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 prijímateľa do tretej krajiny alebo medzinárodnej organizácie podlieha ustanoveniam dohody o bezpečnosti utajovaných skutočností, resp. správneho dojednania, ktoré s danou treťou krajinou alebo medzinárodnou organizáciou uzatvorila Únia, resp. Komisia.

KAPITOLA 6

PLÁNOVANIE KONTINUITY ČINNOSTÍ

Článok 16

Pohotovostné plány a nápravné opatrenia

Orgán poskytujúci grant zabezpečí, aby sa v utajovanej dohode o grante uvádzala povinnosť prijímateľov stanoviť pohotovostné plány (business contingency plans – BCP) na ochranu EUCI, s ktorými sa v rámci plnenia utajovaného grantu 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. Prijímatelia potvrdia orgánu poskytujúcemu grant, že ich BCP sú zavedené.

Článok 17

Nadobudnutie účinnosti

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

V Bruseli 10. februára 2021

Za Komisiu
v mene predsedníčky
Johannes HAHN
člen Komisie

PRÍLOHA I

ŠTANDARDNÉ INFORMÁCIE VO VÝZVE NA PREDKLADANIE NÁVRHOV

(prispôsobiť použitej výzve)

Bezpečnosť

Projekty zahŕňajúce utajované skutočnosti EÚ musia prejsť bezpečnostnou previerkou, aby sa povolilo ich financovanie, a môžu podliehať osobitným bezpečnostným predpisom [podrobnosti v bezpečnostnej doložke (SAL), ktorá je pripojená k dohode o grante].

V týchto pravidlách [na ktoré sa vzťahuje rozhodnutie Komisie (EÚ, Euratom) 2015/444 ([1]) a/alebo vnútroštátne predpisy] sa napríklad stanovuje, že:

— projekty zahŕňajúce skutočnosti so stupňom utajenia TRES SECRET UE/EU TOP SECRET (alebo s rovnocenným stupňom utajenia) **NEMOŽNO** financovať,

— utajované skutočnosti musia byť označené v súlade s platnými bezpečnostnými pokynmi uvedenými v SAL,

— skutočnosti so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo vyšším (a so stupňom utajenia RESTREINT UE/EU RESTRICTED, ak sa to vyžaduje vo vnútroštátnych predpisoch):

  — môžu byť vytvorené alebo sprístupnené iba v objektoch, kde príslušný národný bezpečnostný orgán (NSA) preveril priemyselnú bezpečnosť v súlade s vnútroštátnymi predpismi,

  — môže sa s nimi manipulovať iba v zabezpečenom priestore, ktorý akreditoval príslušný NSA,

  — môžu k nim mať prístup a manipulovať s nimi len osoby s platnou personálnou bezpečnostnou previerkou (PSC) a potrebou poznať,

— na konci grantu sa utajované skutočnosti musia vrátiť, alebo naďalej chrániť v súlade s platnými pravidlami,

— na úkony zahŕňajúce utajované skutočnosti EÚ (EUCI) možno využiť subdodávateľov len na základe predchádzajúceho písomného súhlasu orgánu poskytujúceho grant a len subjekty usadené v členskom štáte EÚ alebo v tretej krajine, ktoré s EÚ uzavreli dohodu o bezpečnosti utajovaných skutočností (alebo správne dojednanie s Komisiou),

— sprístupnenie EUCI tretím stranám podlieha predchádzajúcemu písomnému súhlasu orgánu poskytujúceho grant.

Upozorňujeme, že v závislosti od druhu činnosti môže byť pred podpisom grantu potrebné vykonať priemyselnú bezpečnostnú previerku. Orgán poskytujúci grant posúdi v každom prípade potrebu previerok a stanoví dátum ich vykonania počas prípravy grantu. Upozorňujeme, že za **žiadnych okolností** nemôžeme podpísať žiadnu dohodu o grante, pokiaľ aspoň jeden z prijímateľov v konzorciu nemá priemyselnú bezpečnostnú previerku.

Do dohody o grante sa môžu doplniť ďalšie bezpečnostné odporúčania vo forme bezpečnostných výstupov (*napr. vytvoriť poradnú skupinu pre bezpečnosť, obmedziť úroveň podrobnosti, použiť falošný scenár, vylúčiť použitie utajovaných skutočností atď.*).

