ROZHODNUTÍ KOMISE (EU, Euratom) 2019/1963

ze dne 17. října 2019,

kterým se stanoví prováděcí pravidla pro průmyslovou bezpečnost s ohledem na utajované veřejné zakázky

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie, a zejména na článek 249 této smlouvy,

s ohledem na Smlouvu o založení Evropského společenství pro atomovou energii, a zejména na článek 106 této smlouvy,

s ohledem na rozhodnutí Komise (EU, Euratom) 2015/443 ze dne 13. března 2015 o bezpečnosti v Komisi ([1]),

s ohledem na rozhodnutí Komise (EU, Euratom) 2015/444 ze dne 13. března 2015 o bezpečnostních pravidlech na ochranu utajovaných informací EU ([2]),

s ohledem na rozhodnutí Komise (EU, Euratom) 2017/46 ze dne 10. ledna 2017 o bezpečnosti komunikačních a informačních systémů v Evropské komisi ([3]),

po konzultaci se skupinou odborníků pro bezpečnost v Komisi v souladu s čl. 41 odst. 5 rozhodnutí (EU, Euratom) 2015/444,

vzhledem k těmto důvodům:

(1) Články 41, 42, 47 a 48 rozhodnutí (EU, Euratom) 2015/444 stanoví, že v prováděcích pravidlech pro průmyslovou bezpečnost musí být stanovena podrobnější ustanovení pro doplnění a podporu kapitoly 6 uvedeného rozhodnutí, která budou řídit otázky, jako jsou nabídková řízení, uzavírání utajovaných smluv, bezpečnostní prověrky zařízení, bezpečnostní prověrky personálu, návštěvy a přenos a přeprava utajovaných informací Evropské unie.

(2) Rozhodnutí (EU, Euratom) 2015/444 uvádí, že utajované smlouvy mají být prováděny v úzké spolupráci s vnitrostátním bezpečnostním orgánem, určeným bezpečnostním orgánem nebo jakýmkoli jiným příslušným orgánem dotyčných členských států; členské státy souhlasily, že zajistí, aby jakýkoli subjekt podléhající jejich pravomoci, který může obdržet nebo vypracovat utajované informace pocházející z Komise, byl náležitě bezpečnostně prověřen a byl schopen poskytovat vhodnou ochranu rovnocennou ochraně poskytované bezpečnostními pravidly Rady Evropské unie na ochranu utajovaných informací EU, které nesou odpovídající označení stupně utajení, jak jsou uvedena v dohodě mezi členskými státy Evropské unie zasedajícími v Radě o ochraně utajovaných informací vyměňovaných v zájmu Evropské unie (2011/C 202/05) ([4]).

(3) Rada, Komise a vysoká představitelka Unie pro zahraniční věci a bezpečnostní politiku se dohodly, že zajistí maximální důslednost při uplatňování bezpečnostních pravidel pro jejich ochranu utajovaných informací EU, a současně zohlední své zvláštní institucionální a organizační potřeby v souladu s prohlášeními připojenými k zápisu ze zasedání Rady, na němž bylo přijato rozhodnutí Rady 2013/488/EU ([5]) o bezpečnostních pravidlech na ochranu utajovaných informací EU.

(4) Prováděcí pravidla Komise pro průmyslovou bezpečnost s ohledem na utajované smlouvy by tedy rovněž měla zajistit maximální důslednost a zohlednit pokyny v oblasti průmyslové bezpečnosti schválené Bezpečnostním výborem Rady dne 13. prosince 2016 a články 7 a 22 směrnice Evropského parlamentu a Rady 2009/81/ES ([6]).

(5) Dne 4. května 2016 Komise přijala rozhodnutí ([7]), které zmocňuje člena Komise odpovědného za bezpečnostní otázky přijímat jménem Komise a na její odpovědnost prováděcí pravidla stanovená v článku 60 rozhodnutí (EU, Euratom) 2015/444,

([1]) Úř. věst. L 72, 17.3.2015, s. 41.
([2]) Úř. věst. L 72, 17.3.2015, s. 53.
([3]) Úř. věst. L 6, 11.1.2017, s. 40.
([4]) Úř. věst. C 202, 8.7.2011, s. 13.
([5]) Rozhodnutí Rady 2013/488/EU ze dne 23. září 2013 o bezpečnostních pravidlech na ochranu utajovaných informací EU (Úř. věst. L 274, 15.10.2013, s. 1).
([6]) Směrnice Evropského parlamentu a Rady 2009/81/ES ze dne 13. července 2009 o koordinaci postupů při zadávání některých zakázek na stavební práce, dodávky a služby zadavateli v oblasti obrany a bezpečnosti (Úř. věst. L 216, 20.8.2009, s. 76).
([7]) Rozhodnutí Komise ze dne 4. května 2016 o zmocnění týkajícím se bezpečnosti [C(2016) 2797 final].

PŘIJALA TOTO ROZHODNUTÍ:

KAPITOLA 1

OBECNÁ USTANOVENÍ

Článek 1

Předmět a oblast působnosti

1. Toto rozhodnutí stanoví prováděcí pravidla pro průmyslovou bezpečnost s ohledem na utajované veřejné zakázky s cílem podpořit provádění rozhodnutí (EU, Euratom) 2015/444, a to zejména kapitoly 6 uvedeného rozhodnutí.

2. Toto rozhodnutí stanoví zvláštní požadavky, které mají zajistit ochranu utajovaných informací EU ze strany hospodářských subjektů v předsmluvní fázi, v průběhu celého životního cyklu utajovaných smluv uzavřených Evropskou komisí a v subdodavatelských smlouvách uzavřených dodavateli Komise.

3. Toto rozhodnutí se týká informací utajovaných na následujících úrovních:

a) RESTREINT UE/EU RESTRICTED;

b) CONFIDENTIEL UE/EU CONFIDENTIAL;

c) SECRET UE/EU SECRET.

Článek 2

Odpovědnost v rámci Komise

1. V rámci povinností popsaných ve finančním nařízení ([8]) každá schvalující osoba Komise jakožto veřejného zadavatele zajistí, aby utajovaná smlouva odkazovala na minimální standardy průmyslové bezpečnosti stanovené v kapitole 6 rozhodnutí (EU, Euratom) 2015/444 a v těchto prováděcích pravidlech a v příslušných případech v oznámení o zahájení zadávacího řízení nebo ve výzvě k podávání nabídek, a aby byly tyto standardy v průběhu provádění dodržovány.

2. Za tímto účelem požaduje dotčená schvalující osoba ve všech fázích poradenství od bezpečnostního orgánu Komise ohledně otázek týkajících se bezpečnostních prvků utajované smlouvy, programu nebo projektu a informuje místního bezpečnostního úředníka o uzavřených smlouvách. Rozhodnutí o stupni utajení konkrétních subjektů přijímá veřejný zadavatel s náležitým ohledem na příručku pro stanovování stupňů utajení.

3. Při dodržování požadavků těchto prováděcích pravidel bezpečnostní orgán Komise úzce spolupracuje s vnitrostátními bezpečnostními orgány a určenými bezpečnostními orgány dotčených členských států, zejména pokud jde o bezpečnostní prověrky zařízení a bezpečnostní prověrky personálu, postupy týkající se návštěv a plány na přepravu.

KAPITOLA 2

VYŘIZOVÁNÍ VÝZEV K PODÁVÁNÍ NABÍDEK NA UTAJOVANÉ SMLOUVY

Článek 3

Základní zásady

1. Utajované smlouvy budou uzavřeny pouze s hospodářskými subjekty registrovanými v členském státě nebo s hospodářskými subjekty registrovanými ve třetí zemi či zřízenými mezinárodní organizací, pokud tato třetí země nebo mezinárodní organizace uzavřela dohodu o bezpečnosti informací s Evropskou unií nebo uzavřela správní ujednání s Komisí ([9]).

2. Před zveřejněním výzvy k podávání nabídek na utajovanou smlouvu veřejný zadavatel určí stupeň utajení veškerých informací, které by mohly být uchazečům poskytnuty. Veřejný zadavatel rovněž určí maximální stupeň utajení veškerých informací vypracovaných při provádění smlouvy, programu či projektu nebo alespoň předpokládaný objem a druh informací, které mají být poskytnuty nebo zpracovány, a potřebu utajovaného informačního a komunikačního systému (CIS).

([8]) Nařízení Evropského parlamentu a Rady (EU, Euratom) 2018/1046 ze dne 18. července 2018, kterým se stanoví finanční pravidla pro souhrnný rozpočet Unie, mění nařízení (EU) č. 1296/2013, (EU) č. 1301/2013, (EU) č. 1303/2013, (EU) č. 1304/2013, (EU) č. 1309/2013, (EU) č. 1316/2013, (EU) č. 223/2014 a (EU) č. 283/2014 a rozhodnutí č. 541/2014/EU a zrušuje nařízení (EU, Euratom) č. 966/2012 (Úř. věst. L 193, 30.7.2018, s. 1).

([9]) Seznam dohod uzavřených Evropskou unií a správních ujednání uzavřených Evropskou komisí, na základě kterých mohou být utajované informace EU vyměňovány s třetími zeměmi a mezinárodními organizacemi, je uveden na internetových stránkách Komise.

3. Veřejný zadavatel zajistí, aby v oznámení o zahájení zadávacího řízení pro utajované smlouvy byly uvedeny informace o zvláštních bezpečnostních povinnostech týkajících se utajovaných informací. Příloha I obsahuje vzorovou šablonu pro informace, jež mají být v oznámení o zahájení zadávacího řízení uvedeny.

4. Veřejný zadavatel zajistí, aby informace se stupněm utajení RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL a SECRET UE/EU SECRET byly uchazečům předány až poté, co podepíšou dohodu o mlčenlivosti, která uchazeče zavazuje, aby s utajovanými informacemi EU nakládali a chránili je v souladu s rozhodnutím (EU, Euratom) 2015/444 a jeho prováděcími pravidly.

5. Všichni dodavatelé, od nichž se vyžaduje, aby v rámci svých zařízení nakládali s informacemi se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL nebo SECRET UE/EU SECRET nebo je uchovávali, a to buď během samotného plnění utajované smlouvy, nebo v předsmluvní fázi, musí být držiteli bezpečnostní prověrky zařízení na požadované úrovni. Níže jsou uvedeny tři scénáře, které mohou nastat ve fázi nabídkového řízení na utajovanou smlouvu, která zahrnuje utajované informace EU se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL nebo SECRET UE/EU SECRET:

a) žádný přístup k utajovaným informacím EU se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL nebo SECRET UE/EU SECRET během fáze nabídkového řízení:

   Pokud se oznámení o zahájení zadávacího řízení nebo výzva k podávání nabídek týká smlouvy, která bude zahrnovat utajované informace EU se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL nebo SECRET UE/EU SECRET, ale nevyžaduje, aby uchazeč s těmito informacemi během fáze nabídkového řízení nakládal, potom uchazeč, který není držitelem bezpečnostní prověrky zařízení na požadované úrovni, není z nabídkového řízení vyloučen na základě toho, že není držitelem bezpečnostní prověrky zařízení.

b) přístup k utajovaným informacím EU se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL nebo SECRET UE/EU SECRET v prostorách veřejného zadavatele během fáze nabídkového řízení:

   Přístup je udělen členům personálu uchazeče, kteří jsou držiteli bezpečnostní prověrky personálu na požadované úrovni a utajované informace potřebují znát. Před udělením tohoto přístupu veřejný zadavatel prostřednictvím bezpečnostního orgánu Komise ověří u příslušného vnitrostátního bezpečnostního orgánu či určeného bezpečnostního orgánu, zda vnitrostátní právní předpisy v této fázi požadují i bezpečnostní prověrku zařízení.

c) nakládání s utajovanými informacemi EU se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL nebo SECRET UE/EU SECRET a jejich uchovávání v prostorách uchazeče během fáze nabídkového řízení:

   Pokud oznámení o zahájení zadávacího řízení nebo výzva k podávání nabídek požaduje po uchazečích, aby s utajovanými informacemi EU nakládali nebo je uchovávali ve svých prostorách, musí být uchazeč držitelem bezpečnostní prověrky zařízení na požadované úrovni. Za těchto okolností obdrží veřejný zadavatel prostřednictvím bezpečnostního orgánu Komise od příslušného vnitrostátního bezpečnostního orgánu či určeného bezpečnostního orgánu ujištění o tom, že uchazeči byla udělena náležitá bezpečnostní prověrka zařízení. Přístup je udělen členům personálu uchazeče, kteří jsou držiteli bezpečnostní prověrky personálu na požadované úrovni a utajované informace potřebují znát.

