ODLUKA KOMISIJE (EU, Euratom) 2019/1963

od 17. listopada 2019.

o utvrđivanju provedbenih pravila o gospodarskoj sigurnosti u pogledu klasificiranih ugovora o javnoj nabavi

EUROPSKA KOMISIJA,

uzimajući u obzir Ugovor o funkcioniranju Europske unije, a posebno njegov članak 249.,

uzimajući u obzir Ugovor o osnivanju Europske zajednice za atomsku energiju, a posebno njegov članak 106.,

uzimajući u obzir Odluku Komisije (EU, Euratom) 2015/443 od 13. ožujka 2015. o sigurnosti u Komisiji ([1]),

uzimajući u obzir Odluku Komisije (EU, Euratom) 2015/444 od 13. ožujka 2015. o sigurnosnim propisima za zaštitu klasificiranih podataka EU-a ([2]),

uzimajući u obzir Odluku Komisije (EU, Euratom) 2017/46 od 10. siječnja 2017. o sigurnosti komunikacijskih i informacijskih sustava u Europskoj komisiji ([3]),

nakon savjetovanja s Komisijinom stručnom skupinom za sigurnost, u skladu s člankom 41. stavkom 5. Odluke (EU, Euratom) 2015/444,

budući da:

(1) Člancima 41., 42., 47. i 48. Odluke (EU, Euratom) 2015/444 propisuje se da će se detaljne odredbe za dopunu i potporu poglavlja 6. Odluke utvrditi u provedbenim pravilima o gospodarskoj sigurnosti, kojima će se urediti pitanja kao što su natječajni postupak, sklapanje klasificiranih ugovora, uvjerenja o sigurnosnoj provjeri pravne osobe, uvjerenja o sigurnosnoj provjeri osobe, posjeti te slanje i prijenos klasificiranih podataka Europske unije (EUCI).

(2) U Odluci (EU, Euratom) 2015/444 navodi se da je klasificirane ugovore potrebno provesti u bliskoj suradnji s nacionalnim sigurnosnim tijelom, zaduženim sigurnosnim tijelom ili bilo kojim drugim nadležnim tijelom dotične države članice; države članice sporazumjele su se da će osigurati da je svaki subjekt u njihovoj nadležnosti koji smije zaprimati ili generirati klasificirane podatke koji potječu od Komisije uspješno prošao odgovarajuću sigurnosnu provjeru te da je sposoban osigurati zaštitu odgovarajućeg stupnja tajnosti koja je istovjetna razini zaštite klasificiranih podataka koja se osigurava sigurnosnim pravilima Vijeća Europske unije za zaštitu klasificiranih podataka EU-a koji nose odgovarajuću oznaku stupnja tajnosti, kako je to utvrđeno u Sporazumu između država članica Europske unije, koje su se sastale u okviru Vijeća, o zaštiti klasificiranih podataka koji se razmjenjuju u interesu Europske unije (2011/C 202/05) ([4]).

(3) Vijeće, Komisija i Visoki predstavnik Unije za vanjske poslove i sigurnosnu politiku sporazumjeli su se da će osigurati najveću moguću dosljednost u primjeni sigurnosnih pravila za zaštitu klasificiranih podataka EU-a, uzimajući u obzir posebne institucijske i organizacijske potrebe, u skladu s izjavama priloženima zapisniku sa sjednice Vijeća na kojoj je donesena Odluka Vijeća 2013/488/EU ([5]) o sigurnosnim propisima za zaštitu klasificiranih podataka EU-a.

(4) Stoga bi se provedbenim pravilima Komisije o gospodarskoj sigurnosti u pogledu klasificiranih ugovora trebala osigurati i najveća moguća dosljednost te je potrebno uzeti u obzir smjernice o gospodarskoj sigurnosti koje je Sigurnosni odbor Vijeća odobrio 13. prosinca 2016. te članke 7. i 22. Direktive 2009/81/EZ Europskog parlamenta i Vijeća ([6]).

(5) Komisija je 4. svibnja 2016. donijela odluku ([7]) kojom je člana Komisije nadležnog za sigurnosna pitanja ovlastila da u ime Komisije i pod njezinom odgovornošću donese provedbena pravila propisana člankom 60. Odluke (EU, Euratom) 2015/444,

([1]) SL L 72, 17.3.2015., str. 41.
([2]) SL L 72, 17.3.2015., str. 53.
([3]) SL L 6, 11.1.2017., str. 40.
([4]) SL C 202, 8.7.2011., str. 13.
([5]) Odluka Vijeća 2013/488/EU od 23. rujna 2013. o sigurnosnim propisima za zaštitu klasificiranih podataka EU-a (SL L 274, 15.10.2013., str. 1.).
([6]) Direktiva 2009/81/EZ Europskog Parlamenta i Vijeća od 13. srpnja 2009. o usklađivanju postupaka nabave za određene ugovore o radovima, ugovore o nabavi robe i ugovore o uslugama koje sklapaju javni naručitelji ili naručitelji u području obrane i sigurnosti (SL L 216, 20.8.2009., str. 76.).
([7]) Odluka Komisije od 4. svibnja 2016. o ovlaštenju povezanom sa sigurnošću [C(2016) 2797 final].

DONIJELA JE OVU ODLUKU:

POGLAVLJE 1.

OPĆE ODREDBE

Članak 1.

Predmet i područje primjene

1. Ovom Odlukom utvrđuju se provedbena pravila o gospodarskoj sigurnosti u pogledu klasificiranih ugovora o javnoj nabavi kojima se podupire provedba Odluke (EU, Euratom) 2015/444, a posebno njezina poglavlja 6.

2. U ovoj se Odluci utvrđuju posebni zahtjevi kako bi se osiguralo da gospodarski subjekti štite klasificirane podatke EU-a (EUCI) u fazi prije sklapanja ugovora, tijekom životnog ciklusa klasificiranih ugovora koje je sklopila Europska komisija te u podugovorima koje su sklopili ugovaratelji Komisije.

3. Ova Odluka odnosi se na podatke klasificirane sljedećim stupnjevima tajnosti:

(a) RESTREINT UE/EU RESTRICTED;

(b) CONFIDENTIEL UE/EU CONFIDENTIAL;

(c) SECRET UE/EU SECRET.

Članak 2.

Odgovornost unutar Komisije

1. U okviru odgovornosti opisanih u Financijskoj uredbi ([8]) svaki dužnosnik za ovjeravanje Komisijina javnog naručitelja osigurava da se u klasificiranom ugovoru upućuje na minimalne standarde gospodarske sigurnosti utvrđene u poglavlju 6. Odluke (EU, Euratom) 2015/444 i ovim provedbenim pravilima te, prema potrebi, obavijesti o nadmetanju ili pozivu na dostavu ponuda i da su ti standardi zadovoljeni tijekom provedbe.

2. U tu svrhu dotični dužnosnik za ovjeravanje u svim se fazama savjetuje sa sigurnosnim tijelom Komisije o pitanjima sigurnosnih elemenata klasificiranog ugovora, programa ili projekta te o sklopljenim ugovorima obavještava lokalnog službenika za sigurnost. Odluku o stupnju tajnosti određenih tema donosi javni naručitelj uzimajući u obzir vodič za stupnjeve tajnosti.

3. Pri poštovanju zahtjeva iz ovih provedbenih pravila sigurnosno tijelo Komisije blisko surađuje s nacionalnim sigurnosnim tijelima (NST) i zaduženim sigurnosnim tijelima (ZST) dotične države članice, osobito u pogledu uvjerenja o sigurnosnoj provjeri pravne osobe (USPPO) i uvjerenja o sigurnosnoj provjeri osobe (USP), postupaka za posjete i planova prijevoza.

POGLAVLJE 2.

POSTUPANJE S POZIVIMA ZA PODNOŠENJE PONUDA ZA KLASIFICIRANE UGOVORE

Članak 3.

Osnovna načela

1. Klasificirani ugovori dodjeljuju se samo gospodarskim subjektima koji su registrirani u državi članici ili gospodarskim subjektima koji su registrirani u trećoj zemlji ili ih je osnovala međunarodna organizacija, pri čemu je ta treća zemlja ili međunarodna organizacija sklopila sporazum o sigurnosti podataka s Europskom unijom ili administrativni dogovor s Komisijom ([9]).

2. Prije objavljivanja poziva na dostavu ponuda za klasificirani ugovor javni naručitelj određuje stupanj tajnosti svakog podatka koji bi se mogao dostaviti ponuditeljima. Javni naručitelj određuje i najviši stupanj tajnosti svakog podatka koji će se stvoriti tijekom izvršenja ugovora, programa ili projekta, ili barem očekivanu količinu i vrstu podataka koji će se proizvesti ili s kojima će se postupati, te potrebu za klasificiranim komunikacijskim i informacijskim sustavom (CIS).

([8]) Uredba (EU, Euratom) 2018/1046 Europskog parlamenta i Vijeća od 18. srpnja 2018. o financijskim pravilima koja se primjenjuju na opći proračun Unije, o izmjeni uredaba (EU) br. 1296/2013, (EU) br. 1301/2013, (EU) br. 1303/2013, (EU) br. 1304/2013, (EU) br. 1309/2013, (EU) br. 1316/2013, (EU) br. 223/2014, (EU) br. 283/2014 i Odluke br. 541/2014/EU te o stavljanju izvan snage Uredbe (EU, Euratom) br. 966/2012 (SL L 193, 30.7.2018., str. 1.).