Prijímatelia musia zabezpečiť, aby ich projekty nepodliehali vnútroštátnym bezpečnostným požiadavkám/bezpečnostným požiadavkám tretej krajiny, ktoré by mohli ovplyvniť plnenie alebo spochybniť udelenie grantu (*napr. technologické obmedzenia, národná bezpečnostná klasifikácia atď.*). Orgán poskytujúci grant musí byť okamžite informovaný o akýchkoľvek potenciálnych bezpečnostných otázkach.

[dodatočná OPCIA pre žiadosti o rámcové partnerstvo: V prípade rámcových partnerstiev sa žiadosti o rámcové partnerstvo aj žiadosti o grant môžu podrobiť bezpečnostnej previerke.]

([1]) Pozri rozhodnutie Komisie (EÚ, Euratom) 2015/444 z 13. marca 2015 o bezpečnostných predpisoch na ochranu utajovaných skutočností EÚ (Ú. v. EÚ L 72, 17.3.2015, s. 53).

PRÍLOHA II

ŠTANDARDNÉ DOLOŽKY DOHODY O GRANTE

(prispôsobiť použitej dohode o grante)

13.2. Bezpečnosť – utajované skutočnosti

Zmluvné strany musia manipulovať s utajovanými skutočnosťami (EÚ alebo vnútroštátnymi) v súlade s platnými právnymi predpismi EÚ alebo vnútroštátnymi právnymi predpismi o utajovaných skutočnostiach [najmä rozhodnutie Komisie (EÚ, Euratom) 2015/444 ([1]) a jeho vykonávacie predpisy].

Osobitné bezpečnostné predpisy (ak existujú) sa uvádzajú v prílohe 5.

PRÍLOHA 5

Bezpečnosť – utajované skutočnosti EÚ

[OPCIA pre úkony s utajovanými skutočnosťami EÚ (štandard): Ak sa pri úkone používajú alebo tvoria utajované skutočnosti EÚ, s takýmito skutočnosťami treba až do zrušenia ich utajenia zaobchádzať v súlade so sprievodcom stupňami utajenia (SCG) a s bezpečnostnou doložkou (SAL) uvedených v prílohe 1, ako aj v súlade s rozhodnutím (EÚ, Euratom) 2015/444 a jeho vykonávacími predpismi.

Výstupy zahŕňajúce utajované skutočnosti EÚ sa musia odovzdať v súlade s osobitnými postupmi dohodnutými s orgánom poskytujúcim grant.

Na úkony zahŕňajúce utajované skutočnosti EÚ možno využiť subdodávateľov len na základe predchádzajúceho písomného súhlasu orgánu poskytujúceho grant a len subjekty usadené v členskom štáte EÚ alebo tretej krajine, ktoré s EÚ uzavreli dohodu o bezpečnosti utajovaných skutočností (alebo správne dojednanie s Komisiou).

Utajované skutočnosti EÚ nemožno sprístupniť žiadnej tretej strane (vrátane účastníkov zapojených do vykonávania úkonu) bez predchádzajúceho výslovného písomného súhlasu orgánu poskytujúceho grant.]

([1]) Rozhodnutie Komisie (EÚ, Euratom) 2015/444 z 13. marca 2015 o bezpečnostných predpisoch na ochranu utajovaných skutočností EÚ (Ú. v. EÚ L 72, 17.3.2015, s. 53).

PRÍLOHA III

[Príloha IV (k .....)]

BEZPEČNOSTNÁ DOLOŽKA (SAL) [1]

[Vzor]

[1] Tento vzor SAL sa uplatňuje, ak sa Komisia považuje za pôvodcu utajovaných skutočností, ktoré boli vytvorené a s ktorými sa manipulovalo na účely plnenia dohody o grante. Ak pôvodcom utajovaných skutočností, ktoré boli vytvorené a s ktorými sa manipuluje na účely plnenia dohody o grante, nie je Komisia, a ak členské štáty, ktoré sa zúčastňujú na grante, zriadili osobitný bezpečnostný rámec, môžu sa uplatniť iné vzory SAL.

Dodatok A

BEZPEČNOSTNÉ POŽIADAVKY

Orgán poskytujúci grant musí v bezpečnostnej doložke (SAL) uviesť nasledujúce bezpečnostné požiadavky. Niektoré ustanovenia sa na danú dohodu o grante nemusia vzťahovať. Tie sú uvedené v hranatých zátvorkách.