6. Bezpečnostní prověrka zařízení obecně není požadována pro přístup k informacím se stupněm utajení RESTREINT UE/EU RESTRICTED, a to ani ve fázi nabídkového řízení, ani při plnění smlouvy. Pokud členské státy požadují bezpečnostní prověrku zařízení pro smlouvy nebo subdodavatelské smlouvy se stupněm utajení RESTREINT UE/EU RESTRICTED v rámci svých vnitrostátních právních předpisů uvedených v příloze IV, neukládají tyto vnitrostátní požadavky žádné dodatečné povinnosti jiným členským státům ani nevylučují ze souvisejících smluv či subdodavatelských smluv nebo ze soutěže o tyto zakázky uchazeče, dodavatele či subdodavatele z členských států, které nemají žádné takové požadavky na bezpečnostní prověrky zařízení na přístup k informacím se stupněm utajení RESTREINT UE/EU RESTRICTED. Tyto zakázky jsou prováděny v členských státech v souladu s jejich vnitrostátními právními předpisy.

7. Pokud je bezpečnostní prověrka zařízení požadována pro plnění utajované smlouvy, veřejný zadavatel předloží prostřednictvím bezpečnostního orgánu Komise žádost vnitrostátnímu bezpečnostnímu orgánu či určenému bezpečnostnímu orgánu dodavatele, k čemuž použije informační list pro bezpečnostní prověrku zařízení. Příklad informačního listu pro bezpečnostní prověrku zařízení ([10]) je uveden v dodatku D přílohy III. Utajovaná smlouva není uzavřena, dokud vnitrostátní bezpečnostní orgán či určený bezpečnostní orgán dodavatele uchazečovu bezpečnostní prověrku zařízení nepotvrdí. Odpověď na informační list pro bezpečnostní prověrku zařízení je pokud možno poskytnuta do deseti pracovních dnů ode dne podání žádosti.

([10]) Další používané formuláře se od příkladu uvedeného v těchto prováděcích pravidlech mohou lišit ve své koncepci.

Článek 4

Subdodávky u utajovaných smluv

1. Podmínky, za nichž může dodavatel, který uzavřel utajovanou smlouvu s Komisí, uzavřít subdodavatelskou smlouvu, jsou stanoveny ve výzvě k podávání nabídek a v zadávací dokumentaci. Pokud utajovaná smlouva povoluje subdodavatelské smlouvy týkající se některých jejích částí, podléhají tyto subdodavatelské smlouvy předchozímu písemnému souhlasu veřejného zadavatele. Před udělením souhlasu veřejný zadavatel konzultuje bezpečnostní orgán Komise.

2. Utajované zakázky budou na základě subdodavatelských smluv svěřeny pouze hospodářským subjektům registrovaným v členském státě nebo hospodářským subjektům registrovaným ve třetí zemi či zřízeným mezinárodní organizací, pokud tato třetí země nebo mezinárodní organizace uzavřela dohodu o bezpečnosti informací s EU nebo uzavřela správní ujednání s Komisí ([11]).

KAPITOLA 3

UZAVÍRÁNÍ UTAJOVANÝCH SMLUV S KOMISÍ

Článek 5

Základní zásady

1. Při uzavírání utajované smlouvy veřejný zadavatel společně s bezpečnostním orgánem Komise zajistí, aby povinnosti dodavatele týkající se ochrany utajovaných informací EU, které jsou tomuto dodavateli poskytnuty nebo jsou vypracovány při plnění smlouvy, byly nedílnou součástí smlouvy. Bezpečnostní požadavky pro konkrétní smlouvu jsou poskytnuty ve formě seznamu bezpečnostních požadavků (SAL). Vzorová šablona seznamu SAL je stanovena v příloze III.

2. Před podpisem utajované smlouvy veřejný zadavatel vyhotoví po konzultaci s bezpečnostním orgánem Komise příručku pro stanovování stupňů utajení (SCG) pro úkoly, jež mají být provedeny, a informace, které jsou vypracovány, a to při plnění smlouvy nebo na úrovni programu či projektu. Příručka SCG je součástí seznamu SAL.

3. Bezpečnostní požadavky pro konkrétní program nebo projekt mají formu bezpečnostních pokynů k programu (nebo projektu). Bezpečnostní pokyny k programu (nebo projektu) mohou být sepsány s využitím šablony seznamu SAL stanovené v příloze III. Tyto pokyny vypracuje útvar Komise, který program nebo projekt řídí, v úzké spolupráci s bezpečnostním orgánem Komise a předloží je ke konzultaci skupině odborníků pro bezpečnost v Komisi. Pokud je smlouva součástí programu nebo projektu s vlastními bezpečnostními pokyny k programu (nebo projektu), seznam SAL smlouvy je ve zjednodušené formě a obsahuje odkaz na bezpečnostní ustanovení stanovená v bezpečnostních pokynech daného programu či projektu.

4. Veřejný zadavatel je považován za původce utajovaných informací, jež byly vytvořeny a s nimiž se nakládá pro účely plnění smlouvy.

5. Veřejný zadavatel prostřednictvím bezpečnostního orgánu Komise uvědomí vnitrostátní bezpečnostní orgány či určené bezpečnostní orgány všech dodavatelů a subdodavatelů o uzavření utajovaných smluv nebo subdodavatelských smluv a o veškerých prodlouženích nebo předčasných ukončeních těchto smluv nebo subdodavatelských smluv. Seznam požadavků jednotlivých zemí je uveden v příloze IV.

6. Smlouvy obsahující utajované informace se stupněm utajení RESTREINT UE/EU RESTRICTED zahrnují smluvní doložku o bezpečnosti, jež činí ustanovení stanovená v dodatku E přílohy III závaznými pro dodavatele. Tyto smlouvy zahrnují seznam SAL, který stanoví minimální požadavky na nakládání s informacemi se stupněm utajení RESTREINT UE/EU RESTRICTED, včetně aspektů zabezpečení informací, a zvláštní požadavky, které má splnit dodavatel z pověření veřejného zadavatele za účelem akreditace informačního a komunikačního systému dodavatele, který nakládá s informacemi se stupněm utajení RESTREINT UE/EU RESTRICTED.

([11]) Seznam dohod uzavřených Evropskou unií a správních ujednání uzavřených Evropskou komisí, na základě kterých mohou být utajované informace EU vyměňovány s třetími zeměmi a mezinárodními organizacemi, je uveden na internetových stránkách Komise.

7. Pokud jsou utajované informace se stupněm utajení RESTREINT UE/EU RESTRICTED poskytnuty uchazečům nebo potenciálním dodavatelům, minimální požadavky uvedené v odstavci 6 musí být zahrnuty do nabídkových řízení nebo do příslušných dohod o mlčenlivosti uzavřených ve fázi nabídkového řízení.

8. Pokud to vyžadují vnitrostátní právní předpisy členských států, vnitrostátní bezpečnostní orgány či určené bezpečnostní orgány zajistí, aby dodavatelé nebo subdodavatelé v jejich pravomoci splňovali platná bezpečnostní ustanovení pro ochranu informací se stupněm utajení RESTREINT UE/EU RESTRICTED, a provádějí inspekce v zařízeních dodavatelů nacházejících se na jejich území. Pokud vnitrostátní bezpečnostní orgán či určený bezpečnostní orgán tuto povinnost nemá, veřejný zadavatel zajistí, aby dodavatel prováděl požadovaná bezpečnostní ustanovení uvedená v příloze III.

Článek 6

Přístup personálu dodavatelů a subdodavatelů k utajovaným informacím EU

1. Útvar Komise jakožto veřejný zadavatel zajistí, aby utajované smlouvy zahrnovaly ustanovení o tom, že členům personálu dodavatele či subdodavatele, kteří pro účely plnění utajované smlouvy nebo subdodavatelské smlouvy vyžadují přístup k utajovaným informacím EU, může být tento přístup udělen pouze tehdy, pokud:

a) bylo prokázáno, že utajované informace potřebují znát;

b) jim příslušný vnitrostátní bezpečnostní orgán či určený bezpečnostní orgán nebo jakýkoli jiný příslušný bezpečnostní orgán udělil bezpečnostní prověrku personálu na příslušné úrovni pro informace se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL nebo SECRET UE/EU SECRET;

c) byli poučeni o příslušných bezpečnostních pravidlech pro ochranu utajovaných informací EU a vzali na vědomí své povinnosti ohledně ochrany těchto informací.

2. Pokud dodavatel či subdodavatel hodlá zaměstnat státního příslušníka země mimo EU na pracovním místě, které vyžaduje přístup k utajovaným informacím EU se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL nebo SECRET UE/EU SECRET, je povinností tohoto dodavatele či subdodavatele, aby zahájil bezpečnostní prověrku dané osoby v souladu s vnitrostátními právními předpisy platnými v místě, kde má být přístup k utajovaným informacím EU udělen.

KAPITOLA 4

NÁVŠTĚVY V SOUVISLOSTI S UTAJOVANÝMI SMLOUVAMI

Článek 7

Základní zásady

1. Pokud Komise, dodavatelé či subdodavatelé potřebují pro plnění utajované smlouvy přístup k informacím se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL nebo SECRET UE/EU SECRET v prostorách druhé strany, sjednají se návštěvy ve spolupráci s příslušnými vnitrostátními bezpečnostními orgány či určenými bezpečnostními orgány nebo s kterýmkoli jiným příslušným bezpečnostním orgánem.

2. Na návštěvy uvedené v odstavci 1 se vztahují tyto požadavky:

a) návštěva musí mít oficiální účel týkající se utajované smlouvy uzavřené Komisí;

b) za účelem přístupu k utajovaným informacím EU, jež byly poskytnuty nebo vypracovány při plnění utajované smlouvy uzavřené Komisí, musí být každý návštěvník držitelem bezpečnostní prověrky personálu na požadované úrovni a musí být nezbytné, aby utajované informace znal.