([9]) Popis sporazuma koje je sklopio EU i administrativnih dogovora koje je sklopila Europska komisija, u okviru kojih se klasificirani podaci EU-a mogu razmjenjivati s trećim zemljama i međunarodnim organizacijama, nalazi se na internetskim stranicama Komisije.

3. Javni naručitelj osigurava da se u obavijestima o nadmetanju za klasificirane ugovore pružaju informacije o posebnim sigurnosnim obvezama povezanima s klasificiranim podacima. U Prilogu I. nalazi se primjer predloška informacija za obavijesti o nadmetanju.

4. Javni naručitelj osigurava da se podaci klasificirani stupnjem tajnosti RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET otkrivaju ponuditeljima tek nakon što potpišu ugovor o povjerljivosti podataka, kojim se ponuditelje obvezuje da s klasificiranim podacima EU-a postupaju i štite ih u skladu s Odlukom (EU, Euratom) 2015/444 i njezinim provedbenim pravilima.

5. Svi ugovaratelji koji postupaju s podacima klasificiranima stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET ili ih čuvaju u svojim objektima tijekom izvršenja samog klasificiranog ugovora ili u fazi prije sklapanja ugovora moraju imati USPPO potrebne razine. U nastavku su utvrđena tri scenarija koja mogu nastati tijekom faze dostave ponuda za klasificirane ugovore koji obuhvaćaju klasificirane podatke EU-a stupnja tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET:

(a) nema pristupa klasificiranim podacima EU-a stupnja tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET tijekom faze dostave ponuda:

Ako se obavijest o nadmetanju ili poziv na dostavu ponuda odnosi na ugovor koji će obuhvaćati klasificirane podatke EU-a stupnja tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET, ali ponuditelj u fazi dostave ponuda ne treba postupati s tim podacima, ponuditelj koji nema USPPO potrebne razine ne može se isključiti iz procesa nadmetanja zato što nema USPPO;

(b) pristup klasificiranim podacima EU-a stupnja tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET u prostorima javnog naručitelja tijekom faze dostave ponuda:

Pristup se odobrava osoblju ponuditelja koje ima USP potrebne razine i za koje je utvrđena nužnost pristupa podacima. Prije nego što odobri taj pristup, javni naručitelj preko sigurnosnog tijela Komisije provjerava kod nadležnog NST-a/ZST-a je li USPPO u toj fazi potreban i u skladu s nacionalnim zakonima i propisima;

(c) postupanje s klasificiranim podacima EU-a stupnja tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET ili njihovo čuvanje u prostorima ponuditelja tijekom faze dostave ponuda:

Ako se u obavijesti o nadmetanju ili pozivu na dostavu ponuda od ponuditelja zahtijeva da postupa s klasificiranim podacima EU-a ili ih čuva u svojim prostorima, ponuditelj mora imati USPPO potrebne razine. U takvim okolnostima javni naručitelj preko sigurnosnog tijela Komisije dobiva od nadležnog NST-a/ZST-a uvjerenje da je ponuditelju odobren odgovarajući USPPO. Pristup se odobrava osoblju ponuditelja koje ima USP potrebne razine i za koje je utvrđena nužnost pristupa podacima.

6. USPPO u načelu nije potreban za pristup podacima stupnja tajnosti RESTREINT UE/EU RESTRICTED, ni u fazi dostave ponuda ni za izvršenje ugovora. Ako države članice zahtijevaju USPPO za ugovore ili podugovore stupnja tajnosti RESTREINT UE/EU RESTRICTED u skladu sa svojim nacionalnim zakonima i propisima, kako je navedeno u Prilogu IV., tim se nacionalnim zahtjevima ne nalaže nikakva dodatna obveza drugim državama članicama niti se iz povezanih ugovora/podugovora ili nadmetanja za njih isključuju ponuditelji, ugovaratelji ili podugovaratelji iz država članica koje nemaju takve zahtjeve u pogledu USPPO-a za pristup podacima stupnja tajnosti RESTREINT UE/EU RESTRICTED. Ti se ugovori izvršavaju u državama članicama u skladu s njihovim nacionalnim zakonima i propisima.

7. Ako je USPPO potreban za izvršenje klasificiranog ugovora, javni naručitelj preko sigurnosnog tijela Komisije podnosi zahtjev NST-u/ZST-u ugovaratelja koristeći se informativnim obrascem o uvjerenju o sigurnosnoj provjeri pravne osobe (USPPO). Dodatak D Prilogu III. sadržava primjer informativnog obrasca o uvjerenju o sigurnosnoj provjeri pravne osobe ([10]). Klasificirani ugovor ne dodjeljuje se sve dok NST/ZST ugovaratelja ne potvrdi da ponuditelj ima USPPO. Odgovor na informativni obrazac o uvjerenju o sigurnosnoj provjeri pravne osobe dostavlja se u roku od deset radnih dana od datuma podnošenja zahtjeva.

([10]) Drugi upotrijebljeni obrasci mogu se razlikovati od primjera iz ovih provedbenih pravila.

Članak 4.

Podugovaranje s klasificiranim ugovorima

1. Uvjeti pod kojima ugovaratelj kojemu je dodijeljen klasificirani ugovor Komisije može sklapati podugovore utvrđuju se u pozivu na dostavu ponuda i ugovornoj dokumentaciji. Ako je klasificiranim ugovorom dopušteno davanje nekih njegovih dijelova u podugovor, to podugovaranje podliježe prethodnoj pisanoj suglasnosti javnog naručitelja. Prije davanja suglasnosti javni naručitelj savjetuje se sa sigurnosnim tijelom Komisije.

2. Klasificirani ugovori daju se u podugovor samo gospodarskim subjektima koji su registrirani u državi članici ili gospodarskim subjektima koji su registrirani u trećoj zemlji ili ih je osnovala međunarodna organizacija, pri čemu je ta treća zemlja ili međunarodna organizacija sklopila sporazum o sigurnosti podataka s EU-om ili administrativni dogovor s Komisijom ([11]).

POGLAVLJE 3.

SKLAPANJE KOMISIJINIH KLASIFICIRANIH UGOVORA

Članak 5.

Osnovna načela

1. Pri sklapanju klasificiranih ugovora javni naručitelj zajedno sa sigurnosnim tijelom Komisije osigurava da ugovor obuhvaća obveze ugovaratelja u pogledu zaštite klasificiranih podataka EU-a koji su dostavljeni tom ugovaratelju ili nastali pri izvršenju ugovora. Sigurnosni zahtjevi povezani s pojedinim ugovorom u obliku su pisma o sigurnosnim aspektima (SAL). Primjer predloška pisma o sigurnosnim aspektima nalazi se u Prilogu III.

2. Prije potpisivanja klasificiranog ugovora javni naručitelj nakon savjetovanja sa sigurnosnim tijelom Komisije priprema vodič za stupnjeve tajnosti (SCG) za zadaće koje će se obavljati i podatke nastale pri izvršenju ugovora ili, ako je primjenjivo, na razini programa ili projekta. Vodič za stupnjeve tajnosti dio je pisma o sigurnosnim aspektima.

3. Sigurnosni zahtjevi povezani s pojedinim programom ili projektom imaju oblik sigurnosnih uputa za program (ili projekt) (SUP). Sigurnosne upute za program ili projekt mogu se izraditi upotrebom odredbi iz predloška pisma o sigurnosnim aspektima kako je utvrđeno u Prilogu III. SUP sastavlja služba Komisije koja upravlja programom ili projektom, u bliskoj suradnji sa sigurnosnim tijelom Komisije, te ga u procesu savjetovanja podnosi Komisijinoj stručnoj skupini za sigurnost. Ako je ugovor dio programa ili projekta s vlastitim SUP-om, pismo o sigurnosnim aspektima ugovora ima pojednostavnjeni oblik te se u njemu upućuje na sigurnosne odredbe utvrđene u SUP-u programa ili projekta.

4. Javni naručitelj smatra se autorom klasificiranih podataka koji su stvoreni i s kojima se postupa radi izvršenja ugovora.

5. Javni naručitelj preko sigurnosnog tijela Komisije obavještava NST-ove/ZST-ove svih ugovaratelja i podugovaratelja o sklapanju klasificiranih ugovora ili podugovora te o produljenju ili prijevremenom raskidu takvih ugovora ili podugovora. Popis zahtjeva po zemljama naveden je u Prilogu IV.

6. Ugovori koji obuhvaćaju podatke klasificirane stupnjem tajnosti RESTREINT UE/EU RESTRICTED sadržavaju ugovornu klauzulu o sigurnosti kojom odredbe utvrđene u Dodatku E Prilogu III. postaju obvezujuće za ugovaratelja. Ti ugovori obuhvaćaju pismo o sigurnosnim aspektima u kojem se utvrđuju minimalni zahtjevi za postupanje s podacima stupnja tajnosti RESTREINT UE/EU RESTRICTED, uključujući aspekte o informacijskoj sigurnosti i posebne zahtjeve koje ugovaratelj kojemu je javni naručitelj prenio ovlast treba ispuniti u svrhu akreditacije CIS-a ugovaratelja koji postupa s podacima stupnja tajnosti RESTREINT UE/EU RESTRICTED.

([11]) Popis sporazuma koje je sklopio EU i administrativnih dogovora koje je sklopila Europska komisija, u okviru kojih se klasificirani podaci EU-a mogu razmjenjivati s trećim zemljama i međunarodnim organizacijama, nalazi se na internetskim stranicama Komisije.