Zoznam ustanovení nie je úplný. V závislosti od povahy utajovaného grantu možno pridať ďalšie ustanovenia.

VŠEOBECNÉ PODMIENKY [*Pozn.: uplatniteľné na všetky utajované dohody o grante*]

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

2. Na prijímateľov grantu sa vzťahujú všetky povinnosti stanovené v rozhodnutí Komisie (EÚ, Euratom) 2015/444 ([2]) (ďalej len „RK 2015/444“) a jeho vykonávacích predpisoch ([3]). Ak prijímateľ grantu čelí problému s uplatňovaním platného právneho rámca v členskom štáte, musí sa obrátiť na bezpečnostný orgán Komisie a národný bezpečnostný orgán (NSA) alebo určený bezpečnostný orgán (DSA).

3. Utajované skutočnosti vzniknuté pri plnení dohody o grante treba označiť ako utajované skutočnosti EÚ (EUCI) so stupňom utajenia podľa sprievodcu stupňami utajenia (SCG) v dodatku B k tejto doložke. Odchýlenie sa od stupňa utajenia uvedeného v SCG je možné iba na základe písomného schválenia orgánu poskytujúceho grant.

4. Práva pôvodcu ku všetkým EUCI, ktoré vznikli a s ktorými sa manipuluje na účely plnenia utajovanej dohody o grante, si uplatňuje Komisia ako orgán poskytujúci grant.

5. Bez písomného súhlasu orgánu poskytujúceho grant nesmie prijímateľ ani subdodávateľ použiť žiadne skutočnosti či veci dodané orgánom poskytujúcim grant alebo vytvorené v mene uvedeného orgánu na žiaden iný účel, než je plnenie dohody o grante.

6. Ak sa na plnenie dohody o grante vyžaduje bezpečnostná previerka zariadenia (FSC), prijímateľ musí požiadať orgán poskytujúci grant, aby prikročil k vybaveniu žiadosti o FSC.

7. Prijímateľ musí vyšetriť všetky narušenia bezpečnosti súvisiace s EUCI a čo najskôr ich nahlásiť orgánu poskytujúcemu grant. Prijímateľ alebo subdodávateľ musia bezodkladne oznámiť svojmu NSA alebo DSA, a ak to umožňujú vnútroštátne právne predpisy, aj bezpečnostnému orgánu Komisie všetky prípady, v ktorých je známe alebo existuje dôvod domnievať sa, že EUCI poskytnuté alebo vzniknuté v rámci dohody o grante sa stratili alebo boli sprístupnené nepovolaným osobám.

([2]) Rozhodnutie Komisie (EÚ, Euratom) 2015/444 z 13. marca 2015 o bezpečnostných predpisoch na ochranu utajovaných skutočností EÚ (Ú. v. EÚ L 72, 17.3.2015, s. 53).

([3]) Orgán poskytujúci grant by mal po prijatí vykonávacích predpisov doplniť odkazy.

8. Po skončení dohody o grante musí prijímateľ alebo subdodávateľ bezodkladne vrátiť všetky EUCI, ktoré má v držbe, orgánu poskytujúcemu grant. Ak je to možné, prijímateľ alebo subdodávateľ môžu EUCI namiesto vrátenia zničiť. Treba tak urobiť v súlade s vnútroštátnymi právnymi predpismi krajiny, v ktorej je prijímateľ usadený, na základe predchádzajúceho súhlasu bezpečnostného orgánu Komisie a podľa jeho pokynov. EUCI treba zničiť tak, aby sa nedali vcelku ani čiastočne obnoviť.

9. Ak majú prijímateľ alebo subdodávateľ povolenie ponechať si EUCI po vypovedaní alebo uzavretí dohody o grante, tieto EUCI musia byť naďalej chránené v súlade s RK 2015/444 a jeho vykonávacími predpismi ([4]).

10. 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 prijímateľa, ktoré sa používajú na manipuláciu s EUCI na účely plnenia dohody o grante (ďalej len „prijímateľov CIS“) musia byť akreditované ([5]), že všetky elektronické prenosy EUCI musia byť zabezpečené kryptografickými produktmi schválenými v súlade s článkom 36 ods. 4 RK 2015/444 a že treba vykonávať bezpečnostné opatrenia TEMPEST v súlade s článkom 36 ods. 6 RK 2015/444.