Článek 8

Žádosti o návštěvu

1. Návštěvy dodavatelů v zařízeních jiných dodavatelů nebo v prostorách Komise, které zahrnují přístup k utajovaným informacím se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL nebo SECRET UE/EU SECRET, se sjednají v souladu s tímto postupem:

a) bezpečnostní úředník zařízení, které vysílá návštěvníka, vyplní všechny příslušné části formuláře žádosti o návštěvu a předloží žádost vnitrostátnímu bezpečnostnímu orgánu či určenému bezpečnostnímu orgánu daného zařízení. Šablona formuláře žádosti o návštěvu je stanovena v dodatku C přílohy III;

b) vnitrostátní bezpečnostní orgán či určený bezpečnostní orgán vysílajícího zařízení musí potvrdit návštěvníkovu bezpečnostní prověrku personálu předtím, než předloží žádost o návštěvu vnitrostátnímu bezpečnostnímu orgánu či určenému bezpečnostnímu orgánu hostitelského zařízení (nebo bezpečnostnímu orgánu Komise, pokud se jedná o návštěvu prostor Komise);

c) bezpečnostní úředník vysílajícího zařízení poté obdrží od svého vnitrostátního bezpečnostního orgánu či určeného bezpečnostního orgánu odpověď vnitrostátního bezpečnostního orgánu či určeného bezpečnostního orgánu hostitelského zařízení (nebo bezpečnostního orgánu Komise), která žádost o návštěvu buď povoluje, nebo zamítá;

d) žádost o návštěvu se považuje za schválenou, pokud nejsou vzneseny žádné námitky do pěti pracovních dnů před datem návštěvy.

2. Návštěvy úředníků Komise v zařízeních dodavatelů, které zahrnují přístup k utajovaným informacím se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL nebo SECRET UE/EU SECRET, se sjednají v souladu s tímto postupem:

a) návštěvník vyplní všechny příslušné části formuláře žádosti o návštěvu a předloží ji bezpečnostnímu orgánu Komise;

b) bezpečnostní orgán Komise potvrdí návštěvníkovu bezpečnostní prověrku personálu a poté předloží žádost o návštěvu vnitrostátnímu bezpečnostnímu orgánu či určenému bezpečnostnímu orgánu hostitelského zařízení;

c) bezpečnostní orgán Komise obdrží odpověď od vnitrostátního bezpečnostního orgánu či určeného bezpečnostního orgánu hostitelského zařízení, která žádost o návštěvu buď povoluje, nebo zamítá;

d) žádost o návštěvu se považuje za schválenou, pokud nejsou vzneseny žádné námitky do pěti pracovních dnů před datem návštěvy.

3. Žádost o návštěvu se může vztahovat na jedinou návštěvu nebo na opakované návštěvy. V případě opakovaných návštěv může žádost o návštěvu platit po dobu jednoho roku od požadovaného data zahájení.

4. Platnost jakékoli žádosti o návštěvu nepřesahuje platnost návštěvníkovy bezpečnostní prověrky personálu.

5. Žádost o návštěvu by se zpravidla měla předkládat příslušnému bezpečnostnímu orgánu hostitelského zařízení alespoň 15 pracovních dnů před datem návštěvy.

Článek 9

Postupy týkající se návštěv

1. Dříve než bezpečnostní úředník hostitelského zařízení umožní návštěvníkovi přístup k utajovaným informacím EU, musí bezpečnostní úředník splnit všechny bezpečnostní postupy a pravidla týkající se návštěv, jež stanovil jeho vnitrostátní bezpečnostní orgán či určený bezpečnostní orgán.

2. Návštěvníci prokážou svou totožnost při příjezdu do hostitelského zařízení tím, že předloží platný průkaz totožnosti nebo cestovní pas. Identifikační údaje musí odpovídat údajům uvedeným v žádosti o návštěvu.

3. Hostitelské zařízení zajistí, aby se vedly záznamy o všech návštěvnících, včetně jejich jmen, organizace, kterou zastupují, data skončení platnosti bezpečnostní prověrky personálu, data návštěvy a jmen navštívených osob. Tyto záznamy se uchovávají po dobu nejméně pěti let, případně déle, vyžadují-li to vnitrostátní pravidla a předpisy země, v níž se hostitelské zařízení nachází.

Článek 10

Návštěvy sjednané přímo

1. V souvislosti s konkrétními projekty se mohou příslušné vnitrostátní bezpečnostní orgány či určené bezpečnostní orgány a bezpečnostní orgán Komise dohodnout na postupu, podle kterého lze návštěvy za účelem konkrétní utajované smlouvy sjednávat přímo mezi bezpečnostním úředníkem návštěvníka a bezpečnostním úředníkem zařízení, v němž má být návštěva vykonána. Šablona formuláře, který je třeba použít za tímto účelem, je uvedena v dodatku C přílohy III. Tento výjimečný postup je stanoven v bezpečnostních pokynech k programu (nebo projektu) nebo v rámci jiných zvláštních ujednání. V takových případech se postupy uvedené v článku 8 a v čl. 9 odst. 1 nepoužijí.

2. Návštěvy, které zahrnují přístup k utajovaným informacím se stupněm utajení RESTREINT UE/EU RESTRICTED, jsou sjednány přímo mezi vysílajícím a přijímajícím subjektem, aniž by bylo třeba dodržovat postupy stanovené v článku 8 a v čl. 9 odst. 1.

KAPITOLA 5

PŘENOS A PŘEPRAVA UTAJOVANÝCH INFORMACÍ EU PŘI PLNĚNÍ UTAJOVANÝCH SMLUV

Článek 11

Základní zásady

Veřejný zadavatel zajistí, aby všechna rozhodnutí týkající se přesunu a přepravy utajovaných informací EU byla v souladu s rozhodnutím (EU, Euratom) 2015/444 a jeho prováděcími pravidly a s podmínkami utajované smlouvy, včetně souhlasu původce.

Článek 12

Elektronické nakládání s informacemi

1. Elektronické nakládání s utajovanými informacemi EU a jejich přenos se provádí v souladu s kapitolami 5 a 6 rozhodnutí (EU, Euratom) 2015/444 a jeho prováděcími pravidly.

Komunikační a informační systémy, které vlastní dodavatel a používají se k nakládání s utajovanými informacemi EU při provádění smlouvy („komunikační a informační systémy dodavatele"), podléhají akreditaci ze strany odpovědného orgánu pro bezpečnostní akreditaci. Jakékoli elektronické předávání utajovaných informací EU je chráněno kryptografickými prostředky schválenými v souladu s čl. 36 odst. 4 rozhodnutí (EU, Euratom) 2015/444. „Opatření TEMPEST" jsou prováděna v souladu s čl. 36 odst. 6 tohoto rozhodnutí.

2. Bezpečnostní akreditací informačních a komunikačních systémů dodavatele, které nakládají s utajovanými informacemi EU se stupněm utajení RESTREINT UE/EU RESTRICTED, a jakýmkoli jejich propojením může být pověřen bezpečnostní úředník dodavatele, pokud to dovolují vnitrostátní právní předpisy. Pokud je tímto úkolem někdo pověřen, dodavatel odpovídá za plnění minimálních bezpečnostních požadavků uvedených v seznamu SAL při nakládání s informacemi se stupněm utajení RESTREINT UE/EU RESTRICTED ve svém informačním a komunikačním systému. Příslušné vnitrostátní bezpečnostní orgány či určené bezpečnostní orgány a orgány pro bezpečnostní akreditaci však nesou odpovědnost za ochranu informací se stupněm utajení RESTREINT UE/EU RESTRICTED, s nimiž nakládá dodavatel, a mají právo na inspekci bezpečnostních opatření přijatých dodavateli. Navíc dodavatel musí veřejnému zadavateli a – vyžadují-li to vnitrostátní právní předpisy – příslušnému vnitrostátnímu orgánu pro bezpečnostní akreditaci předložit prohlášení o vyhovění požadavkům osvědčující, že komunikační a informační systémy dodavatele a související propojení byly akreditovány k nakládání s utajovanými informacemi EU se stupněm utajení RESTREINT UE/EU RESTRICTED ([12]).

Článek 13

Přeprava obchodními kurýry

Přeprava utajovaných informací EU obchodními kurýry se řídí příslušnými ustanoveními rozhodnutí Komise týkajících se prováděcích pravidel pro nakládání s informacemi se stupněm utajení RESTREINT UE/EU RESTRICTED a CONFIDENTIEL UE/EU CONFIDENTIAL.

Článek 14

Osobní přenos

1. Osobní přenos utajovaných informací podléhá přísným bezpečnostním požadavkům.

2. Personál dodavatele může v rámci EU osobně přenášet informace se stupněm utajení RESTREINT UE/EU RESTRICTED, pokud jsou splněny tyto požadavky:

a) použitá obálka nebo obal jsou neprůhledné a není na nich označena klasifikace jejich obsahu;

([12]) Minimální požadavky na komunikační a informační systémy, které nakládají s utajovanými informacemi EU se stupněm utajení RESTREINT UE/EU RESTRICTED, jsou uvedeny v dodatku E přílohy III.

b) osoba, která utajované informace přenáší, je má stále u sebe;

c) obálka nebo obal nesmí být během přenosu otevřeny.

3. Pokud jde o informace se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL a SECRET UE/EU SECRET, osobní přenos personálem dodavatele v rámci členského státu EU je předem sjednán mezi vysílajícími a přijímajícími subjekty. Odesílající orgán nebo zařízení informuje přijímající orgán nebo zařízení o podrobnostech zásilky včetně odkazu, klasifikace, očekávané doby příjezdu a jména kurýra. Tento osobní přenos je povolen, pokud jsou splněny následující požadavky:

a) utajované informace jsou přenášeny ve dvojité obálce nebo obalu;

b) vnější obálka nebo obal jsou zabezpečeny a není na nich označena klasifikace jejich obsahu, zatímco na vnitřní obálce je označen stupeň utajení;

c) osoba, která utajované informace EU přenáší, je má stále u sebe;

d) obálka nebo obal nesmí být během přenosu otevřeny;

e) obálka nebo obal jsou přenášeny v uzamykatelném kufru nebo podobném schváleném pouzdře takové velikosti a váhy, že ho přenášející osoba může mít neustále u sebe a nemusí ho umísťovat do zavazadlového prostoru;

f) kurýr je držitelem osvědčení kurýra vydaného jeho příslušným bezpečnostním úřadem, který kurýra opravňuje k přenosu určené utajované zásilky.

4. Pro osobní přenos informací se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL a SECRET UE/EU SECRET personálem dodavatele z jednoho členského státu EU do jiného platí tato dodatečná pravidla:

a) kurýr odpovídá za bezpečnou úschovu přenášeného utajovaného materiálu, dokud není předán příjemci;

b) v případě narušení bezpečnosti může vnitrostátní bezpečnostní orgán či určený bezpečnostní orgán odesílatele požádat, aby orgány v zemi, kde k tomuto narušení došlo, provedly vyšetřování, podaly zprávu o svých zjištěních a podnikly právní nebo případně jiné kroky;

c) kurýr byl poučen o všech bezpečnostních povinnostech, které je během přenosu třeba dodržovat, a podepsal náležité potvrzení;

d) pokyny pro kurýra jsou přiloženy k osvědčení kurýra;

e) kurýrovi byl poskytnut popis zásilky a plán cesty;

f) dokumenty budou po dokončení cest(y) vráceny vydávajícímu vnitrostátnímu bezpečnostnímu orgánu či určenému bezpečnostnímu orgánu nebo je bude uchovávat příjemce za účelem sledování;

g) pokud celníci, imigrační orgány nebo pohraniční policie požádají o přezkoumání a kontrolu zásilky, je jim povoleno otevřít a prohlédnout dostatečné části zásilky, aby ověřili, že neobsahuje žádný jiný materiál, než jaký je ohlášen;

h) celní orgány by měly být naléhavě vyzvány, aby ctily úřední povahu průvodních dokladů a oprávnění přenášených kurýrem.