7. Ako se ponuditeljima ili mogućim ugovarateljima dostavljaju podaci stupnja tajnosti RESTREINT UE/EU RESTRICTED, minimalni zahtjevi iz stavka 6. uvrštavaju se u ponude ili odgovarajuće ugovore o povjerljivosti podataka sklopljene u fazi natječaja.

8. Ako se to zahtijeva nacionalnim zakonima i propisima država članica, NST-ovi/ZST-ovi osiguravaju da ugovaratelji ili podugovaratelji u njihovoj nadležnosti poštuju primjenjive sigurnosne odredbe za zaštitu podataka stupnja tajnosti RESTREINT UE/EU RESTRICTED te provode posjete radi provjere objekata ugovaratelja koji se nalaze na njihovu državnom području. Ako NST/ZST nema takvu obvezu, javni naručitelj osigurava da ugovaratelj provodi potrebne sigurnosne odredbe utvrđene u Prilogu III.

Članak 6.

Pristup osoblja ugovaratelja i podugovaratelja klasificiranim podacima EU-a

1. Služba Komisije kao javni naručitelj osigurava da klasificirani ugovori obuhvaćaju odredbe u kojima se navodi da se osoblju ugovaratelja ili podugovaratelja kojemu je za potrebe izvršenja klasificiranog ugovora ili podugovora potreban pristup klasificiranim podacima EU-a takav pristup može odobriti samo u sljedećim slučajevima:

(a) za osoblje je utvrđena nužnost pristupa podacima;

(b) nadležni NST/ZST ili drugo nadležno sigurnosno tijelo odobrilo je USP odgovarajuće razine za podatke klasificirane stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET;

(c) osoblje je upoznato s primjenjivim sigurnosnim pravilima za zaštitu klasificiranih podataka EU-a te je dalo izjavu u preuzimanju odgovornosti povezanih sa zaštitom takvih podataka.

2. Ako ugovaratelj ili podugovaratelj želi na radno mjesto za koje je potreban pristup klasificiranim podacima EU-a stupnja tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET zaposliti državljanina zemlje koja nije članica EU-a, odgovornost je tog ugovaratelja ili podugovaratelja da pokrene postupak za sigurnosnu provjeru te osobe u skladu s nacionalnim zakonima i propisima koji se primjenjuju na lokaciji na kojoj je potrebno odobriti pristup klasificiranim podacima EU-a.

POGLAVLJE 4.

POSJETI POVEZANI S KLASIFICIRANIM UGOVORIMA

Članak 7.

Osnovna načela

1. Ako je Komisiji, ugovarateljima ili podugovarateljima za potrebe izvršenja klasificiranog ugovora potreban pristup podacima klasificiranima stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET u prostorima jednih ili drugih, posjeti se organiziraju u dogovoru s dotičnim NST-om/ZST-om ili drugim nadležnim sigurnosnim tijelom.

2. Na posjete iz stavka 1. primjenjuju se sljedeći zahtjevi:

(a) posjeti se obavljaju u službene svrhe povezane s klasificiranim ugovorom koji je sklopila Komisija;

(b) kako bi pristupili klasificiranim podacima EU-a koji su dostavljeni ili nastali pri izvršenju klasificiranog ugovora koji je sklopila Komisija, svi posjetitelji moraju imati USP potrebne razine i utvrđenu nužnost pristupa podacima.

Članak 8.

Zahtjevi za posjete

1. Posjeti ugovaratelja objektima drugih ugovaratelja ili prostorima Komisije koji obuhvaćaju pristup podacima klasificiranima stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET organiziraju se u skladu sa sljedećim postupkom:

(a) službenik za sigurnost objekta koji šalje posjetitelja ispunjava sve relevantne dijelove obrasca zahtjeva za posjet te ga podnosi NST-u/ZST-u objekta. Predložak obrasca zahtjeva za posjet nalazi se u Dodatku C Prilogu III.;

(b) NST/ZST objekta koji šalje posjetitelja treba potvrditi USP posjetitelja prije nego što NST-u/ZST-u objekta koji prima posjetitelja (ili sigurnosnom tijelu Komisije ako se posjećuju prostorije Komisije) podnese zahtjev za posjet;

(c) službenik za sigurnost objekta koji šalje posjetitelja zatim od svojeg NST-a/ZST-a dobiva odgovor NST-a/ZST-a objekta koji prima posjetitelja (ili sigurnosnog tijela Komisije), kojim se zahtjev za posjet odobrava ili odbija;

(d) zahtjev za posjet smatra se odobrenim ako do pet radnih dana prije datuma posjeta nije uložen nikakav prigovor.

2. Posjeti dužnosnika Komisije objektima ugovaratelja koji obuhvaćaju pristup podacima klasificiranima stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET organiziraju se u skladu sa sljedećim postupkom:

(a) posjetitelj ispunjava sve relevantne dijelove obrasca zahtjeva za posjet i podnosi ga sigurnosnom tijelu Komisije;

(b) sigurnosno tijelo Komisije potvrđuje USP posjetitelja prije nego što NST-u/ZST-u objekta koji prima posjetitelja podnese zahtjev za posjet;

(c) sigurnosno tijelo Komisije dobiva od NST-a/ZST-a objekta koji prima posjetitelja odgovor kojim se zahtjev za posjet odobrava ili odbija;

(d) zahtjev za posjet smatra se odobrenim ako do pet radnih dana prije datuma posjeta nije uložen nikakav prigovor.

3. Zahtjev za posjet može se odnositi na samo jedan posjet ili više njih. U slučaju više posjeta zahtjev za posjet može vrijediti najviše jednu godinu od zatraženog datuma početka.

4. Valjanost zahtjeva za posjet ne može biti dulja od valjanosti USP-a posjetitelja.

5. Zahtjev za posjet u pravilu se podnosi nadležnom sigurnosnom tijelu objekta koji prima posjetitelja najmanje 15 radnih dana prije datuma posjeta.

Članak 9.

Postupci za posjete

1. Prije nego što posjetitelju odobri pristup klasificiranim podacima EU-a, ured za sigurnost objekta koji prima posjetitelja poštuje sve sigurnosne postupke i pravila povezane s posjetom koje je utvrdio NST/ZST tog objekta.

2. Po dolasku u objekt koji prima posjetitelja posjetitelji svoj identitet dokazuju predočenjem važeće osobne iskaznice ili putovnice. Ti identifikacijski podaci odgovaraju podacima navedenima u zahtjevu za posjet.

3. Objekt koji prima posjetitelja osigurava da se vodi evidencija svih posjetitelja, što podrazumijeva njihova imena, organizacije koje predstavljaju, datum isteka USP-a, datum posjeta i imena osoba koje su posjetili. Ta se evidencija čuva najmanje pet godina ili dulje ako se to zahtijeva nacionalnim pravilima i propisima zemlje u kojoj se nalazi objekt koji prima posjetitelja.

Članak 10.

Neposredno organizirani posjeti

1. U kontekstu posebnih projekata, relevantni NST/ZST i sigurnosno tijelo Komisije mogu se sporazumjeti o postupku prema kojem se posjeti za konkretne klasificirane ugovore mogu organizirati neposredno između službenika za sigurnost posjetitelja i službenika za sigurnost objekta koji se posjećuje. Predložak obrasca koji treba upotrijebiti u tu svrhu nalazi se u Dodatku C Prilogu III. Takav izvanredni postupak utvrđuje se u SUP-u ili drugim posebnim aranžmanima. U takvim se slučajevima ne primjenjuju postupci utvrđeni u članku 8. i članku 9. stavku 1.

2. Posjeti koji obuhvaćaju pristup podacima klasificiranima stupnjem tajnosti RESTREINT UE/EU RESTRICTED organiziraju se neposredno između subjekta koji šalje i subjekta koji prima posjetitelja, pri čemu nije potrebno slijediti postupke iz članka 8. i članka 9. stavka 1.

POGLAVLJE 5.

SLANJE I PRIJENOS KLASIFICIRANIH PODATAKA EU-A PRI IZVRŠENJU KLASIFICIRANIH UGOVORA

Članak 11.

Osnovna načela

Javni naručitelj osigurava da su sve odluke povezane sa slanjem i prijenosom klasificiranih podataka EU-a u skladu s Odlukom (EU, Euratom) 2015/444 i njezinim provedbenim pravilima, kao i s uvjetima klasificiranog ugovora, uključujući suglasnost autora podatka.

Članak 12.

Elektroničko postupanje s podacima

1. Elektroničko postupanje s klasificiranim podacima EU-a i elektroničko slanje tih podataka provode se u skladu s poglavljima 5. i 6. Odluke (EU, Euratom) 2015/444 i njezinim provedbenim pravilima.

Komunikacijske i informacijske sustave koji su u vlasništvu ugovaratelja i koji se koriste za postupanje s klasificiranim podacima EU-a za izvršenje ugovora („CIS ugovaratelja”) mora akreditirati nadležno tijelo za sigurnosnu akreditaciju (SAA). Elektroničko slanje klasificiranih podataka EU-a mora biti zaštićeno kriptografskim proizvodima odobrenima u skladu s člankom 36. stavkom 4. Odluke (EU, Euratom) 2015/444. Mjere TEMPEST provode se u skladu s člankom 36. stavkom 6. te odluke.