11. Prijímateľ alebo subdodávateľ musia mať zavedené pohotovostné plány (BCP) na ochranu všetkých EUCI, s ktorými sa v rámci plnenia utajovanej dohody o grante manipuluje, počas núdzových situácií, a musia mať zavedené preventívne a nápravné opatrenia na minimalizáciu vplyvu incidentov súvisiacich s manipuláciou s EUCI a s ich uchovávaním. Prijímateľ alebo subdodávateľ o svojich BCP informujú orgán poskytujúci grant.

DOHODY O GRANTE, KTORÉ SI VYŽADUJÚ PRÍSTUP KU SKUTOČNOSTIAM SO STUPŇOM UTAJENIA RESTREINT UE/EU RESTRICTED

12. V zásade sa na súlad s dohodou o grante nevyžaduje personálna bezpečnostná previerka (PSC) ([6]). Ku skutočnostiam alebo k veciam so stupňom utajenia RESTREINT UE/EU RESTRICTED však smú mať prístup iba zamestnanci prijímateľa, ktorí takéto skutočnosti potrebujú na plnenie dohody o grante (*potreba poznať*), ktorých bezpečnostný úradník prijímateľa poučil o ich povinnostiach a dôsledkoch akéhokoľvek ohrozenia či narušenia bezpečnosti takýchto skutočností a ktorí písomne vzali na vedomie dôsledky zlyhania pri ochrane EUCI.

13. Bez písomného súhlasu orgánu poskytujúceho grant nesmie prijímateľ 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.

14. Prijímateľ alebo subdodávateľ musia zachovať označenia stupňa utajenia utajovaných skutočností vzniknutých alebo poskytnutých v rámci plnenia dohody o grante a nesmú zrušiť utajenie skutočnosti bez písomného súhlasu orgánu poskytujúceho grant.

15. 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 prepravujúceho a nesmú sa počas cesty otvoriť.

([4]) Orgán poskytujúci grant by mal po prijatí vykonávacích predpisov doplniť odkazy.

([5]) Strana, ktorá podstupuje certifikáciu, musí poskytnúť udeľujúcemu orgánu vyhlásenie o zhode, a to prostredníctvom bezpečnostného orgánu Komisie a v koordinácii s príslušným národným bezpečnostným akreditačným orgánom (SAA).

([6]) Ak prijímatelia pochádzajú z členských štátov, ktoré vyžadujú PSC a/alebo FSC pre granty so stupňom utajenia RESTREINT UE/EU RESTRICTED, orgán poskytujúci grant uvedie v SAL tieto požiadavky PSC a FSC pre dotknutých prijímateľov.

16. Prijímateľ alebo subdodávateľ môžu doručovať dokumenty so stupňom utajenia RESTREINT UE/EU RESTRICTED orgánu poskytujúcemu grant s využitím komerčných kuriérskych spoločností, poštových služieb, osobne alebo elektronicky. Na tento účel sa prijímateľ alebo subdodávateľ držia bezpečnostných pokynov pre program (alebo projekt) (PSI), ktoré vydala Komisia, a/alebo jej vykonávacích predpisov pre oblasť priemyselnej bezpečnosti v súvislosti s utajovanými grantmi ([7]).

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

18. Bezpečnostnú certifikáciu prijímateľovho CIS, v ktorom sa manipuluje s EUCI so stupňom utajenia RESTREINT UE/EU RESTRICTED, a všetkých jeho prepojení možno delegovať na bezpečnostného úradníka prijímateľa, ak to povoľujú vnútroštátne právne predpisy. V prípade takéhoto delegovania certifikácie majú príslušné NSA, DSA a orgány bezpečnostnej certifikácie (SAA) naďalej zodpovednosť za ochranu skutočností so stupňom utajenia RESTREINT UE/EU RESTRICTED, s ktorými prijímateľ manipuluje, ako aj právo preveriť bezpečnostné opatrenia prijaté prijímateľom. Okrem toho prijímateľ poskytne orgánu poskytujúcemu grant, a ak to vyžadujú vnútroštátne právne predpisy, príslušnému národnému SAA vyhlásenie o zhode, ktorým potvrdzuje, že prijímateľov CIS a súvisiace prepojenia boli akreditované 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)

19. 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 PRIJÍMATEĽ UZATVÁRAŤ SUBDODÁVATEĽSKÉ ZMLUVY

20. Prijímateľ musí získať povolenie od orgánu poskytujúceho grant skôr, ako zadá ktorúkoľvek časť utajovanej dohody o grante subdodávateľom.