Pokud je zásilka celníky otevřena, mělo by se tak stát mimo dohled neoprávněných osob a pokud možno za přítomnosti kurýra. Kurýr si vyžádá opětovné zabalení zásilky a požádá orgány provádějící kontrolu, aby zásilku znovu zapečetily a písemně potvrdily, že jimi byla otevřena.

5. Na osobní přenos utajovaných informací se stupněm utajení RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL a SECRET UE/EU SECRET personálem dodavatele do třetí země nebo mezinárodní organizace se budou vztahovat ustanovení dohody o bezpečnosti informací nebo správního ujednání uzavřeného mezi Evropskou unií nebo Komisí a danou třetí zemí nebo mezinárodní organizací.

KAPITOLA 6

PLÁNOVÁNÍ KONTINUITY ČINNOSTÍ

Článek 15

Pohotovostní plány a nápravná opatření

Útvar Komise jakožto veřejný zadavatel zajistí, aby utajovaná smlouva požadovala po dodavateli vypracování obchodních pohotovostních plánů na ochranu utajovaných informací EU, s nimiž se nakládá v souvislosti s prováděním utajované smlouvy v mimořádných situacích, a zavedení preventivních a nápravných opatření v rámci plánování kontinuity činností za účelem minimalizace dopadu incidentů spojených s nakládáním s utajovanými informacemi EU a jejich uchováváním. Dodavatel o svém obchodním pohotovostním plánu informuje veřejného zadavatele.

Článek 16

Vstup v platnost

Toto rozhodnutí vstupuje v platnost dvacátým dnem po vyhlášení v *Úředním věstníku Evropské unie*.

V Bruselu dne 17. října 2019.

Za Komisi,

jménem předsedy,

Günther OETTINGER

člen Komise

PŘÍLOHA I

STANDARDNÍ INFORMACE V OZNÁMENÍCH O ZADÁNÍ VEŘEJNÝCH ZAKÁZEK

(bude upraveno podle použitého oznámení o zadávacím řízení)

Pro smlouvy obsahující utajované informace se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL nebo SECRET UE/EU SECRET

Další zvláštní podmínky (*v příslušných případech*)

Plnění smlouvy podléhá zvláštním podmínkám ● ano ○ ne

(*pokud ano*) Popis zvláštních podmínek:

Smlouva bude zahrnovat přístup k informacím se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL nebo SECRET UE/EU SECRET, jež podléhají bezpečnostním pravidlům pro ochranu utajovaných informací EU stanoveným v rozhodnutí (EU, Euratom) 2015/444 a prováděcím pravidlům k uvedenému rozhodnutí [1], nakládání s nimi a/nebo jejich uchovávání.

Bude požadována bezpečnostní prověrka zařízení a rovněž bezpečnostní prověrky personálu pro členy personálu dodavatele, kteří nakládají s utajovanými informacemi.

Součástí smlouvy budou zvláštní bezpečnostní povinnosti (seznam bezpečnostních požadavků přiložený ke smlouvě). Subdodavatelské smlouvy budou podléhat předchozímu písemnému souhlasu veřejného zadavatele a subdodavatel a jeho personál budou dodržovat všechna bezpečnostní pravidla.

Pro smlouvy obsahující utajované informace se stupněm utajení RESTREINT UE/EU RESTRICTED

Další zvláštní podmínky (*v příslušných případech*)

Plnění smlouvy podléhá zvláštním podmínkám ● ano ○ ne

(*pokud ano*) Popis zvláštních podmínek:

Smlouva bude zahrnovat nebo vyžadovat přístup k informacím se stupněm utajení RESTREINT UE/EU RESTRICTED, jež podléhají bezpečnostním pravidlům pro ochranu utajovaných informací EU stanoveným v rozhodnutí (EU, Euratom) 2015/444 a prováděcím pravidlům k uvedenému rozhodnutí [2], nakládání s nimi a/nebo jejich uchovávání.

Součástí smlouvy budou zvláštní bezpečnostní povinnosti (seznam bezpečnostních požadavků přiložený ke smlouvě). Subdodavatelské smlouvy budou podléhat předchozímu písemnému souhlasu veřejného zadavatele a subdodavatel a jeho personál budou dodržovat všechna bezpečnostní pravidla.

[1] Veřejný zadavatel by měl vložit odkazy, jakmile budou prováděcí pravidla přijata.
[2] Veřejný zadavatel by měl vložit odkazy, jakmile budou prováděcí pravidla přijata.

PŘÍLOHA II

STANDARDNÍ USTANOVENÍ SMLUV O VEŘEJNÝCH ZAKÁZKÁCH

(bude upraveno podle použitých smluv)

ČLÁNEK XX

POVINNOSTI TÝKAJÍCÍ SE BEZPEČNOSTI

XX.1 Utajované informace EU

Pokud provádění smlouvy zahrnuje používání nebo vypracovávání utajovaných informací EU, je třeba s těmito informacemi zacházet v souladu se seznamem bezpečnostních požadavků (SAL) a jeho příručkou pro stanovování stupňů utajení (SCG), jak stanoví příloha 1, a s rozhodnutím (EU, Euratom) 2015/444 a jeho prováděcími pravidly [1], dokud nejsou tyto informace odtajněny.

Jakékoli výstupy obsahující utajované informace musí být předloženy v souladu se zvláštními postupy dohodnutými s veřejným zadavatelem.

Akční úkoly, které zahrnují utajované informace, nesmějí být zadávány subdodavatelům bez předchozího výslovného písemného schválení veřejného zadavatele.

Utajované informace EU nesmějí být poskytnuty žádné třetí straně (včetně subdodavatelů) bez předchozího výslovného písemného schválení veřejného zadavatele.

[1] Veřejný zadavatel by měl vložit odkazy, jakmile budou prováděcí pravidla přijata.

PŘÍLOHA III

[Příloha IV (k rámcové smlouvě)]

SEZNAM BEZPEČNOSTNÍCH POŽADAVKŮ (SAL)

[vzor]

Dodatek A

BEZPEČNOSTNÍ POŽADAVKY

Veřejný zadavatel musí do seznamu bezpečnostních požadavků (SAL) zahrnout následující bezpečnostní požadavky. Některá ustanovení nemusí být pro smlouvu použitelná. Ta jsou uvedena v hranatých závorkách.

Seznam ustanovení není vyčerpávající. Další ustanovení mohou být přidána v závislosti na povaze utajované smlouvy.

OBECNÉ PODMÍNKY

[*pozn.: vztahují se na všechny utajované smlouvy*]

1. Tento seznam bezpečnostních požadavků (SAL) je nedílnou součástí utajované smlouvy [nebo subdodavatelské smlouvy] a popisuje bezpečnostní požadavky pro konkrétní smlouvu. Nesplnění těchto požadavků může představovat dostatečné důvody pro ukončení smlouvy.

2. Na dodavatele se vztahují všechny povinnosti stanovené v rozhodnutí (EU, Euratom) 2015/444 a v jeho prováděcích pravidlech ([1]).

3. Utajované informace vypracované při plnění smlouvy musí být označeny jako utajované informace EU s bezpečnostním stupněm utajení stanoveným v příručce pro stanovování stupňů utajení (SCG) v dodatku B k tomuto seznamu. Odchýlení od bezpečnostního stupně utajení stanoveného v příručce SCG je přípustné pouze s písemným povolením veřejného zadavatele.

4. Práva náležející původci jakýchkoli utajovaných informací EU, jež jsou vytvářeny a s nimiž se nakládá pro účely plnění utajované smlouvy, vykonává Komise jakožto veřejný zadavatel.

5. Bez písemného souhlasu veřejného zadavatele nesmí dodavatel či subdodavatel využívat žádné informace nebo materiály poskytnuté veřejným zadavatelem nebo vyhotovené jménem tohoto zadavatele za jakýmkoli jiným účelem než pro účely smlouvy.

6. Dodavatel musí vyšetřovat všechny případy narušení bezpečnosti týkající se utajovaných informací EU a nahlásit je veřejnému zadavateli, jakmile to bude možné. Dodavatel nebo subdodavatel musí svému odpovědnému vnitrostátnímu bezpečnostnímu orgánu nebo určenému bezpečnostnímu orgánu a – pokud to vnitrostátní právní předpisy dovolují – bezpečnostnímu orgánu Komise okamžitě nahlásit všechny případy, v nichž bylo potvrzeno nebo existuje důvodné podezření, že se utajované informace EU poskytnuté nebo vypracované v souladu se smlouvou ztratily nebo byly zpřístupněny neoprávněným osobám.

7. Po zániku této smlouvy musí dodavatel nebo subdodavatel vrátit co nejdříve veškeré utajované informace EU, které uchovává, veřejnému zadavateli. Pokud je to vhodné, dodavatel nebo subdodavatel mohou utajované informace EU namísto vrácení zničit. To je nutné učinit v souladu s vnitrostátními předpisy země, kde je dodavatel usazen, s předchozím souhlasem bezpečnostního orgánu Komise a podle jeho pokynů. Utajované informace EU musí být zničeny takovým způsobem, aby nemohly být obnoveny, a to zcela ani částečně.

8. Pokud je dodavatel nebo subdodavatel oprávněn ponechat si utajované informace EU i po ukončení platnosti nebo vypovězení smlouvy, utajované informace EU musí být i nadále chráněny v souladu s rozhodnutím Komise (EU, Euratom) 2015/444 (dále jen „rozhodnutí Komise 2015/444“) a jeho prováděcími pravidly ([2]).

9. Při jakémkoli elektronickém nakládání s utajovanými informacemi EU a jejich předávání je třeba dodržovat ustanovení stanovená v kapitolách 5 a 6 rozhodnutí Komise 2015/444. Ta zahrnují mimo jiné požadavek, že komunikační a informační systémy, které vlastní dodavatel a používá je k nakládání s utajovanými informacemi EU pro účely smlouvy (dále jen „komunikační a informační systémy dodavatele“), musí podléhat akreditaci ([3]), že jakékoli elektronické předávání utajovaných informací EU musí být chráněno kryptografickými prostředky schválenými v souladu s čl. 36 odst. 4 rozhodnutí Komise 2015/444 a že opatření TEMPEST musí být prováděna v souladu s čl. 36 odst. 6 rozhodnutí Komise 2015/444.

([1]) Veřejný zadavatel by měl vložit odkazy, jakmile budou prováděcí pravidla přijata.
([2]) Veřejný zadavatel by měl vložit odkazy, jakmile budou prováděcí pravidla přijata.
([3]) Strana provádějící akreditaci bude muset předložit veřejnému zadavateli prohlášení o vyhovění požadavkům prostřednictvím bezpečnostního orgánu Komise a ve spolupráci s příslušným vnitrostátním orgánem pro bezpečnostní akreditaci.

10. Dodavatel nebo subdodavatel musí mít obchodní pohotovostní plány na ochranu veškerých utajovaných informací EU, s nimiž se při provádění utajované smlouvy nakládá, v mimořádných situacích a zavede preventivní a nápravná opatření za účelem minimalizace dopadu incidentů souvisejících s nakládáním s utajovanými informacemi EU a jejich uchováváním. Dodavatel nebo subdodavatel musí o svém obchodním pohotovostním plánu informovat veřejného zadavatele.