2. Sigurnosna akreditacija CIS-a ugovaratelja koji postupa s klasificiranim podacima EU-a stupnja tajnosti RESTREINT UE/EU RESTRICTED i svako njihovo međusobno povezivanje mogu se delegirati službeniku za sigurnost ugovaratelja ako je to u skladu s nacionalnim zakonima i propisima. Ako se ta zadaća delegira, ugovaratelj je odgovoran za to da se pri postupanju s podacima stupnja tajnosti RESTREINT UE/EU RESTRICTED u njegovu CIS-u provode minimalni sigurnosni zahtjevi opisani u pismu o sigurnosnim aspektima. Međutim, nadležni NST-ovi/ZST-ovi i SAA-ovi i dalje su odgovorni za zaštitu podataka stupnja tajnosti RESTREINT UE/EU RESTRICTED s kojima ugovaratelj postupa te zadržavaju pravo na inspekciju sigurnosnih mjera koje su ugovaratelji poduzeli. Osim toga, ugovaratelj javnom naručitelju i, ako se to zahtijeva nacionalnim zakonima i propisima, nadležnom nacionalnom tijelu za sigurnosnu akreditaciju podnosi izjavu o sukladnosti kojom potvrđuje da su CIS ugovaratelja i povezana međusobna povezivanja akreditirana za postupanje s klasificiranim podacima EU-a stupnja tajnosti RESTREINT UE/EU RESTRICTED ([12]).

Članak 13.

Prijevoz komercijalnom kurirskom službom

Pri prijevozu klasificiranih podataka EU-a komercijalnom kurirskom službom poštuju se relevantne odredbe odluka Komisije o provedbenim pravilima za postupanje s podacima stupnja tajnosti RESTREINT UE/EU RESTRICTED i CONFIDENTIEL UE/EU CONFIDENTIAL.

Članak 14.

Ručni prijenos

1. Na ručni prijenos klasificiranih podataka primjenjuju se strogi sigurnosni zahtjevi.

2. Osoblje ugovaratelja može podatke stupnja tajnosti RESTREINT UE/EU RESTRICTED ručno prenositi unutar EU-a ako su ispunjeni sljedeći zahtjevi:

(a) upotrebljava se neprozirna omotnica ili ambalaža te se na njima ne navodi oznaka stupnja tajnosti sadržaja;

([12]) Minimalni zahtjevi za komunikacijske i informacijske sustave koji postupaju s klasificiranim podacima EU-a stupnja tajnosti RESTREINT UE/EU RESTRICTED utvrđeni su u Dodatku E Prilogu III.

(b) klasificirani podaci stalno su uz nositelja;

(c) omotnica ili ambalaža putem se ne otvaraju.

3. Ručni prijenos podataka klasificiranih stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET koji osoblje ugovaratelja obavlja unutar države članice EU-a organizira se unaprijed između subjekata koji šalju i primaju podatke. Tijelo ili objekt koji šalje podatke obavještava tijelo ili objekt koji prima podatke o detaljima pošiljke, uključujući referentnu oznaku, stupanj tajnosti, očekivano vrijeme dolaska i ime kurirske službe. Takav ručni prijenos dopušten je ako su ispunjeni sljedeći zahtjevi:

(a) klasificirani podaci prenose se u dvostrukoj omotnici ili ambalaži;

(b) vanjska omotnica ili ambalaža dobro su zatvoreni te se na njima ne navodi oznaka tajnosti sadržaja, dok se na unutarnjoj omotnici navodi stupanj tajnosti;

(c) klasificirani podaci EU-a stalno su uz nositelja;

(d) omotnica ili ambalaža putem se ne otvaraju;

(e) omotnica ili ambalaža prenose se u aktovci koja se može zaključati ili sličnom odobrenom spremniku čija veličina i težina omogućuju da ih nositelj cijelo vrijeme drži uza se i da ih ne mora predati u predanu prtljagu;

(f) kurir nosi kurirsku potvrdu koju izdaje njegovo nadležno sigurnosno tijelo i kojom ga to tijelo ovlašćuje za prijenos utvrđene klasificirane pošiljke.

4. Na ručni prijenos podataka klasificiranih stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET iz jedne države članice EU-a u drugu koji obavlja osoblje ugovaratelja primjenjuju se sljedeća dodatna pravila:

(a) kurir je odgovoran za sigurno čuvanje klasificiranog materijala koji nosi sve do njegove predaje primatelju;

(b) u slučaju povrede sigurnosti NST/ZST pošiljatelja može zatražiti da tijela u zemlji u kojoj je došlo do povrede provedu istragu, izvijeste o rezultatima istrage i poduzmu primjerene pravne ili druge mjere;

(c) kurira se upoznaje sa svim sigurnosnim obvezama kojih se treba pridržavati pri prijenosu te on potpisuje odgovarajuću izjavu;

(d) upute kuriru prilažu se kurirskoj potvrdi;

(e) kuriru se daje opis pošiljke i plan kretanja

(f) nakon završetka putovanja dokumenti se vraćaju NST-u/ZST-u koji ih je izdao ili ostaju dostupni primatelju za potrebe praćenja;

(g) ako carina, tijelo nadležno za imigraciju ili granična policija zatraži pregled i inspekciju pošiljke, dopušta se otvaranje pošiljke i pregled njezina dostatnog dijela kako bi se utvrdilo da sadržava samo prijavljeni materijal;

(h) carinska tijela treba pozvati da poštuju službenu ovlast otpremnih dokumenata i dokumenata odobrenja koje kurir prenosi.

Ako carina otvara pošiljku, treba je otvoriti izvan vidokruga neovlaštenih osoba i, ako je moguće, u prisutnosti kurira. Kurir je dužan od tijela koja provode inspekciju zahtijevati da se pošiljka prepakira te tražiti da pošiljku ponovno zapečate i u pisanom obliku potvrde da su je oni otvorili.

5. Ručni prijenos podataka klasificiranih stupnjem tajnosti RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET u treću zemlju ili međunarodnu organizaciju koji obavlja osoblje ugovaratelja podliježe odredbama sporazuma o sigurnosti podataka ili administrativnog dogovora koji su Europska unija ili Komisija sklopile s trećom zemljom ili međunarodnom organizacijom.

POGLAVLJE 6.

PLANIRANJE NEPREKIDNOSTI POSLOVANJA

Članak 15.

Krizni planovi i mjere oporavka

Služba Komisije kao javni naručitelj osigurava da klasificirani ugovor obvezuje ugovaratelja da donese krizne poslovne planove (BCP) za zaštitu klasificiranih podataka EU-a s kojima se postupa pri izvršenju klasificiranog ugovora u izvanrednim situacijama i da u kontekstu planiranja neprekidnosti poslovanja uspostavi preventivne mjere i mjere oporavka kako bi nepredviđeni događaji što manje utjecali na postupanje s klasificiranim podacima EU-a i njihovo čuvanje. Ugovaratelj o svojem kriznom poslovnom planu obavještava javnog naručitelja.

Članak 16.

Stupanje na snagu

Ova Odluka stupa na snagu dvadesetog dana od dana objave u *Službenom listu Europske unije*.

Sastavljeno u Bruxellesu 17. listopada 2019.

Za Komisiju,

u ime predsjednika,

Günther OETTINGER

Član Komisije

PRILOG I.

STANDARDNE INFORMACIJE U OBAVIJESTIMA O NADMETANJU ZA UGOVOR O JAVNOJ NABAVI

(prilagoditi upotrijebljenim obavijestima o nadmetanju)

Za ugovore koji obuhvaćaju podatke klasificirane stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET

Ostali posebni uvjeti (*ako je primjenjivo*)

Izvršenje ugovora podliježe posebnim uvjetima ● da ○ ne

(*ako da*) Opis posebnih uvjeta:

Ugovor će obuhvaćati pristup podacima klasificiranima stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET, postupanje s njima i/ili njihovo čuvanje, što podliježe sigurnosnim propisima za zaštitu klasificiranih podataka EU-a utvrđenima u Odluci (EU, Euratom) 2015/444 i provedbenim pravilima Odluke ([1]).

Za osoblje ugovaratelja koje postupa s klasificiranim podacima bit će potrebno uvjerenje o sigurnosnoj provjeri pravne osobe, kao i uvjerenje o sigurnosnoj provjeri osobe.

Posebne sigurnosne obveze bit će dio ugovora (pismo o sigurnosnim aspektima priloženo ugovoru). Za podugovaranje će biti potrebna prethodna pisana suglasnost javnog naručitelja te će podugovaratelj i njegovo osoblje morati poštovati sva sigurnosna pravila.

Za ugovore koji obuhvaćaju podatke klasificirane stupnjem tajnosti RESTREINT UE/EU RESTRICTED

Ostali posebni uvjeti (*ako je primjenjivo*)

Izvršenje ugovora podliježe posebnim uvjetima ● da ○ ne

(*ako da*) Opis posebnih uvjeta:

Ugovor će obuhvaćati ili će se njime zahtijevati pristup podacima klasificiranima stupnjem tajnosti RESTREINT UE/EU RESTRICTED, postupanje s njima i/ili njihovo čuvanje, što podliježe sigurnosnim propisima za zaštitu klasificiranih podataka EU-a utvrđenima u Odluci (EU, Euratom) 2015/444 i Odluci o provedbenim pravilima ([2]).

Posebne sigurnosne obveze bit će dio ugovora (pismo o sigurnosnim aspektima priloženo ugovoru). Za podugovaranje će biti potrebna prethodna pisana suglasnost javnog naručitelja te će podugovaratelj i njegovo osoblje morati poštovati sva sigurnosna pravila.

([1]) Javni naručitelj treba umetnuti upućivanja nakon donošenja provedbenih pravila.
([2]) Javni naručitelj treba umetnuti upućivanja nakon donošenja provedbenih pravila.

PRILOG II.