21. Žiadna subdodávateľská zmluva sa nesmie uzatvoriť so subjektom registrovaným v tretej krajine ani so subjektom patriacim medzinárodnej organizácii, pokiaľ daná tretia krajina alebo medzinárodná organizácia nemá s EÚ uzatvorenú dohodu o bezpečnosti utajovaných skutočností alebo správne dojednanie s Komisiou.

22. Ak prijímateľ uzatvoril subdodávateľskú zmluvu, bezpečnostné ustanovenia dohody o grante platia *mutatis mutandis* aj pre subdodávateľa a jeho zamestnancov. V takom prípade je zodpovednosťou prijímateľa zabezpečiť, aby všetci subdodávatelia uplatňovali tieto zásady na svoje vlastné subdodávateľské dohody. Na zaistenie primeraného bezpečnostného dohľadu musí bezpečnostný orgán Komisie informovať NSA a/alebo DSA prijímateľa a subdodávateľa o uzavretí všetkých súvisiacich utajovaných subdodávateľských zmlúv na stupni utajenia CONFIDENTIEL UE/EU CONFIDENTIAL a SECRET UE/EU SECRET. Orgánom NSA a/alebo DSA prijímateľa a subdodávateľa sa podľa potreby poskytne kópia osobitných bezpečnostných ustanovení danej subdodávateľskej zmluvy. Zoznam NSA a DSA, ktoré vyžadujú informovanie o bezpečnostných ustanoveniach utajovaných dohôd o grante so stupňom utajenia RESTREINT UE/EU RESTRICTED, je uvedený v prílohe k vykonávacím predpisom Komisie pre oblasť priemyselnej bezpečnosti v súvislosti s utajovanými dohodami o grante ([8]).

23. Prijímateľ nesmie poskytnúť žiadne EUCI subdodávateľovi bez predchádzajúceho písomného súhlasu orgánu poskytujúceho grant. Ak sa majú EUCI subdodávateľom zasielať často alebo rutinne, orgán poskytujúci grant môže udeliť súhlas na určené časové obdobie (napr. 12 mesiacov) alebo na trvanie subdodávateľskej zmluvy.

([7]) Orgán poskytujúci grant by mal po prijatí vykonávacích predpisov doplniť odkazy.
([8]) Orgán poskytujúci grant by mal po prijatí vykonávacích predpisov doplniť odkazy.

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, orgán poskytujúci grant musí zahrnúť body 24, 25 a 26 a vymazať bod 27. Ak sa návštevy zahŕňajúce skutočnosti so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo SECRET UE/EU SECRET organizujú priamo medzi vysielajúcimi a prijímajúcimi subjektmi, orgán poskytujúci grant musí vymazať body 25 a 26 a zahrnúť len bod 27.

24. Návštevy zahŕňajúce prístup alebo potenciálny prístup ku skutočnostiam so stupňom utajenia RESTREINT UE/EU RESTRICTED sa usporadúvajú priamo medzi vysielajúcimi a prijímajúcimi subjektmi bez potreby dodržiavať postup opísaný ďalej v bodoch 25 až 27.

[25. 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 národnému bezpečnostnému orgánu alebo určenému bezpečnostnému orgánu daného zariadenia;

b) NSA alebo DSA vysielajúceho zariadenia musia potvrdiť PSC návštevníka pred tým, než žiadosť o návštevu predložia národnému bezpečnostnému orgánu alebo určenému bezpečnostnému orgánu hostiteľského zariadenia (alebo bezpečnostnému orgánu Komisie, ak ide o návštevu objektu orgánu poskytujúceho grant);

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

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

[26. 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 alebo DSA.]

[27. 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).]

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

29. 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

30. Bezpečnostný orgán Komisie môže v spolupráci s príslušnými NSA alebo DSA navštíviť zariadenia prijímateľov alebo subdodávateľov, aby skontroloval, či sú splnené bezpečnostné požiadavky na manipuláciu s EUCI.