SMLOUVY VYŽADUJÍCÍ PŘÍSTUP K INFORMACÍM SE STUPNĚM UTAJENÍ RESTREINT UE/EU RESTRICTED

11. K dodržování smlouvy nejsou nezbytné bezpečnostní prověrky personálu. Informace nebo materiály se stupněm utajení RESTREINT UE/EU RESTRICTED je však možné zpřístupnit pouze zaměstnancům dodavatele, kteří tyto informace vyžadují za účelem plnění smlouvy (podle zásady, že *utajované informace potřebují znát*) a kteří byli poučeni bezpečnostním úředníkem dodavatele o svých povinnostech a o následcích jakéhokoli ohrožení nebo narušení bezpečnosti těchto informací a písemně potvrdili, že jsou si vědomi následků nesplnění ochrany utajovaných informací EU.

12. S výjimkou případů, kdy veřejný zadavatel udělí písemný souhlas, nesmí dodavatel nebo subdodavatel poskytnout přístup k informacím nebo materiálu se stupněm utajení RESTREINT UE/EU RESTRICTED jakémukoli jinému subjektu či osobě než členům svého personálu, kteří utajované informace potřebují znát.

13. Dodavatel nebo subdodavatel musí zachovat označení stupně utajení utajovaných informací vypracovaných nebo poskytnutých během plnění smlouvy a nesmí tyto informace odtajnit bez písemného souhlasu veřejného zadavatele.

14. Informace nebo materiál se stupněm utajení RESTREINT UE/EU RESTRICTED je třeba uchovávat v uzamčeném kancelářském nábytku, není-li zrovna používán. Když jsou dokumenty přepravovány, musí se nacházet v neprůhledné obálce. Osoba, která tyto dokumenty přenáší, je musí mít stále u sebe a nesmí je během přenosu otevřít.

15. Dodavatel nebo subdodavatel může předávat dokumenty se stupněm utajení RESTREINT UE/EU RESTRICTED Komisi prostřednictvím obchodních kurýrních společností, poštovních služeb, osobního přenosu nebo elektronických prostředků. Za tímto účelem se dodavatel nebo subdodavatel musí držet bezpečnostních pokynů k programu (nebo projektu) vydaných Komisí a/nebo prováděcích pravidel Komise týkajících se průmyslové bezpečnosti s ohledem na utajované veřejné zakázky ([4]).

16. Pokud již nejsou dokumenty se stupněm utajení RESTREINT UE/EU RESTRICTED zapotřebí, musí být zničeny takovým způsobem, aby nemohly být obnoveny, a to zcela ani částečně.

17. Bezpečnostní akreditací informačních a komunikačních systémů dodavatele, které nakládají s utajovanými informacemi EU se stupněm utajení RESTREINT UE/EU RESTRICTED, a jakýmkoli jejich propojením může být pověřen bezpečnostní úředník dodavatele, pokud to dovolují vnitrostátní právní předpisy. Pokud je akreditace takto delegována, vnitrostátní bezpečnostní orgány, určené bezpečnostní orgány či orgány pro bezpečnostní akreditaci nesou odpovědnost za ochranu veškerých informací se stupněm utajení RESTREINT UE/EU RESTRICTED, s nimiž nakládá dodavatel, a mají právo na inspekci bezpečnostních opatření přijatých dodavatelem. Navíc dodavatel musí veřejnému zadavateli a – vyžadují-li to vnitrostátní právní předpisy – příslušnému vnitrostátnímu orgánu pro bezpečnostní akreditaci předložit prohlášení o vyhovění požadavkům osvědčující, že komunikační a informační systémy dodavatele a související propojení byly akreditovány k nakládání s utajovanými informacemi EU se stupněm utajení RESTREINT UE/EU RESTRICTED.

NAKLÁDÁNÍ S INFORMACEMI SE STUPNĚM UTAJENÍ RESTREINT UE/EU RESTRICTED V KOMUNIKAČNÍCH A INFORMAČNÍCH SYSTÉMECH

18. Minimální požadavky na nakládání s informacemi se stupněm utajení RESTREINT UE/EU RESTRICTED v komunikačních a informačních systémech jsou stanoveny v dodatku E k tomuto seznamu SAL.

PODMÍNKY, ZA NICHŽ MŮŽE DODAVATEL UZAVŘÍT SUBDODAVATELSKOU SMLOUVU

19. Předtím než dodavatel zadá jakoukoli část utajované smlouvy subdodavateli, musí získat povolení od dotyčného útvaru Komise jakožto veřejného zadavatele.

([4]) Veřejný zadavatel by měl vložit odkazy, jakmile budou prováděcí pravidla přijata.

20. Žádná subdodavatelská smlouva nesmí být uzavřena se společností registrovanou mimo členské státy EU nebo se subjektem náležejícím k mezinárodní organizaci, pokud tento stát mimo EU nebo mezinárodní organizace neuzavřely dohodu o bezpečnosti informací s EU nebo správní ujednání s Komisí.

21. Pokud dodavatel uzavřel smlouvu se subdodavatelem, bezpečnostní ustanovení smlouvy obdobně platí pro subdodavatele i jeho/jejich personál. V takovém případě je povinností dodavatele zajistit, aby všichni subdodavatelé uplatnili tyto zásady na své vlastní subdodavatelské smlouvy. Za účelem zajištění bezpečnostního dohledu je vnitrostátním bezpečnostním orgánům či určeným bezpečnostním orgánům dodavatele a subdodavatele oznámeno uzavírání veškerých souvisejících utajovaných subdodavatelských smluv se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL a SECRET UE/EU SECRET. Vnitrostátním bezpečnostním orgánům či určeným bezpečnostním orgánům dodavatele a subdodavatele je v příslušných případech poskytnuta kopie bezpečnostních požadavků pro subdodavatelskou smlouvu. Vnitrostátní bezpečnostní orgány či určené bezpečnostní orgány, jež požadují oznamování bezpečnostních ustanovení utajovaných smluv se stupněm utajení RESTREINT UE/EU RESTRICTED, jsou uvedeny v příloze prováděcích pravidel Komise pro průmyslovou bezpečnost s ohledem na utajované veřejné zakázky ([1]).

22. Dodavatel nesmí poskytnout utajované informace EU subdodavateli bez předchozího písemného souhlasu veřejného zadavatele. Pokud jsou utajované informace EU zasílány subdodavatelům často nebo pravidelně, veřejný zadavatel může udělit souhlas na stanovené časové období (např. 12 měsíců) nebo na dobu platnosti subdodavatelské smlouvy.

NÁVŠTĚVY

Pokud se na návštěvy zahrnující informace se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL nebo SECRET UE/EU SECRET má uplatnit standardní postup podání žádosti o návštěvu, musí veřejný zadavatel začlenit odstavce 23, 24 a 25 a vyškrtnout odstavec 26. Pokud jsou návštěvy zahrnující informace se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL nebo SECRET UE/EU SECRET sjednány přímo mezi vysílajícím a přijímajícím zařízením, veřejný zadavatel musí vyškrtnout odstavce 24 a 25 a zahrnout pouze odstavec 26.

23. Návštěvy, které zahrnují přístup nebo potenciální přístup k utajovaným informacím se stupněm utajení RESTREINT UE/EU RESTRICTED, jsou sjednány přímo mezi vysílajícím a přijímajícím zařízením, aniž by bylo třeba dodržovat postup uvedený v odstavcích 24 až 26 níže.

[24. Návštěvy, které zahrnují přístup nebo potenciální přístup k utajovaným informacím se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL nebo SECRET UE/EU SECRET, jsou podrobeny následujícímu postupu:

a) bezpečnostní úředník zařízení, které vysílá návštěvníka, vyplní všechny příslušné části formuláře žádosti o návštěvu (dodatek C) a předloží žádost vnitrostátnímu bezpečnostnímu orgánu či určenému bezpečnostnímu orgánu daného zařízení;

b) vnitrostátní bezpečnostní orgán či určený bezpečnostní orgán vysílajícího zařízení musí potvrdit návštěvníkovu bezpečnostní prověrku personálu a poté předloží žádost o návštěvu vnitrostátnímu bezpečnostnímu orgánu či určenému bezpečnostnímu orgánu hostitelského zařízení (nebo bezpečnostnímu orgánu Komise, pokud se jedná o návštěvu prostor Komise);

c) bezpečnostní úředník vysílajícího zařízení poté obdrží od svého vnitrostátního bezpečnostního orgánu či určeného bezpečnostního orgánu odpověď vnitrostátního bezpečnostního orgánu či určeného bezpečnostního orgánu hostitelského zařízení (nebo bezpečnostního orgánu Komise), která žádost o návštěvu buď povoluje, nebo zamítá;

d) žádost o návštěvu se považuje za schválenou, pokud nejsou vzneseny žádné námitky do pěti pracovních dnů před datem návštěvy.]

[25. Předtím než je návštěvníkům poskytnut přístup k informacím se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL nebo SECRET UE/EU SECRET, musí hostitelské zařízení získat povolení od svého vnitrostátního bezpečnostního orgánu či určeného bezpečnostního orgánu.]

[26. Návštěvy, které zahrnují přístup nebo potenciální přístup k utajovaným informacím se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL nebo SECRET UE/EU SECRET, jsou sjednány přímo mezi vysílajícím a přijímajícím zařízením (příklad formuláře, který je možné za tímto účelem použít, je uveden v dodatku C).]

([1]) Veřejný zadavatel by měl vložit odkazy, jakmile budou prováděcí pravidla přijata.

27. Návštěvníci musí prokázat svou totožnost při příjezdu do hostitelského zařízení tím, že předloží platný průkaz totožnosti nebo cestovní pas.

28. Zařízení, které návštěvu hostí, musí zajistit, aby se vedly záznamy o všech návštěvnících. Tyto záznamy musí zahrnovat jejich jména, organizaci, kterou zastupují, datum skončení platnosti bezpečnostní prověrky personálu (je-li to relevantní), datum návštěvy a jména navštívených osob. Aniž jsou dotčena evropská pravidla pro ochranu údajů, je třeba tyto záznamy uchovávat po dobu nejméně pěti let nebo v příslušných případech v souladu s vnitrostátními pravidly a předpisy.

HODNOTÍCÍ NÁVŠTĚVY

29. Bezpečnostní orgán Komise může ve spolupráci s příslušným vnitrostátním bezpečnostním orgánem či určeným bezpečnostním orgánem provádět návštěvy zařízení dodavatelů či subdodavatelů za účelem kontroly dodržování bezpečnostních požadavků ohledně nakládání s utajovanými informacemi EU.

PŘÍRUČKA PRO STANOVOVÁNÍ STUPŇŮ UTAJENÍ

30. Příručka pro stanovování stupňů utajení obsahuje seznam všech prvků ve smlouvě, které jsou nebo budou utajované v průběhu plnění smlouvy, pravidla pro tuto činnost a specifikace použitelných stupňů utajení. Příručka pro stanovování stupňů utajení je nedílnou součástí smlouvy a nachází se v dodatku B této přílohy.

Dodatek B

PŘÍRUČKA PRO STANOVOVÁNÍ STUPŇŮ UTAJENÍ

[konkrétní znění bude upraveno podle předmětu smlouvy]

Dodatek C

ŽÁDOST O NÁVŠTĚVU

(VZOR)

Podrobné pokyny pro vyplnění žádosti o návštěvu

(Žádost může být předložena pouze v angličtině.)