STANDARDNE KLAUZULE U UGOVORU O JAVNOJ NABAVI

(treba prilagoditi upotrijebljenim ugovorima)

ČLANAK XX.

OBVEZE POVEZANE SA SIGURNOŠĆU

XX.1 Klasificirani podaci EU-a

Ako provedba ugovora obuhvaća upotrebu ili stvaranje klasificiranih podataka EU-a, takvi se podaci moraju obrađivati u skladu s pismom o sigurnosnim aspektima (SAL) i vodičem za stupnjeve tajnosti (SCG) kako je utvrđeno u Prilogu 1. i Odluci (EU, Euratom) 2015/444 i njezinim provedbenim pravilima ([1]), dok se ne deklasificiraju.

Svi izlazni proizvodi koji sadržavaju klasificirane podatke moraju se podnijeti u skladu s posebnim postupcima dogovorenima s javnim naručiteljem.

Zadaće djelovanja koje obuhvaćaju klasificirane podatke ne smiju se podugovarati bez prethodnog izričitog pisanog odobrenja javnog naručitelja

Klasificirani podaci EU-a ne smiju se otkrivati trećim stranama (uključujući podugovaratelje) bez prethodnog izričitog pisanog odobrenja javnog naručitelja.

([1]) Javni naručitelj treba umetnuti upućivanja nakon donošenja provedbenih pravila.

PRILOG III.

[Prilog IV. (Okvirnom ugovoru)]

PISMO O SIGURNOSNIM ASPEKTIMA (SAL)

[model]

Dodatak A.

SIGURNOSNI ZAHTJEVI

Javni naručitelj mora u pismo o sigurnosnim aspektima (SAL) uvrstiti sljedeće sigurnosne zahtjeve. Neke se klauzule možda ne primjenjuju na ugovor. One se nalaze u uglatim zagradama.

Popis klauzula nije iscrpan. Mogu se dodati dodatne klauzule ovisno o prirodi klasificiranog ugovora.

OPĆI UVJETI

[*Napomena: primjenjuju se na sve klasificirane ugovore*]

1. Pismo o sigurnosnim aspektima (SAL) sastavni je dio klasificiranog ugovora [ili podugovora] te se u njemu opisuju sigurnosni zahtjevi povezani s pojedinim ugovorom. Neispunjavanje tih zahtjeva može biti dovoljan razlog za raskid ugovora.

2. Ugovaratelji podliježu svim obvezama utvrđenima u Odluci (EU, Euratom) 2015/444 i njezinim provedbenim pravilima ([1]).

3. Klasificirani podaci koji su stvoreni pri izvršenju ugovora moraju se označiti kao klasificirani podaci EU-a (EUCI) stupnja tajnosti koji je utvrđen u vodiču za stupnjeve tajnosti (SCG) u Dodatku B ovom pismu. Odstupanje od stupnja tajnosti propisanog SCG-om dopušteno je samo uz pisano odobrenje tijela za ugovaranje.

4. Komisija, kao javni naručitelj, ostvaruje prava koja pripadaju autoru bilo kojeg klasificiranog podatka EU-a koji je stvoren i s kojim se postupa radi izvršenja klasificiranog ugovora.

5. Ugovaratelj ili podugovaratelj ne smije bez pisane suglasnosti javnog naručitelja upotrebljavati nijedan podatak ni materijal primljen od javnog naručitelja ili stvoren u ime tog naručitelja ni u koju svrhu osim za potrebe tog ugovora.

6. Ugovaratelj mora ispitati sve povrede sigurnosti povezane s klasificiranim podacima EU-a te ih što prije prijaviti javnom naručitelju. Ugovaratelj ili podugovaratelj mora svojem nacionalnom sigurnosnom tijelu (NST) ili zaduženom sigurnosnom tijelu (ZST) te, ako je to u skladu s nacionalnim zakonima i propisima, sigurnosnom tijelu Komisije odmah prijaviti sve slučajeve u kojima se zna ili postoji razlog za sumnju da su klasificirani podaci EU-a koji su dostavljeni ili stvoreni u skladu s ugovorom izgubljeni ili otkriveni neovlaštenim osobama.

7. Nakon isteka ugovora ugovaratelj ili podugovaratelj mora javnom naručitelju što prije vratiti sve klasificirane podatke EU-a koje posjeduje. Ako je izvedivo, ugovaratelj ili podugovaratelj može uništiti klasificirane podatke EU-a umjesto da ih vrati. To se mora provesti u skladu s nacionalnim zakonima i propisima zemlje u kojoj se ugovaratelj nalazi, uz prethodnu suglasnost sigurnosnog tijela Komisije i na temelju njegovih uputa. Klasificirani podaci EU-a moraju se uništiti tako da se ne mogu djelomično ili u cijelosti rekonstruirati.

8. Ako je ugovaratelj ili podugovaratelj po raskidu ili sklapanju ugovora ovlašten zadržati klasificirane podatke EU-a, ti se podaci moraju nastaviti štititi u skladu s Odlukom (EU, Euratom) 2015/444 (dalje u tekstu: Odluka 2015/444) i njezinim provedbenim pravilima ([2]).

9. Sva elektronička postupanja, obrada i slanje klasificiranih podataka EU-a moraju biti u skladu s odredbama utvrđenima u poglavljima 5. i 6. Odluke Komisije 2015/444. One obuhvaćaju, među ostalim, zahtjev da komunikacijski i informacijski sustavi koje ugovaratelj posjeduje i kojima se koristi za postupanje s klasificiranim podacima EU-a za potrebe ugovora (dalje u tekstu: CIS ugovaratelja) moraju biti akreditirani ([3]), da elektroničko slanje klasificiranih podataka EU-a mora biti zaštićeno kriptografskim proizvodima odobrenima u skladu s člankom 36. stavkom 4. Odluke 2015/444 i da se mjere TEMPEST moraju provoditi u skladu s člankom 36. stavkom 6. Odluke 2015/444.

([1]) Javni naručitelj treba umetnuti upućivanja nakon donošenja provedbenih pravila.
([2]) Javni naručitelj treba umetnuti upućivanja nakon donošenja provedbenih pravila.
([3]) Stranka koja provodi akreditaciju morat će javnom naručitelju preko sigurnosnog tijela Komisije i u suradnji s nadležnim tijelom za sigurnosnu akreditaciju (SAA) dostaviti izjavu o sukladnosti.

10. Ugovaratelj ili podugovaratelj dužan je imati krizni poslovni plan (BCP) za zaštitu svih klasificiranih podataka EU-a s kojima se postupa pri izvršenju klasificiranog ugovora u izvanrednim situacijama te provodi preventivne mjere i mjere oporavka kako bi nepredviđeni događaji što manje utjecali na postupanje s klasificiranim podacima EU-a i njihovo čuvanje. Ugovaratelj ili podugovaratelj o svojem kriznom poslovnom planu mora obavijestiti javnog naručitelja.

UGOVORI ZA KOJE JE POTREBAN PRISTUP PODACIMA KLASIFICIRANIMA STUPNJEM TAJNOSTI RESTREINT UE/EU RESTRICTED

11. Uvjerenje o sigurnosnoj provjeri osobe (USP) nije potrebno za ispunjavanje ugovora. Međutim, podaci ili materijal klasificirani stupnjem tajnosti RESTREINT UE/EU RESTRICTED moraju biti dostupni samo osoblju ugovaratelja kojima su ti podaci potrebni za izvršenje ugovora (*načelo nužnosti pristupa podacima*), koje je službenik za sigurnost ugovaratelja upoznao s njihovim odgovornostima i posljedicama bilo kakvog ugrožavanja ili povrede sigurnosti takvih podataka i koje je u pisanom obliku priznalo da razumije posljedice propusta u zaštiti klasificiranih podataka EU-a.

12. Ako javni naručitelj nije dao pisanu suglasnost, ugovaratelj ili podugovaratelj ne smije nijednom subjektu ni osobi, osim svojem osoblju za koje je utvrđena nužnost pristupa podacima, omogućiti pristup podacima ili materijalu klasificiranima oznakom tajnosti RESTREINT UE/EU RESTRICTED.

13. Ugovaratelj ili podugovaratelj mora zadržati oznake stupnja tajnosti klasificiranih podataka stvorenih ili dostavljenih tijekom izvršenja ugovora i ne smije deklasificirati podatke bez pisane suglasnosti javnog naručitelja.

14. Podatke ili materijal klasificiran oznakom stupnja tajnosti RESTREINT UE/EU RESTRICTED koji se ne koristi potrebno je čuvati u zaključanom uredskom ormariću. Kad se prenose, dokumente treba nositi u neprozirnoj omotnici. Dokumenti stalno moraju biti uz nositelja i ne smiju se putem otvarati.

15. Ugovaratelj ili podugovaratelj može dokumente klasificirane oznakom tajnosti RESTREINT UE/EU RESTRICTED slati Komisiji komercijalnom kurirskom službom, poštanskom službom, ručnim prijenosom ili elektroničkim putem. Ugovaratelj ili podugovaratelj u tu svrhu mora slijediti sigurnosne upute za program (ili projekt) (SUP) koje je izdala Komisija i/ili Komisijina provedbena pravila o gospodarskoj sigurnosti u pogledu klasificiranih ugovora o javnoj nabavi ([4]).

16. Kad više nisu potrebni, dokumenti klasificirani stupnjem tajnosti RESTREINT UE/EU RESTRICTED moraju se uništiti tako da se ne mogu djelomično ili u cijelosti rekonstruirati.