SPRIEVODCA STUPŇAMI UTAJENIA

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

Dodatok B

SPRIEVODCA STUPŇAMI UTAJENIA

[konkrétny text upraviť v závislosti od predmetu dohody o grante]

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-mailovú adresu 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 ([9]).

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

([9]) 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.

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:

SIGNATURE:

STAMP

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 ([10])>

([10]) 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 ([11])>

([11]) 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 ([12])>

([12]) 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 PRIEMYSELNEJ BEZPEČNOSTNEJ PREVIERKY (FSCIS) (VZOR)

1. **ÚVOD**

1.1. Pripojený je príklad informačného listu priemyselnej bezpečnostnej previerky (FSCIS) na rýchlu výmenu informácií medzi národným bezpečnostným orgánom (NSA) alebo určeným bezpečnostným orgánom (DSA), inými príslušnými národnými bezpečnostnými orgánmi a bezpečnostným orgánom Komisie (konajúcim v mene orgánov poskytujúcich grant) o priemyselnej bezpečnostnej previerke (FSC) zariadenia, ktoré je súčasťou žiadosti o utajované granty alebo subdodávateľské zmluvy a zúčastňuje sa na ich plnení.

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

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

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 udeľoval grant či subdodávateľská zmluva, treba o tom informovať vystavujúci NSA alebo DSA.

Postupy a pokyny na používanie informačného listu priemyselnej bezpečnostnej previerky (FSCIS)

Tieto podrobné pokyny sú pre NSA, DSA alebo orgán poskytujúci grant a bezpečnostný orgán Komisie, ktoré FSCIS vypĺňajú. Žiadosť treba prednostne vyplniť veľkými písmenami.

ZÁHLAVIE	Žiadateľ vyplní celý názov NSA/DSA a krajiny.
1. **DRUH ŽIADOSTI**	Žiadajúci orgán poskytujúci grant 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 výzvy na predkladanie návrhov alebo grantu. Uveďte potrebnú kapacitu na uchovávanie, stupeň utajenia v danom CIS atď. Mali by sa uviesť aj všetky prípadné dátumy konečných termínov/lehôt/udelenia grantu, ktoré majú vplyv na dokončenie FSC.

4. **ŽIADAJÚCI NSA/DSA**	Uveďte názov skutočného žiadateľa (v mene NSA/DSA) a dátum žiadosti v číselnom formáte (dd/mm/rrrr).
5. **ODDIEL PRE 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 prijímateľ či subdodávateľ.
6. **POZNÁMKY**	Možno použiť na dodatočné informácie vzhľadom na FSC, zariadenie alebo uvedené položky.
7. **VYSTAVUJÚCI NSA/DSA**	Uveďte názov poskytujúceho orgánu (v mene NSA/DSA) a dátum odpovede v číselnom formáte (dd/mm/rrrr).

INFORMAČNÝ LIST PRIEMYSELNEJ BEZPEČNOSTNEJ PREVIERKY (FSCIS) (VZOR)

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

ŽIADOSŤ O UISTENIE O PRIEMYSELNEJ BEZPEČNOSTNEJ PREVIERKE

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 prijímateľa alebo subdodávateľa – postup 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.)	
……	……
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), grante alebo subdodávateľskej zmluve, programe/projekte atď.]

……

Žiadajúci NSA/DSA/udeľujúci orgán: Meno: …… Dátum: (dd/mm/rrrr) ……

ODPOVEĎ (do desiatich 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 akreditovaný/schválený 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 Meno: ..... *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 ([13])>

([13]) 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 prijímateľovom CIS

Všeobecné ustanovenia

1. Prijímateľ 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 odporúča orgán poskytujúci grant alebo prípadne národný bezpečnostný orgán (NSA) alebo určený bezpečnostný orgán (DSA).

2. Je zodpovednosťou prijímateľa plniť 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 kľúčov, CD, SD kariet atď.

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

5. Prijímateľ musí zriadiť 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 prijímateľa na uchovávanie alebo spracovanie skutočností so stupňom utajenia RESTREINT UE/EU RESTRICTED nie je povolené.