HEADING	Zaškrtněte políčka pro druh návštěvy a druh informací a uveďte, kolik míst bude navštíveno, a počet návštěvníků.
4. **ADMINISTRATIVE DATA**	Toto pole vyplní žádající vnitrostátní bezpečnostní orgán či určený bezpečnostní orgán.
5. **REQUESTING ORGANISATION OR INDUSTRIAL FACILITY**	Uveďte celé jméno a poštovní adresu. Podle okolností uveďte město, stát a poštovní směrovací číslo.
6. **ORGANISATION OR INDUSTRIAL FACILITY TO BE VISITED**	Uveďte celé jméno a poštovní adresu. Uveďte město, stát, poštovní směrovací číslo, číslo dálnopisu či faxu (pokud existuje), telefonní číslo a e-mail. Uveďte jméno a telefonní/faxové číslo a e-mail vaší hlavní kontaktní osoby nebo osoby, se kterou jste se na návštěvě domluvili. Poznámky: 1) Uvedení správného poštovního směrovacího čísla je důležité, protože společnost může mít několik různých zařízení. 2) Mají-li být navštívena dvě nebo více zařízení v souvislosti se stejným předmětem, může být při ručním podání žádosti použita příloha 1. Je-li příloha použita, v položce 3 by se mělo uvést: „SEE ANNEX 1, NUMBER OF FAC: …“ (uveďte počet zařízení).
7. **DATES OF VISIT**	Uveďte skutečné datum nebo dobu trvání (od – do) návštěvy ve formátu „den – měsíc – rok“. V příslušných případech uveďte alternativní datum nebo období v závorkách.
8. **TYPE OF INITIATIVE**	Upřesněte, zda návštěvu iniciovala žádající organizace či zařízení nebo pozvánka ze strany zařízení, jež má být navštíveno.
9. **THE VISIT RELATES TO:**	Uveďte celý název projektu, smlouvy nebo výzvy k podávání nabídek za použití pouze běžně užívaných zkratek.

10. **SUBJECT TO BE DISCUSSED/ JUSTIFICATION**	Stručně popište důvod(y) návštěvy. Nepoužívejte nevysvětlené zkratky. Poznámky: V případě opakovaných návštěv by tato položka měla uvádět „Recurring visits“ (Opakované návštěvy) jako první slova v datovém prvku (např. Recurring visits to discuss_____).
11. **ANTICIPATED LEVEL OF CLASSIFIED INFORMATION TO BE INVOLVED**	Uveďte SECRET UE/EU SECRET (S-UE/EU-S) nebo CONFIDENTIEL UE/EU CONFIDENTIAL (C-UE/EU-C) podle daného případu.
12. **PARTICULARS OF VISITOR**	Poznámka: účastní-li se návštěvy více než dva návštěvníci, je třeba použít přílohu 2.
13. **THE SECURITY OFFICER OF THE REQUESTING ENTITY**	Tato položka vyžaduje jméno, telefonní číslo, faxové číslo a e-mail bezpečnostního úředníka žádajícího zařízení.
14. **CERTIFICATION OF SECURITY CLEARANCE**	Toto pole vyplní certifikační orgán. Poznámky pro certifikační orgán: a. Uveďte jméno, adresu, telefonní číslo, faxové číslo a e-mail (může být předtištěno). b. Tato položka by měla být podepsána a opatřena razítkem (existuje-li).
15. **REQUESTING SECURITY AUTHORITY**	Toto pole vyplní vnitrostátní bezpečnostní orgán/určený bezpečnostní orgán. Poznámka pro vnitrostátní bezpečnostní orgán/určený bezpečnostní orgán: a. Uveďte jméno, adresu, telefonní číslo, faxové číslo a e-mail (může být předtištěno). b. Tato položka by měla být podepsána a opatřena razítkem (existuje-li).

Všechna pole musí být vyplněna a formulář předložen prostřednictvím mezivládních kanálů ([2]).

([2]) Pokud bylo dohodnuto, že návštěvy zahrnující přístup nebo potenciální přístup k utajovaným informacím EU se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL a SECRET UE/EU SECRET mohou být sjednány přímo, vyplněný formulář lze předložit přímo bezpečnostnímu úředníkovi zařízení, jež má být navštíveno.

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:

STAMP

TELEPHONE NO:

E-MAIL ADDRESS:

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

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

NAME:

ADDRESS:

TELEPHONE NO:

E-MAIL ADDRESS:

STAMP

SIGNATURE: DA TE *(dd/mm/yyyy)*: _____/_____/_____

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

<Místo vyhrazené pro odkaz na platné právní předpisy o ochraně osobních údajů a pro odkaz na povinné informace pro subjekt údajů, např. jak je prováděn článek 13 obecného nařízení o ochraně osobních údajů ([3]).>

([3]) Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (Úř. věst. L 119, 4.5.2016, s. 1).

ANNEX 1 to RFV FORM

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)

<Místo vyhrazené pro odkaz na platné právní předpisy o ochraně osobních údajů a pro odkaz na povinné informace pro subjekt údajů, např. jak je prováděn článek 13 obecného nařízení o ochraně osobních údajů ([1]).>

([1]) Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (Úř. věst. L 119, 4.5.2016, s. 1).

ANNEX 2 to RFV FORM

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)

<Místo vyhrazené pro odkaz na platné právní předpisy o ochraně osobních údajů a pro odkaz na povinné informace pro subjekt údajů, např. jak je prováděn článek 13 obecného nařízení o ochraně osobních údajů ([1]).>

([1]) Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (Úř. věst. L 119, 4.5.2016, s. 1).

Dodatek D

INFORMAČNÍ LIST PRO BEZPEČNOSTNÍ PROVĚRKU ZAŘÍZENÍ

(VZOR)

1. **Úvod**

1.1. Je přiložen vzorový informační list pro bezpečnostní prověrku zařízení pro rychlou výměnu informací mezi vnitrostátním bezpečnostním orgánem či určeným bezpečnostním orgánem, jinými příslušnými vnitrostátními bezpečnostními orgány a Komisí (jakožto veřejným zadavatelem) s ohledem na bezpečnostní prověrku zařízení zapojeného do utajovaných nabídkových řízení, smluv nebo subdodavatelských smluv.

1.2. Informační list pro bezpečnostní prověrku zařízení je platný pouze tehdy, je-li opatřen razítkem příslušného vnitrostátního bezpečnostního orgánu či určeného bezpečnostního orgánu nebo jiného příslušného orgánu.

1.3. Informační list pro bezpečnostní prověrku zařízení je rozdělen na oddíl pro žádost a pro odpověď a může být použit pro výše uvedené účely nebo pro jakékoli jiné účely, pro něž je u konkrétního zařízení vyžadován status bezpečnostní prověrky zařízení. Důvod pro šetření musí být žádajícím vnitrostátním bezpečnostním orgánem či určeným bezpečnostním orgánem uveden v poli 7 oddílu pro žádost.

1.4. Podrobnosti obsažené v informačním listu pro bezpečnostní prověrku zařízení nejsou obvykle utajované; když se tedy informační list pro bezpečnostní prověrku zařízení odesílá mezi příslušnými vnitrostátními bezpečnostními orgány/určenými bezpečnostními orgány/Komisí, mělo by se to provádět pokud možno elektronickými prostředky.

1.5. Vnitrostátní bezpečnostní orgány či určené bezpečnostní orgány by měly vyvinout veškeré úsilí, aby odpověděly na žádost informačního listu pro bezpečnostní prověrku zařízení do deseti pracovních dnů.

1.6. Pokud jsou v souvislosti s tímto ujištěním přenášeny jakékoli utajované informace nebo uzavřena smlouva, je třeba informovat vydávající vnitrostátní bezpečnostní orgán či určený bezpečnostní orgán.

Postupy a pokyny pro používání informačního listu pro bezpečnostní prověrku zařízení

Tyto podrobné pokyny jsou určeny pro vnitrostátní bezpečnostní orgán či určený bezpečnostní orgán nebo pro Komisi jakožto veřejného zadavatele, které informační list pro bezpečnostní prověrku zařízení vyplňují. Žádost by měla být napsána nejlépe hůlkovým písmem.

HLAVIČKA	Žadatel uvede celý název vnitrostátního bezpečnostního orgánu/určeného bezpečnostního orgánu a země.
1. **TYP ŽÁDOSTI**	Žádající veřejný zadavatel vybere vhodné zaškrtávací políčko pro typ žádosti informačního listu pro bezpečnostní prověrku zařízení. Uveďte požadovanou úroveň bezpečnostní prověrky. Používají se tyto zkratky: SECRET UE/EU SECRET = S-UE/EU-S CONFIDENTIEL UE/EU CONFIDENTIAL = C-UE/EU-C CIS = komunikační a informační systémy pro zpracování utajovaných informací

2. **PODROBNOSTI O SUBJEKTU**	Pole 1 až 6 jsou zcela zřejmá. V poli 4 se použije standardní dvoumístný kód země. Pole 5 je volitelné.
3. **DŮVOD ŽÁDOSTI**	Uveďte konkrétní důvod žádosti a předložte ukazatele projektu, číslo smlouvy nebo výzvu k podávání nabídek. Upřesněte potřebnou skladovací kapacitu, stupeň utajení komunikačních a informačních systémů atd. Je třeba zahrnout jakékoli stanovené lhůty/data skončení platnosti/data zadání zakázky, jež mohou mít vliv na dokončení bezpečnostní prověrky zařízení.
4. **ŽÁDAJÍCÍ VNITROSTÁTNÍ BEZPEČNOSTNÍ ORGÁN/URČENÝ BEZPEČNOSTNÍ ORGÁN**	Uveďte jméno skutečného žadatele (jménem vnitrostátního bezpečnostního orgánu/určeného bezpečnostního orgánu) a datum žádosti v číselném formátu (dd/mm/rrrr).
5. **ODDÍL PRO ODPOVĚĎ**	Pole 1–5: vyberte vhodná pole. Pole 2: pokud se na bezpečnostní prověrce zařízení pracuje, doporučuje se poskytnout žadateli lhůtu potřebnou ke zpracování (je-li známa). Pole 6: a) Ačkoli se potvrzení platnosti v jednotlivých zemích nebo dokonce zařízeních liší, doporučuje se uvést konec doby platnosti bezpečnostní prověrky zařízení. b) Je-li ujištění o bezpečnostní prověrce zařízení vydáno na neomezenou dobu, je možné toto pole vyškrtnout. c) V souladu s příslušnými vnitrostátními pravidly a předpisy odpovídá za podání žádosti o obnovení bezpečnostní prověrky zařízení žadatel nebo dodavatel/subdodavatel.
6. **POZNÁMKY**	Lze využít pro další informace týkající se bezpečnostní prověrky zařízení, zařízení nebo výše uvedených položek.
7. **VYDÁVAJÍCÍ VNITROSTÁTNÍ BEZPEČNOSTNÍ ORGÁN/URČENÝ BEZPEČNOSTNÍ ORGÁN**	Uveďte jméno poskytujícího orgánu (jménem vnitrostátního bezpečnostního orgánu/určeného bezpečnostního orgánu) a datum odpovědi v číselném formátu (dd/mm/rrrr).