17. Sigurnosna akreditacija CIS-a ugovaratelja koji postupa s klasificiranim podacima EU-a stupnja tajnosti RESTREINT UE/EU RESTRICTED i svako njihovo međusobno povezivanje mogu se delegirati službeniku za sigurnost ugovaratelja ako to dopuštaju nacionalni zakoni i propisi. U slučaju tako delegirane akreditacije, NST-ovi/ZST-ovi i SAA-ovi i dalje su odgovorni za zaštitu svih podataka stupnja tajnosti RESTREINT UE/EU RESTRICTED s kojima ugovaratelj postupa te zadržavaju pravo na inspekciju sigurnosnih mjera koje je ugovaratelj poduzeo. Osim toga, ugovaratelj javnom naručitelju i, ako se to zahtijeva nacionalnim zakonima i propisima, nadležnom nacionalnom tijelu za sigurnosnu akreditaciju podnosi izjavu o sukladnosti kojom potvrđuje da su CIS ugovaratelja i povezana međusobna povezivanja akreditirana za postupanje s klasificiranim podacima EU-a stupnja tajnosti RESTREINT UE/EU RESTRICTED.

POSTUPANJE S PODACIMA KLASIFICIRANIMA STUPNJEM TAJNOSTI RESTREINT UE/EU RESTRICTED U KOMUNIKACIJSKIM I INFORMACIJSKIM SUSTAVIMA (CIS)

18. Minimalni zahtjevi za CIS koji postupa s podacima klasificiranima stupnjem tajnosti RESTREINT UE/EU RESTRICTED utvrđeni su u Dodatku E ovom pismu o sigurnosnim aspektima.

UVJETI POD KOJIMA UGOVARATELJ MOŽE SKLAPATI PODUGOVORE

19. Ugovaratelj mora prije podugovaranja bilo kojeg dijela klasificiranog ugovora dobiti dopuštenje dotične službe Komisije kao javnog naručitelja

([4]) Javni naručitelj treba umetnuti upućivanja nakon donošenja provedbenih pravila.

20. Poduzeću registriranom u zemlji koja nije članica EU-a ili subjektu koji pripada međunarodnoj organizaciji ne može se dati podugovor ako ta zemlja koja nije članica EU-a ili međunarodna organizacija nije sklopila sporazum o sigurnosti podataka s EU-om ili administrativni dogovor s Komisijom.

21. Ako je ugovaratelj sklopio podugovor, sigurnosne odredbe ugovora primjenjuju se *mutatis mutandis* na podugovaratelja (podugovaratelje) i njegovo (njihovo) osoblje. U tom je slučaju odgovornost ugovaratelja osigurati da svi podugovaratelji ta načela primjenjuju na vlastite sporazume o podugovaranju. Kako bi se osigurao primjeren nadzor sigurnosti, NST-ove/ZST-ove ugovaratelja i podugovaratelja obavještava se o dodjeli svih povezanih klasificiranih podugovora stupnja tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET. Po potrebi se NST-ovima/ZST-ovima ugovaratelja i podugovaratelja dostavlja preslika sigurnosnih odredbi povezanih s konkretnim podugovorom. NST-ovi/ZST-ovi koji zahtijevaju obavijest o sigurnosnim odredbama klasificiranih ugovora stupnja tajnosti RESTREINT UE/EU RESTRICTED navedeni su u prilogu Komisijinim provedbenim pravilima o gospodarskoj sigurnosti u pogledu klasificiranih ugovora o javnoj nabavi ([1]).

22. Ugovaratelj ne smije podugovaratelju otkriti nijedan klasificirani podatak EU-a bez prethodnog pisanog odobrenja javnog naručitelja. Ako se klasificirani podaci EU-a podugovarateljima šalju često ili rutinski, tada javni naručitelje može dati svoje odobrenje na određeni rok (npr. 12 mjeseci) ili za razdoblje trajanja podugovora.

POSJETI

Ako se na posjete koji obuhvaćaju podatke klasificirane stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET primjenjuje standardni postupak zahtjeva za posjet, javni naručitelj mora uvrstiti stavke 23., 24. i 25. te izbrisati stavak 26. Ako su posjeti koji obuhvaćaju podatke klasificirane stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET organizirani neposredno između ustanova koje šalju i primaju posjetitelje, javni naručitelj mora izbrisati stavke 24. i 25. i uvrstiti samo stavak 26.

23. Posjeti koji obuhvaćaju pristup ili potencijalni pristup podacima klasificiranima stupnjem tajnosti RESTREINT UE/EU RESTRICTED organiziraju se neposredno između ustanova koje šalju i primaju posjetitelje, pri čemu nije potrebno slijediti postupak iz stavaka od 24. do 26. u nastavku.

[24. Posjeti koji obuhvaćaju pristup ili potencijalni pristup podacima klasificiranima stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET podliježu sljedećem postupku:

(a) službenik za sigurnost objekta koji šalje posjetitelja ispunjava sve relevantne dijelove obrasca zahtjeva za posjet (Dodatak C) i podnosi zahtjev NST-u/ZST-u objekta;

(b) NST/ZST objekta koji šalje posjetitelja treba potvrditi USP posjetitelja prije nego što NST-u/ZST-u objekta koji prima posjetitelja (ili sigurnosnom tijelu Komisije ako se posjećuju prostori Komisije) podnese zahtjev za posjet;

(c) službenik za sigurnost objekta koji šalje posjetitelja zatim od svojeg NST-a/ZST-a dobiva odgovor NST-a/ZST-a objekta koji prima posjetitelja domaćina (ili sigurnosnog tijela Komisije), kojim se zahtjev za posjet odobrava ili odbija;

(d) zahtjev za posjet smatra se odobrenim ako do pet radnih dana prije datuma posjeta nije uložen nikakav prigovor.]

[25. Prije nego što posjetitelju (posjetiteljima) omogući pristup podacima klasificiranima stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET, objekt koji prima posjetitelja mora za to dobiti odobrenje svojeg NST-a/ZST-a.]

[26. Posjeti koji obuhvaćaju pristup ili potencijalni pristup podacima klasificiranima stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET organiziraju se neposredno između ustanova koje šalju i primaju posjetitelje (primjer obrasca koji se može upotrijebiti za tu svrhu nalazi se u Dodatku C).]

([1]) Javni naručitelj treba umetnuti upućivanja nakon donošenja provedbenih pravila

27. Po dolasku u objekt koji prima posjetitelja posjetitelji moraju dokazati svoj identitet predočenjem važeće osobne iskaznice ili putovnice.

28. Objekt koji prima posjetitelja mora osigurati da se vodi evidencija svih posjetitelja. Ona mora sadržavati njihova imena, organizacije koje predstavljaju, datum isteka USP-a (ako je primjenjivo), datum posjeta i imena osoba koje su posjetili. Ne dovodeći u pitanje europske propise o zaštiti podataka, ta se evidencija čuva najmanje pet godina ili, po potrebi, u skladu s onim što je propisano nacionalnim zakonima i propisima.

POSJETI RADI PROCJENE STANJA

29. Sigurnosno tijelo Komisije može u suradnji s nadležnim NST-om/ZST-om provoditi posjete objektima ugovaratelja ili podugovaratelja kako bi provjerilo poštuju li se sigurnosni zahtjevi za postupanje s klasificiranim podacima EU-a.

VODIČ ZA STUPNJEVE TAJNOSTI

30. Popis svih elemenata ugovora koji su klasificirani ili će se klasificirati tijekom izvršenja ugovora, pravila klasifikacije i specifikacija primjenjivih stupnjeva tajnosti nalaze se u vodiču za stupnjeve tajnosti (SCG). SCG je sastavni dio ovog ugovora i nalazi se u Dodatku B ovom Prilogu.

Dodatak B

VODIČ ZA STUPNJEVE TAJNOSTI

[poseban tekst koji se prilagođava predmetu ugovora]

Dodatak C

ZAHTJEV ZA POSJET

(MODEL)

Detaljne upute za ispunjavanje zahtjeva za posjet

(Zahtjev se podnosi isključivo na engleskom jeziku)

HEADING	Označite polja za vrstu posjeta i vrstu podataka te navedite koliko se lokacija namjerava posjetiti i broj posjetitelja.
4. **ADMINISTRATIVE DATA**	Ispunjava NST/ZST koji podnosi zahtjev.
5. **REQUESTING ORGANISATION OR INDUSTRIAL FACILITY**	Navedite puno ime i poštansku adresu. Prema potrebi uključite grad, državu i poštanski broj.
6. **ORGANISATION OR INDUSTRIAL FACILITY TO BE VISITED**	Navedite puno ime i poštansku adresu. U adresi navedite grad, državu, poštanski broj, broj teleksa ili telefaksa (ako je primjenjivo), broj telefona i e-poštu. Navedite ime i broj telefona/telefaksa te e-poštu glavne točke za kontakt ili osobe s kojom ste dogovorili posjet. Napomene: 1. Važno je navesti točan poštanski broj jer poduzeće može imati različite objekte. 2. Pri ručnom ispunjavanju zahtjeva Prilog 1. može se upotrijebiti ako je potrebno posjetiti dva ili više objekta u pogledu istog predmeta. Pri upotrebi Priloga u stavci 3 trebalo bi navesti: „VIDJETI PRILOG 1., BROJ OBJEKATA…” (navesti broj objekata).
7. **DATES OF VISIT**	Navedite stvarni datum ili razdoblje (od – do) posjeta u obliku „dan – mjesec – godina”. Po potrebi, u zagradama navedite alternativni datum ili razdoblje.
8. **TYPE OF INITIATIVE**	Navedite je li posjet zatražila organizacija ili objekt koji podnosi zahtjev ili je zatražen na poziv objekta koji se posjećuje.
9. **THE VISIT RELATES TO:**	Navedite puni naziv projekta, ugovora ili poziva za podnošenje ponuda i pritom se koristite isključivo uobičajenim kraticama.