7. Certifikáciu prijímateľovho CIS, v ktorom sa manipuluje so skutočnosťami so stupňom utajenia RESTREINT UE/EU RESTRICTED, musí schváliť bezpečnostný akreditačný orgán (SAA) dotknutého členského štátu alebo sa deleguje na prijímateľovho 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 dohody o grante 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 orgánu poskytujúceho grant a alebo príslušného NSA, DSA alebo SAA musí prijímateľ doložiť súlad s bezpečnostnou doložkou zmluvy o grante. Ak sa vyžiada aj audit a kontrola postupov a zariadení prijímateľa na zaistenie súladu s týmito požiadavkami, prijímatelia musia povoliť zástupcom orgánu poskytujúceho grant, NSA, DSA a/alebo 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 sa vykonávať 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 prijímateľovmu CIS, v ktorom sa manipuluje s EUCI, sa povolí striktne na základe potreby poznať a iba oprávneným zamestnancom.

14. Pri všetkých CIS sa vedú aktualizované zoznamy 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 „špeciálne“ znaky (ak to systém umožňuje), ako aj písmená. Heslá sa musia meniť aspoň raz za 180 dní. Ak boli narušené alebo sprístupnené neoprávnenej osobe alebo ak existuje podozrenie z takéhoto narušenia alebo sprístupnenia, musia sa čo najskôr zmeniť.

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 ich úprave, alebo v zmene systémových a bezpečnostných nastavení. Používatelia musia byť automaticky odhlásení z CIS, ak ich zariadenie nie je aktívne určitý vopred stanovený časový interval, alebo CIS musí po 15 minútach nečinnosti 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 povinnosťami a s postupmi, ktoré treba dodržať na ochranu skutočností so stupňom utajenia RESTREINT UE/EU RESTRICTED v danom CIS. Povinnosti a postupy, ktoré sa majú dodržať, sa zdokumentujú a používatelia ich písomne potvrdia.

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

Záznamy, audit a reakcia na incidenty

20. Každý prístup do CIS sa musí 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) vytvorenie, 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. Prijímateľ musí mať zavedenú stratégiu riešenia bezpečnostných incidentov. Používatelia a správcovia musia byť zaškolení, 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 orgánu poskytujúcemu grant. 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 prijímateľov CIS, v ktorom sa manipuluje so skutočnosťami so stupňom utajenia RESTREINT UE/EU RESTRICTED, prepojený s CIS, ktorý nie je akreditovaný, 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 prijímateľa alebo subdodávateľa. V takom prípade musí prijímateľ vykonať vyhodnotenie rizika s cieľom identifikovať dodatočné bezpečnostné požiadavky, ktoré treba implementovať v rámci procesu bezpečnostnej akreditácie. Prijímateľ predloží orgánu poskytujúcemu grant, a ak to vyžadujú vnútroštátne právne predpisy, príslušnému SAA vyhlásenie o zhode, ktorým potvrdzuje, že prijímateľov CIS a súvisiace prepojenia boli akreditované 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 orgán poskytujúci grant, 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. Prijímateľov bezpečnostný úradník musí vykonať kontroly konfigurácie hardvéru a softvéru s cieľom uistiť sa, že nebol zavedený žiaden nepovolený hardvér ani softvér.

30. Zmeny konfigurácie prijímateľovho CIS treba posúdiť z hľadiska dôsledkov pre bezpečnosť 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 akceptovanú priemyselnú normu.

32. Prijímateľ 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.

Sanitizácia 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 ich likvidáciou vykonať na celom systéme alebo pamäťovom médiu tieto sanitizačné 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 obnoviť, 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 orgánom poskytujúcim grant alebo v náležitých prípadoch s NSA, DSA alebo 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

Priemyselná bezpečnostná previerka a personálna bezpečnostná previerka prijímateľov, ktorých práca zahŕňa skutočnosti so stupňom utajenia RESTREINT UE/EU RESTRICTED, a národné bezpečnostné orgány/určené bezpečnostné orgány, ktoré vyžadujú oznamovanie utajovaných dohôd o grante so stupňom utajenia RESTREINT UE/EU RESTRICTED ([1])

Členský štát	FSC		Oznamovanie dohody o grante alebo subdodávateľskej zmluvy zahŕňajúcej skutočnosti so stupňom utajenia R-UE/EU-R národnému bezpečnostnému orgánu a/alebo určenému bezpečnostnému orgánu		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**
Litva	**X**		**X**			**X**
Luxembursko	**X**		**X**		**X**	
Maďarsko		**X**		**X**		**X**
Malta		**X**		**X**		**X**
Holandsko	**X** (iba pri dohodách o grante a subdodávateľských zmluvách v rezorte obrany)		**X** (iba pri dohodách o grante a subdodávateľských zmluvách v rezorte obrany)			**X**
Rakúsko		**X**		**X**		**X**
Poľsko		**X**		**X**		**X**