INFORMAČNÍ LIST PRO BEZPEČNOSTNÍ PROVĚRKU ZAŘÍZENÍ

(VZOR)

Všechna pole musí být vyplněna a formulář předán prostřednictvím mezivládních kanálů nebo kanálů mezi vládami a mezinárodními organizacemi.

ŽÁDOST O UJIŠTĚNÍ O BEZPEČNOSTNÍ PROVĚRCE ZAŘÍZENÍ

PRO: _____

(název vnitrostátního bezpečnostního orgánu/určeného bezpečnostního orgánu a země)

V příslušných případech vyplňte kolonky pro odpověď:

[] Poskytněte ujištění o bezpečnostní prověrce zařízení na úrovni: [] S-UE/EU-S [] C-UE/EU-C

pro zařízení uvedené níže

[] včetně ochrany utajovaného materiálu/informací

[] včetně komunikačních a informačních systémů pro zpracování utajovaných informací

[] Zahajte (přímo nebo na odpovídající žádost dodavatele nebo subdodavatele) postup udělení bezpečnostní prověrky zařízení až do stupně utajení ..... včetně, s úrovní ochrany ..... a úrovní komunikačních a informačních systémů ....., pokud zařízení tyto schopnosti na daném stupni zatím nemá.

Potvrďte správnost údajů o zařízení uvedených níže a podle potřeby poskytněte opravy či doplnění.

1.	Celý název zařízení:	Opravy/doplnění:
.....		.....
2.	Celá adresa zařízení:	
.....		.....
3.	Poštovní adresa (pokud se liší od 2)	
.....		.....
4.	Poštovní směrovací číslo/město/země	
.....		.....
5.	Jméno bezpečnostního úředníka	
.....		.....
6.	Telefon/fax/e-mail bezpečnostního úředníka	
.....		.....

7. Tato žádost se podává z následujících důvodů: (uveďte podrobnosti o předsmluvní fázi (výběr návrhů), smlouvě nebo subdodavatelské smlouvě, programu/projektu atd.)

.....

Žádající vnitrostátní bezpečnostní orgán/určený bezpečnostní orgán/ Komise jakožto veřejný zadavatel: Název: ..... Datum: (dd/mm/rrrr) .....

ODPOVĚĎ (do deseti pracovních dnů)

Tímto se potvrzuje, že:

1. [] výše uvedené zařízení je držitelem bezpečnostní prověrky zařízení až do stupně utajení [] S-UE/EU-S

   [] C-UE/EU-C včetně.

2. Výše uvedené zařízení má schopnost chránit utajované informace/materiál:

   [] ano, na úrovni: ..... [] ne.

3. výše uvedené zařízení má akreditovaný/povolený komunikační a informační systém:

   [] ano, na úrovni: ..... [] ne.

4. [] v souvislosti s výše uvedenou žádostí byl zahájen proces bezpečnostní prověrky zařízení. Budete informováni, až bude bezpečnostní prověrka zařízení uznána nebo zamítnuta.

5. [] výše uvedené zařízení není držitelem bezpečnostní prověrky zařízení.

6. Toto ujištění o bezpečnostní prověrce zařízení vyprší dne: ..... (*dd/mm/rrrr*) nebo k jinému dni oznámenému vnitrostátním bezpečnostním orgánem či určeným bezpečnostním orgánem. V případě dřívějšího prohlášení neplatnosti nebo jakýchkoli změn informací uvedených výše budete informováni.

7. Poznámky:

   .....

vydávající vnitrostátní bezpečnostní orgán či určený bezpečnostní orgán *Název: .....* *Datum: (dd/mm/rrrr) .....*

<Místo vyhrazené pro odkaz na platné právní předpisy o ochraně osobních údajů a pro odkaz na povinné informace pro subjekt údajů, např. jak je prováděn článek 13 obecného nařízení o ochraně osobních údajů ([2]).>

([2]) Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (Úř. věst. L 119, 4.5.2016, s. 1).

Dodatek E

Minimální požadavky na ochranu utajovaných informací EU v elektronické podobě se stupněm utajení RESTREINT UE/EU RESTRICTED, s nimiž se nakládá v komunikačním a informačním systému dodavatele

Obecné informace

1. Dodavatel musí zajistit, aby ochrana informací se stupněm utajení RESTREINT UE/EU RESTRICTED vyhovovala minimálním bezpečnostním požadavkům stanoveným v tomto ustanovení o bezpečnosti a jakýmkoli dalším požadavkům doporučeným veřejným zadavatelem nebo případně vnitrostátním bezpečnostním orgánem či určeným bezpečnostním orgánem.

2. Dodavatel odpovídá za splnění bezpečnostních požadavků stanovených v tomto dokumentu.

3. Pro účely tohoto dokumentu komunikační a informační systém zahrnuje veškeré vybavení, které se používá k nakládání s utajovanými informacemi EU, jejich uchovávání a předávání, včetně pracovních stanic, tiskáren, kopírek, faxových přístrojů, serverů, systémů pro správu sítě, ovladačů sítí a komunikačních ovladačů, laptopů, notebooků, tabletů, chytrých telefonů a přenosných paměťových zařízení, jako jsou paměťové jednotky USB, CD a SD karty atd.

4. Zvláštní vybavení, jako jsou kryptografické prostředky, je třeba chránit v souladu se specializovanými bezpečnostními provozními postupy.

5. Dodavatelé musí vytvořit strukturu odpovědnou za správu zabezpečení komunikačních a informačních systémů, které nakládají s informacemi se stupněm utajení RESTREINT UE/EU RESTRICTED, a jmenovat osobu odpovědnou za bezpečnost dotčeného zařízení.

6. Používání informačních technologií (hardware, software nebo služby) v soukromém vlastnictví pracovníků dodavatele k uchovávání či zpracovávání informací se stupněm utajení RESTREINT UE/EU RESTRICTED není povoleno.

7. Akreditace komunikačních a informačních systémů dodavatele, které nakládají s informacemi se stupněm utajení RESTREINT UE/EU RESTRICTED, musí být schválena orgánem pro bezpečnostní akreditaci dotčeného členského státu nebo delegována na bezpečnostního úředníka dodavatele, povolují-li to vnitrostátní právní předpisy.

8. Pouze s informacemi se stupněm utajení RESTREINT UE/EU RESTRICTED, které jsou zašifrovány pomocí schválených kryptografických prostředků, je možné nakládat, uchovávat je či předávat (kabelově nebo bezdrátově) stejně jako jakékoli jiné neutajované informace v rámci smlouvy. Tyto kryptografické prostředky musí schválit EU nebo daný členský stát.

9. Externí zařízení zapojená do údržby či oprav musí být smluvně vázána, aby dodržovala platná ustanovení týkající se nakládání s informacemi se stupněm utajení RESTREINT UE/EU RESTRICTED, která jsou stanovena v tomto dokumentu.

10. Dodavatel musí na žádost veřejného zadavatele nebo příslušného vnitrostátního bezpečnostního orgánu, určeného bezpečnostního orgánu či orgánu pro bezpečnostní akreditaci doložit soulad se smluvní doložkou o bezpečnosti. Pokud je za účelem zajištění souladu s těmito požadavky vyžádán rovněž audit a inspekce postupů a zařízení dodavatele, dodavatelé povolí zástupcům veřejného zadavatele, příslušného vnitrostátního bezpečnostního orgánu/určeného bezpečnostního orgánu/orgánu pro bezpečnostní akreditaci nebo příslušného bezpečnostního orgánu EU provedení tohoto auditu a inspekce.

Fyzická bezpečnost

11. Prostory, ve kterých se komunikační a informační systémy používají k zobrazování, uchovávání, zpracovávání nebo předávání informací se stupněm utajení RESTREINT UE/EU RESTRICTED, nebo prostory, ve kterých jsou servery, systémy pro správu sítě, ovladače sítí a komunikační ovladače pro tyto komunikační a informační systémy, by měly být zřízeny jako samostatné a kontrolované prostory s vhodným systémem kontroly přístupu. Přístup do těchto samostatných a kontrolovaných prostor by měl být omezen na osoby se zvláštním povolením. Aniž je dotčen odstavec 8, vybavení popsané v odstavci 3 musí být uchováváno v takových samostatných a kontrolovaných prostorách.

12. Musí být uplatňovány bezpečnostní mechanismy a/nebo postupy, jejichž cílem je regulovat zavádění vyměnitelných nosičů dat (jako jsou paměťové jednotky USB, velkokapacitní paměťová zařízení nebo CD-RW) do komponent komunikačních a informačních systémů nebo jejich připojování k těmto komponentám.

Přístup ke komunikačním a informačním systémům

13. Přístup ke komunikačním a informačním systémům dodavatele, které nakládají s utajovanými informacemi EU, se povoluje na základě přísného poskytování přístupu jen těm osobám, které utajované informace potřebují znát, a na základě oprávnění personálu.

14. Všechny komunikační a informační systémy musí mít aktualizované seznamy oprávněných uživatelů. Všichni uživatelé musí být při zahájení každého zpracování ověřeni.

15. Hesla, která jsou součástí většiny bezpečnostních opatření zaměřených na identifikaci a ověřování, musí mít délku alespoň devět znaků a musí obsahovat číselné a „zvláštní" znaky (pokud to systém umožňuje), jakož i abecední znaky. Hesla je třeba měnit alespoň jednou za 180 dní. Pokud budou hesla ohrožena nebo prozrazena neoprávněné osobě nebo pokud existuje podezření na takové ohrožení či prozrazení, je třeba je změnit neprodleně.

16. Všechny komunikační a informační systémy musí mít vnitřní kontroly přístupu, aby se zabránilo neoprávněným uživatelům v přístupu k informacím se stupněm utajení RESTREINT UE/EU RESTRICTED nebo v jejich úpravě a rovněž v úpravě systému a bezpečnostních kontrol. Uživatelé musí být z komunikačního a informačního systému automaticky odhlášeni, pokud jsou jejich terminály po určitou předem stanovenou dobu nečinné, nebo komunikační a informační systém musí po 15 minutách nečinnosti aktivovat spořič obrazovky chráněný heslem.

17. Každému uživateli komunikačního a informačního systému je přidělen jedinečný uživatelský účet a uživatelské jméno. Uživatelské účty se musí automaticky uzamknout nejméně po pěti následných nesprávných pokusech o přihlášení.

18. Všichni uživatelé komunikačního a informačního systému si musí být vědomi svých povinností a postupů, jimiž je třeba se řídit za účelem ochrany informací se stupněm utajení RESTREINT UE/EU RESTRICTED v komunikačním a informačním systému. Povinnosti a postupy, jimiž je třeba se řídit, musí být zdokumentovány a uživateli písemně potvrzeny.

19. Specializované bezpečnostní provozní postupy musí být k dispozici pro všechny uživatele a správce a musí obsahovat popisy bezpečnostních rolí a související seznam úkolů, pokynů a plánů.

Účetnictví, audit a reakce na incidenty

20. Každý přístup ke komunikačnímu a informačnímu systému musí být zaevidován.

21. Je třeba zaznamenat následující události:

    a) všechny pokusy o přihlášení, úspěšné i neúspěšné;

    b) odhlášení (včetně případného vypršení časového limitu);

    c) vytvoření, vymazání nebo pozměnění práv a oprávnění přístupu;

    d) vytvoření, vymazání nebo pozměnění hesel.

22. Ve všech výše uvedených případech je třeba sdělit přinejmenším následující informace:

    a) typ události;

    b) uživatelské jméno;

    c) datum a čas;

    d) ID zařízení.