10. **SUBJECT TO BE DISCUSSED/ JUSTIFICATION**	Ukratko navedite razloge za posjet. Nemojte upotrebljavati kratice koje nisu objašnjene. Napomene: U slučaju više posjeta tekst ove stavke u pogledu podataka trebalo bi započeti riječima „Više posjeta” (npr. Više posjeta radi rasprave o _____).
11. **ANTICIPATED LEVEL OF CLASSIFIED INFORMATION TO BE INVOLVED**	Po potrebi navedite SECRET UE/EU SECRET (S-UE/EU-S) ili CONFIDENTIEL UE/EU CONFIDENTIAL (C-UE/EU-C).
12. **PARTICULARS OF VISITOR**	Napomena: ako posjet obuhvaća više od dva posjetitelja, potrebno je primijeniti Prilog 2.
13. **THE SECURITY OFFICER OF THE REQUESTING ENTITY**	U ovoj stavci potrebno je navesti ime, broj telefona, broj telefaksa i e-poštu službenika za sigurnost objekta koji podnosi zahtjev.
14. **CERTIFICATION OF SECURITY CLEARANCE**	Ovo polje ispunjava tijelo za ovjeravanje. Napomene za tijelo za ovjeravanje: (a) navedite naziv, adresu, broj telefona, broj telefaksa i e-poštu (može se ispisati unaprijed); (b) ovu stavku treba potpisati i ovjeriti pečatom (ako je primjenjivo).
15. **REQUESTING SECURITY AUTHORITY**	Ovo polje ispunjava NST/ZST. Napomena za NST/ZST: (a) navedite naziv, adresu, broj telefona, broj telefaksa i e-poštu (može se ispisati unaprijed); (b) ovu stavku treba potpisati i ovjeriti pečatom (ako je primjenjivo).

Potrebno je ispuniti sva polja i obrazac podnijeti putem međuvladinih kanala ([2]).

([2]) Ako je dogovoreno da se posjeti koji obuhvaćaju pristup ili potencijalni pristup klasificiranim podacima EU-a stupnja tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET mogu organizirati neposredno, ispunjeni obrazac može se podnijeti izravno službeniku za sigurnost ustanove koju se posjećuje.

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

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

<Mjesto za upućivanje na primjenjivo zakonodavstvo o osobnim podacima i poveznica na obvezne informacije za osobu čiji se podaci obrađuju, npr. kako se provodi članak 13. Opće uredbe o zaštiti podataka ([3]).>

([3]) Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) (SL L 119, 4.5.2016., str. 1.).

PRILOG 1. OBRASCU ZAHTJEVA ZA POSJET

ORGANISATION OR INDUSTRIAL FACILITY 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)

<Mjesto za upućivanje na primjenjivo zakonodavstvo o osobnim podacima i poveznica na obvezne informacije za osobu čiji se podaci obrađuju, npr. kako se provodi članak 13. Opće uredbe o zaštiti podataka ([1]).>

([1]) Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) (SL L 119, 4.5.2016., str. 1.).

PRILOG 2. OBRASCU ZAHTJEVA ZA POSJET

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)

<Mjesto za upućivanje na primjenjivo zakonodavstvo o osobnim podacima i poveznica na obvezne informacije za osobu čiji se podaci obrađuju, npr. kako se provodi članak 13. Opće uredbe o zaštiti podataka ([1]).>

([1]) Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) (SL L 119, 4.5.2016., str. 1.).

Dodatak D

INFORMATIVNI OBRAZAC O UVJERENJU O SIGURNOSNOJ PROVJERI PRAVNE OSOBE (FSCIS)

(MODEL)

1. **Uvod**

1.1. Primjer informativnog obrasca o uvjerenju o sigurnosnoj provjeri pravne osobe (FSCIS) priložen je radi brze razmjene informacija između nacionalnog sigurnosnog tijela (NST) ili zaduženog sigurnosnog tijela (ZST), ostalih nadležnih nacionalnih sigurnosnih tijela i Komisije (kao javnog naručitelja) u pogledu uvjerenja o sigurnosnoj provjeri pravne osobe (USPPO) objekta uključenog u klasificirane natječaje, ugovore ili podugovore.

1.2. Informativni obrazac o uvjerenju o sigurnosnoj provjeri pravne osobe valjan je samo uz pečat nadležnog NST-a/ZST-a ili drugog nadležnog tijela.

1.3. Informativni obrazac o uvjerenju o sigurnosnoj provjeri pravne osobe podijeljen je u odjeljke za zahtjev i odgovor te se može upotrijebiti u prethodno utvrđene svrhe ili u bilo koje druge svrhe za koje je potreban USPPO status određenog objekta. NST/ZST koji podnosi zahtjev mora u polju 7. odjeljka za zahtjev navesti razlog za upit.

1.4. Pojedinosti iz informativnog obrasca o uvjerenju o sigurnosnoj provjeri pravne osobe obično nisu klasificirane; u skladu s time poželjno je da se informativni obrazac o uvjerenju o sigurnosnoj provjeri pravne osobe šalje odgovarajućim NST-ovima/ZST-ovima/Komisiji elektroničkim putem.

1.5. NST-ovi/ZST-ovi trebali bi uložiti sve napore da na zahtjev za informativni obrazac o uvjerenju o sigurnosnoj provjeri pravne osobe odgovore u roku od deset radnih dana.

1.6. Ako se u pogledu tog uvjerenja prenese bilo koji klasificirani podatak ili dodijeli ugovor, NST/ZST koji daje odgovor o tome mora biti obaviješten.

Postupci i upute za upotrebu informativnog obrasca o uvjerenju o sigurnosnoj provjeri pravne osobe (FSCIS)

Detaljne upute vrijede za NST/ZST ili javnog naručitelja Komisije, koji ispunjavaju informativni obrazac o uvjerenju o sigurnosnoj provjeri pravne osobe. Poželjno je da se zahtjev ispuni velikim tiskanim slovima.

ZAGLAVLJE	Podnositelj zahtjeva unosi puni naziv NST-a/ZST-a i naziv države.
1. **VRSTA ZAHTJEVA**	Javni naručitelj koji podnosi zahtjev označava odgovarajuća polja za vrstu zahtjeva za informativni obrazac o uvjerenju o sigurnosnoj provjeri pravne osobe. Uvrstiti zahtijevani stupanj sigurnosne provjere. Treba upotrebljavati sljedeće kratice: SECRET UE/EU SECRET = S-UE/EU-S CONFIDENTIEL UE/EU CONFIDENTIAL = C-UE/EU-C CIS = Komunikacijski i informacijski sustavi za obradu klasificiranih podataka

2. **POJEDINOSTI PREDMETA**	Polja od 1 do 6 ne zahtijevaju posebne razloge. U polju 4 upotrebljava se standardna dvoslovna oznaka zemlje. Polje 5 nije obavezno.
3. **RAZLOG ZA ZAHTJEV**	Navedite konkretan razlog za zahtjev, pokazatelje projekta, broj ugovora ili poziv na dostavu ponuda. Navedite potrebu u pogledu sposobnosti čuvanja, stupanj tajnosti CIS-a itd. Trebalo bi uvrstiti sve rokove/datume isteka/datume dodjele koji bi mogli utjecati na kraj USPPO-a.
4. **NST/ZST KOJI PODNOSI ZAHTJEV**	Navedite ime stvarnog podnositelja zahtjeva (u ime NST-a/ZST-a) i datum zahtjeva u obliku broja *(dd/mm/gggg)*.
5. **ODJELJAK ZA ODGOVOR**	Polja 1–5: označite odgovarajuća polja. Polje 2: ako se USPPO obrađuje, preporučuje se da se podnositelju zahtjeva naznači potrebno vrijeme obrade (ako je poznato). Polje 6: (a) iako je valjanost različita u svakoj zemlji ili čak u svakom objektu, preporučuje se navesti datum isteka USPPO-a; (b) ako je datum isteka potvrde o USPPO-u neodređen, ovo se polje može prekrižiti; (c) u skladu s odgovarajućim nacionalnim pravilima i propisima, podnositelj zahtjeva odnosno ugovaratelj ili podugovaratelj odgovoran je za podnošenje zahtjeva za produljenje USPPO-a.
6. **NAPOMENE**	Može se upotrijebiti za dodatne informacije u pogledu USPPO-a, objekta ili prethodno navedene stavke.
7. **NST/ZST KOJI JE IZDAO ODOBRENJE**	Navedite naziv tijela izdavatelja u ime NST-a/ZST-a) i datum odgovora u obliku broja (dd/mm/gggg).

INFORMATIVNI OBRAZAC O UVJERENJU O SIGURNOSNOJ PROVJERI PRAVNE OSOBE (FSCIS)

(MODEL)

Potrebno je ispuniti sva polja i obrazac podnijeti putem međuvladinih kanala ili kanala između vlada i međunarodnih organizacija.