([1]) Týmito vnútroštátnymi požiadavkami na FSC/PSC a oznamovanie pri dohodách o grant zahŕňajúcich skutočnosti so stupňom utajenia RESTREINT UE/EU RESTRICTED sa nesmú ukladať žiadne dodatočné povinnosti iným členským štátom alebo prijímateľom a subdodávateľom spadajúcim do ich právomoci.
Pozn.: Oznamovanie dohôd o grante zahŕňajúcich skutočnosti so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL a SECRET UE/EU SECRET je povinné.

Portugalsko		**X**		**X**		**X**
Rumunsko		**X**		**X**		**X**
Slovinsko	**X**		**X**			**X**
Slovensko	**X**		**X**			**X**
Fínsko		**X**		**X**		**X**
Švédsko		**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

Email: 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
   Email: 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
   Email: office@iksbg.org

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

4. State Agency for Technical Operations (security service)
   29 Shesti Septemvri Street
   1000 Sofia
   Tel.: +359 29824971
   Fax: +359 29461339
   Email: 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

   Email: 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 utajovanej dohody o grante alebo plnia utajovanú zmluvu alebo utajovanú dohodu o grante.)

ČESKO

National Security Authority
Industrial Security Department
PO BOX 49
150 06 Praha 56

Tel.: +420 257283129

Email: 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 prepravy (okrem kryptografie/CCI):
   Federal Ministry for Economic Affairs and Energy

   Industrial Security Division - RS3

   Villemombler Str. 76

   53123 Bonn

   Tel.: +49 228996154028

   Fax: +49 228996152676

   Email: dsagermany-rs3@bmwi.bund.de (office email address)

2. Štandardné žiadosti o návštevy od nemeckých spoločností a v nemeckých spoločnostiach:

Federal Ministry for Economic Affairs and Energy

Industrial Security Division – RS2
Villemombler Str. 76
53123 Bonn

Tel.: +49 228996152401

Fax: +49 228996152603

Email: rs2-international@bmwi.bund.de (office email 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

Email: NDAEU@bsi.bund.de

ESTÓNSKO

National Security Authority Department
Estonian Foreign Intelligence Service
Rahumäe tee 4B
11316 Tallinn

Tel.: +372 6939211

Fax: +372 6935001

Email: 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

Email: 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

Email: daa.industrial@hndgs.mil.gr

ŠPANIELSKO

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Calle Argentona 30
28023 Madrid

Tel.: +34 912832583, +34 912832752, +34 913725928

Fax: +34 913725808

Email: nsa-sp@areatec.com

Informácie týkajúce sa utajovaných programov: programas.ons@areatec.com

V otázkach personálnych bezpečnostných previerok: hps.ons@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

Email: 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

Email: 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

Email: 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

Email: 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

Email: 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

Email: ndi@sab.gov.lv, 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
Pilaitės pr. 19
LT-06264 Vilnius

Tel.: +370 70666128

Email: nsa@vsd.lt

LUXEMBURSKO

Autorité Nationale de Sécurité
207, route d'Esch
L-1471 Luxembourg

Tel.: +352 24782210

Email: 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

Email: 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

Email: 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

   Email: 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

   Email: indussec@mindef.nl

RAKÚSKO

1. Federal Chancellery of Austria

   Department I/10, Federal Office for Information Security

   Ballhausplatz 2
   10104 Vienna

   Tel.: +43 153115202594

   Email: isk@bka.gv.at

2. DSA in the military sphere:

   BMLV/Abwehramt

   Postfach 2000
   1030 Vienna

   Email: 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

Email: 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

Email: 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

Email: 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

Email: gp.uvtp@gov.si

SLOVENSKO

Národný bezpečnostný úrad
Odbor bezpečnostných previerok
Budatínska 30
851 06 Bratislava

Tel.: +421 268691111

Fax: +421 268691700

Email: podatelna@nbu.gov.sk

FÍNSKO

National Security Authority
Ministry for Foreign Affairs
P.O. Box 453
FI-00023 Government

Email: 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
   Email: ud-nsa@gov.se

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