23. Účetní záznamy by měly bezpečnostnímu úředníkovi pomoci vyšetřit potenciální bezpečnostní incidenty. Rovněž mohou být využity za účelem podpory jakýchkoli právních šetření v případě bezpečnostního incidentu. Všechny bezpečnostní záznamy je třeba pravidelně kontrolovat, aby se určily potenciální bezpečnostní incidenty. Účetní záznamy musí být chráněny před neoprávněným smazáním nebo úpravou.

24. Dodavatel musí mít zavedenou strategii reakce pro řešení bezpečnostních incidentů. Uživatelé a správci musí mít pokyny, jak na incidenty reagovat, jak je hlásit a co dělat v mimořádných případech.

25. O ohrožení nebo předpokládaném ohrožení informací se stupněm utajení RESTREINT UE/EU RESTRICTED je třeba podat zprávu veřejnému zadavateli. Zpráva musí obsahovat popis dotčených informací a popis okolností daného ohrožení nebo předpokládaného ohrožení. Všichni uživatelé komunikačního a informačního systému musí vědět, jak podat zprávu o skutečném nebo předpokládaném bezpečnostním incidentu bezpečnostnímu úředníkovi.

Sítě a vzájemné propojení

26. Když je komunikační a informační systém dodavatele, který nakládá s informacemi se stupněm utajení RESTREINT UE/EU RESTRICTED, propojen s komunikačním a informačním systémem, který není akreditován, významně se tím zvýší ohrožení bezpečnosti tohoto komunikačního a informačního systému a informací se stupněm utajení RESTREINT UE/EU RESTRICTED, s nimiž tento systém nakládá. To zahrnuje internet a další veřejné či soukromé komunikační a informační systémy, jako jsou jiné komunikační a informační systémy ve vlastnictví dodavatele nebo subdodavatele. V takovém případě musí dodavatel provést posouzení rizika, aby zjistil dodatečné bezpečnostní požadavky, které je třeba uplatnit v rámci procesu bezpečnostní akreditace. Dodavatel musí veřejnému zadavateli a – vyžadují-li to vnitrostátní právní předpisy – příslušnému orgánu pro bezpečnostní akreditaci předložit prohlášení o vyhovění požadavkům osvědčující, že komunikační a informační systém dodavatele a související propojení byly akreditovány k nakládání s utajovanými informacemi EU se stupněm utajení RESTREINT UE/EU RESTRICTED.

27. Vzdálený přístup z jiných systémů ke službám LAN (např. vzdálený přístup k e-mailu a vzdálené podpoře systému) je zakázán, pokud nejsou uplatněna zvláštní bezpečnostní opatření a nejsou schválena veřejným zadavatelem a – pokud to vyžadují vnitrostátní právní předpisy – orgánem pro bezpečnostní akreditaci.

Správa konfigurace

28. Podrobná konfigurace hardwaru a softwaru, jež vyplývá z akreditační/schvalovací dokumentace (včetně systémových a síťových diagramů), musí být dostupná a je třeba ji pravidelně udržovat.

29. Bezpečnostní úředník dodavatele musí provádět kontroly konfigurace hardwaru a softwaru, aby zajistil, že nebyl zaveden žádný neoprávněný hardware či software.

30. Změny konfigurace komunikačních a informačních systémů dodavatelů musí být posouzeny z hlediska jejich bezpečnostních důsledků a schváleny bezpečnostním úředníkem a – pokud to vyžadují vnitrostátní právní předpisy – orgánem pro bezpečnostní akreditaci.

31. Alespoň jednou za čtvrtletí je třeba provést sken systému, aby se zjistila slabá místa v zabezpečení. Software na zjišťování malwaru musí být nainstalován a průběžně aktualizován. Tento software by měl být pokud možno držitelem vnitrostátního nebo uznávaného mezinárodního schválení, v opačném případě by měl splňovat obecně uznávanou průmyslovou normu.

32. Dodavatel musí vytvořit plán pro zachování kontinuity provozu. Je třeba stanovit postupy zálohování, které budou zaměřeny na řešení následujících otázek:

    a) frekvence zálohování;

    b) požadavky na uchovávání na místě (v ohnivzdorných kontejnerech) nebo mimo místo;

    c) kontrola oprávněného přístupu ke kopiím záloh.

Vyčištění a zničení

33. V případě komunikačních a informačních systémů nebo nosičů pro ukládání dat, na nichž byly někdy uloženy informace se stupněm utajení RESTREINT UE/EU RESTRICTED, je třeba celý systém nebo paměťové médium před jeho odstraněním vyčistit:

    a) paměť typu flash (např. paměťové jednotky USB, SD karty, polovodičové pevné disky (SSD), hybridní pevné disky (HHD)) musí být alespoň třikrát přepsána a poté ověřena, aby se zajistilo, že původní obsah nemůže být obnoven, nebo je třeba ji vymazat pomocí schváleného softwaru pro mazání;

    b) magnetické nosiče (např. pevné disky) musí být přepsány nebo odmagnetizovány;

c) optické nosiče (např. CD a DVD) je třeba rozřezat skartovacím strojem nebo rozdrtit;

d) v případě jakýchkoli jiných paměťových médií by měl být konzultován veřejný zadavatel nebo případně vnitrostátní bezpečnostní orgán, určený bezpečnostní orgán či orgán pro bezpečnostní akreditaci ohledně bezpečnostních požadavků, které mají být splněny.

34. Předtím, než jsou nosiče pro ukládání dat poskytnuty jakémukoli subjektu, který nemá oprávnění k přístupu k informacím se stupněm utajení RESTREINT UE/EU RESTRICTED (např. pro účely údržby), je třeba z nich informace se stupněm utajení RESTREINT UE/EU RESTRICTED odstranit.

PŘÍLOHA IV

Bezpečnostní prověrky zařízení a bezpečnostní prověrky personálu pro dodavatele, kteří nakládají s informacemi se stupněm utajení RESTREINT UE/EU RESTRICTED, a vnitrostátní bezpečnostní orgány/určené bezpečnostní orgány, jež požadují oznamování utajovaných smluv se stupněm utajení RESTREINT UE/EU RESTRICTED [1]

Členský stát	Bezpečnostní prověrka zařízení		Oznámení smlouvy nebo subdodavatelské smlouvy zahrnující informace se stupněm utajení R-UE/EU-R vnitrostátnímu bezpečnostnímu orgánu či určenému bezpečnostnímu orgánu		Bezpečnostní prověrka personálu	
	ANO	NE	ANO	NE	ANO	NE
Belgie		X		X		X
Bulharsko		X		X		X
Česko		X		X		X
Dánsko	X		X		X	
Německo		X		X		X
Estonsko	X		X			X
Irsko		X		X		X
Řecko	X			X	X	
Španělsko		X	X			X
Francie		X		X		X
Chorvatsko		X	X			X
Itálie		X	X			X
Kypr		X	X			X
Lotyšsko		X		X		X

[1] Tyto vnitrostátní požadavky na bezpečnostní prověrku zařízení a bezpečnostní prověrku personálu a oznamování smluv zahrnujících informace se stupněm utajení RESTREINT UE/EU RESTRICTED nesmí ukládat žádné další povinnosti jiným členským státům nebo dodavatelům v jejich pravomoci.
Pozn.: Oznamování smluv zahrnujících informace se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL a SECRET UE/EU SECRET je povinné.

Členský stát	Bezpečnostní prověrka zařízení		Oznámení smlouvy nebo subdodavatelské smlouvy zahrnující informace se stupněm utajení R-UE/EU-R vnitrostátnímu bezpečnostnímu orgánu či určenému bezpečnostnímu orgánu		Bezpečnostní prověrka personálu	
	ANO	NE	ANO	NE	ANO	NE
Litva	X		X			X
Lucembursko	X		X		X	
Maďarsko		X		X		X
Malta		X		X		X
Nizozemsko	X (pouze pro zakázky týkající se obrany)		X (pouze pro zakázky týkající se obrany)			X
Rakousko		X		X		X
Polsko		X		X		X
Portugalsko		X		X		X
Rumunsko		X		X		X
Slovinsko	X		X			X
Slovensko	X		X			X
Finsko		X		X		X
Švédsko	X (pouze pro zakázky týkající se obrany)		X (pouze pro zakázky týkající se obrany)		X (pouze pro zakázky týkající se obrany)	
Spojené království		X		X		X

PŘÍLOHA V

SEZNAM ÚTVARŮ VNITROSTÁTNÍCH BEZPEČNOSTNÍCH ORGÁNŮ/URČENÝCH BEZPEČNOSTNÍCH ORGÁNŮ ODPOVĚDNÝCH ZA POSTUPY VYŘIZOVÁNÍ SOUVISEJÍCÍ S PRŮMYSLOVOU BEZPEČNOSTÍ

BELGIE

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

   (Příslušné orgány uvedené výše provádějí schvalovací postupy pro vydávání bezpečnostních prověrek zařízení právním subjektům, které žádají o uzavření utajované smlouvy, a bezpečnostních prověrek personálu osobám provádějícím utajovanou smlouvu pro potřeby těchto orgánů.)

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

   (Výše uvedená bezpečnostní služba provádí schvalovací postupy pro vydávání bezpečnostních prověrek zařízení a bezpečnostních prověrek personálu všem dalším právním subjektům a osobám v této zemi, jež žádají o uzavření utajované smlouvy nebo takovou smlouvu provádějí.)

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

NĚMECKO

1. Pro záležitosti týkající se politiky průmyslové bezpečnosti, bezpečnostních prověrek zařízení, plánů na přepravu (vyjma kryptografické ochrany/kontrolovaných kryptografických prostředků):
Federal Ministry of Economic Affairs and Energy
Industrial Security Division - ZB3
Villemombler S. 76
53123 Bonn
Tel. +49 228996154028
Fax +49 228996152676
E-mail: dsagermany-zb3@bmwi.bund.de (office email address)

2. Pro standardní žádosti o návštěvu německých podniků:
Federal Ministry of Economic Affairs and Energy
Industrial Security Division – ZB2
Villemombler S. 76
53123 Bonn
Tel. +49 228996152401
Fax +49 228996152603
E-mail: zb2-international@bmwi.bund.de (office email address)

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

ESTONSKO

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

IRSKO

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

ŘECKO

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

ŠPANĚLSKO

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
Pro záležitosti týkající se bezpečnostních prověrek personálu: asip@areatec.com
Pro plány na přepravu a mezinárodní návštěvy: sp-ivtco@areatec.com

FRANCIE

National Security Authority (NSA) (pro politiku a provádění v oblastech mimo obranný průmysl)
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 (pro provádění v obranném průmyslu)
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: pro formuláře a odchozí žádosti o návštěvu: dga-ssdi.ai.fct@intradef.gouv.fr
pro příchozí žádosti o návštěvu: dga-ssdi.visit.fct@intradef.gouv.fr

CHORVATSKO

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

ITÁLIE

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

KYPR

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

LUCEMBURSKO

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

NIZOZEMSKO

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

RAKOUSKO

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

POLSKO

Internal Security Agency
Department for the Protection of Classified Information
Rakowiecka 2 A
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

FINSKO

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

SPOJENÉ KRÁLOVSTVÍ

UK National Security Authority
Room 335, 3rd Floor
70 Whitehall
London
SW1 A 2AS
Tel. +44 2072765497, +44 2072765645
E-mail: UK-NSA@cabinet-office.x.gsi.gov.uk