ZAHTJEV ZA POTVRDU O UVJERENJU O SIGURNOSNOJ PROVJERI PRAVNE OSOBE

Adresat: _____

(naziv zemlje NST-a/ZST-a)

Ispunite polja za odgovor, prema potrebi:

[] Navedite potvrdu o USPPO-u za razinu: [] S-UE/EU-S [] C-UE/EU-C

za objekt naveden u nastavku

[] uključujući zaštitu klasificiranog materijala/podataka

[] uključujući komunikacijske i informacijske sustave (CIS) za obradu klasificiranih podataka

[] Izravno ili na odgovarajući zahtjev ugovaratelja ili podugovaratelja pokrenite postupak stjecanja USPPO-a do razine i uključujući razinu ..... s ..... razinom zaštite i ..... razinom CIS-a, ako objekt trenutačno ne posjeduje te razine sposobnosti.

Potvrdite točnost podataka u nastavku navedenog objekta i po potrebi navedite ispravke/nadopune.

1. Puno ime objekta:	Ispravci/nadopune:
.....	.....
2. Puna adresa objekta:	
.....	.....
3. Poštanska adresa (ako je različita od adrese u točki 2.)	
.....	.....
4. Poštanski broj/grad/država	
.....	.....
5. Ime službenika za sigurnost	
.....	.....
6. Telefon/telefaks/e-pošta službenika za sigurnost	
.....	.....

7. Ovaj je zahtjev podnesen iz sljedećih razloga: (navedite pojedinosti o fazi prije sklapanja ugovora (odabir prijedloga), ugovoru ili podugovoru, programu/projektu itd.)

.....

Requesting NSA/DSA/Commission contracting authority: Ime: ..... Datum: (dd/mm/gggg) .....

ODGOVOR (u roku od deset radnih dana)

Potvrđuje se da:

1. [] prethodno navedeni objekt posjeduje USPPO do razine i uključujući razinu [] S-UE/EU-S

   [] C-UE/EU-C.

2. Prethodno navedeni objekt sposoban je štititi klasificirane podatke/materijal:

   [] da, razina: ..... [] ne.

3. Prethodno navedeni objekt ima akreditirani/ovlašteni CIS:

   [] da, razina: ..... [] ne.

4. [] kad je riječ o prethodno navedenom zahtjevu, pokrenut je postupak za USPPO. Bit ćete obaviješteni kad USPPO bude utvrđen ili odbijen.

5. [] prethodno navedeni objekt ne posjeduje USPPO.

6. Ova potvrda o USPPO-u ističe: ..... (*dd/mm/gggg*), ili prema drukčijoj preporuci NST-a/ZST-a. U slučaju ranijeg poništenja ili bilo kakvih promjena prethodno navedenih podataka bit ćete obaviješteni.

7. Napomene:

   .....

   NST/ZST koji daje odgovor Ime: ..... Datum *(dd/mm/gggg)* .....

<Mjesto za upućivanje na primjenjivo zakonodavstvo o osobnim podacima i poveznica na obvezne informacije za osobu čiji se podaci obrađuju, npr. kako se provodi članak 13. Opće uredbe o zaštiti podataka ([2]).>

([2]) Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) (SL L 119, 4.5.2016., str. 1.).

Dodatak E

Minimalni zahtjevi za zaštitu klasificiranih podataka EU-a u elektroničkom obliku stupnja tajnosti RESTREINT UE/EU RESTRICTED s kojima se postupa u CIS-u ugovaratelja

Općenito

1. Ugovaratelj je dužan osigurati da je zaštita podataka stupnja tajnosti RESTREINT UE/EU RESTRICTED u skladu s minimalnim sigurnosnim zahtjevima propisanima u ovoj klauzuli o sigurnosti i sa svim ostalim dodatnim zahtjevima koje preporučuje javni naručitelj ili, po potrebi, nacionalno sigurnosno tijelo (NST) ili zaduženo sigurnosno tijelo (ZST).

2. Odgovornost je ugovaratelja da primijeni sigurnosne zahtjeve utvrđene u ovom dokumentu.

3. Za potrebe ovog dokumenta komunikacijski i informacijski sustav (CIS) obuhvaća svu opremu koja se upotrebljava za postupanje s klasificiranim podacima EU-a, njihovo čuvanje i slanje, uključujući radne stanice, pisače, kopirne uređaje, telefaks uređaje, poslužitelje, sustave za upravljanje mrežom, upravljače mrežom i upravljače komunikacijom, prijenosna računala, računala notebook, tablet računala, pametne telefone i prijenosne uređaje za pohranu podataka kao što su USB-ovi, CD-ovi, SD kartice itd.

4. Posebna oprema, kao što su kriptografski proizvodi, mora biti zaštićena u skladu s odgovarajućim sigurnosno-operativnim postupcima (SecOP-i).

5. Ugovaratelji moraju uspostaviti strukturu odgovornu za upravljanje sigurnošću CIS-a koji postupa s podacima klasificiranima stupnjem tajnosti RESTREINT UE/EU RESTRICTED i imenovati službenika za sigurnost odgovornog za dotičan objekt.

6. Upotreba informatičkih rješenja (hardver, softver ili usluge) u privatnom vlasništvu osoblja ugovaratelja za čuvanje ili obradu podataka stupnja tajnosti RESTREINT UE/EU RESTRICTED nije dopuštena.

7. Akreditaciju CIS-a ugovaratelja koji postupa s podacima klasificiranima stupnjem tajnosti RESTREINT UE/EU RESTRICTED mora odobriti tijelo za sigurnosnu akreditaciju (SAA) dotične države članice ili je treba delegirati službeniku za sigurnost ugovaratelja u skladu s nacionalnim zakonima i propisima.

8. Samo se s podacima klasificiranima stupnjem tajnosti RESTREINT UE/EU RESTRICTED koji su kodirani upotrebom odobrenih kriptografskih proizvoda može postupati odnosno može ih se čuvati ili slati (putem žice ili bežičnim putem) kao i sve druge neklasificirane podatke u okviru ugovora. Te kriptografske proizvode mora odobriti EU ili država članica.

9. Vanjski objekti koji sudjeluju u radovima održavanja/popravka moraju biti ugovorno obvezani da će poštovati primjenjive odredbe za postupanje s podacima klasificiranima stupnjem tajnosti RESTREINT UE/EU RESTRICTED, kako je utvrđeno u ovom dokumentu.

10. Na zahtjev javnog naručitelja ili nadležnog NST-a/ZST-a/SAA-a ugovaratelj mora dostaviti dokaz o poštovanju ugovorne klauzule o sigurnosti. Ako je za osiguranje poštovanja tih zahtjeva ujedno potrebno provesti reviziju i inspekciju postupaka i objekata ugovaratelja, ugovaratelji predstavnicima javnog naručitelja, NST-a/ZST-a/SAA-a ili relevantnog sigurnosnog tijela EU-a dopuštaju provođenje takve revizije i inspekcije.

Fizička sigurnost

11. Područja na kojima se CIS upotrebljava za prikaz, čuvanje, obradu ili slanje podataka stupnja tajnosti RESTREINT UE/EU RESTRICTED ili područja na kojima se nalaze poslužitelji, sustavi za upravljanje mrežom, upravljači mrežom i upravljači komunikacijom za takav CIS trebala bi biti odvojena i kontrolirana mjesta s primjerenim sustavom za kontrolu pristupa. Pristup tim odvojenim i kontroliranim područjima trebao bi se ograničiti na pojedince s posebnim ovlaštenjem. Ne dovodeći u pitanje stavak 8., oprema opisana u stavku 3. mora se čuvati u takvim odvojenim i kontroliranim mjestima.

12. Sigurnosni mehanizmi i/ili postupci moraju se provesti kako bi se uredilo uvođenje ili povezivanje uklonjivih računalnih medija za pohranu podataka (kao što su USB-ovi, uređaji za masovnu pohranu ili CD-RW-ovi) s komponentama CIS-a.

Pristup CIS-u

13. Pristup CIS-u ugovaratelja koji postupa s klasificiranim podacima EU-a dopušta se na temelju stroge nužnosti pristupa podacima i ovlaštenja osoblja.

14. Svi CIS-ovi moraju imati ažurirane popise ovlaštenih korisnika. Svi korisnici moraju na početku svake sesije obrade proći provjeru autentičnosti.

15. Lozinke, koje su dio većine sigurnosnih mjera identifikacije i provjere autentičnosti, moraju sadržavati najmanje devet znakova i moraju sadržavati numeričke znakove i „posebne" znakove (ako sustav to dopušta) te abecedne znakove. Lozinke se moraju mijenjati najmanje svakih 180 dana. Moraju se promijeniti što prije ako su ugrožene ili otkrivene neovlaštenoj osobi ili ako se sumnja na takvu ugroženost ili otkrivanje.

16. Svi CIS-ovi moraju imati unutarnju kontrolu pristupa kako bi se spriječilo da neovlašteni korisnici pristupe podacima klasificiranima stupnjem tajnosti RESTREINT UE/EU RESTRICTED ili ih izmijene ili da izmijene kontrole sustava i sigurnosne kontrole. Odjava korisnika iz CIS-a je automatska ako su njihovi terminali određeno vrijeme neaktivni ili CIS mora nakon 15 minuta neaktivnosti aktivirati čuvara zaslona zaštićenog lozinkom.

17. Svakom korisniku CIS-a dodjeljuju se jedinstven korisnički račun i korisničko ime. Korisnički računi moraju se automatski zaključati ako je došlo do najmanje pet uzastopnih pokušaja prijava s pogrešnim podacima.

18. Svi korisnici CIS-a moraju biti svjesni svojih odgovornosti i postupaka koje trebaju slijediti kako bi zaštitili podatke koji su u CIS-u klasificirani stupnjem tajnosti RESTREINT UE/EU RESTRICTED. Odgovornosti i postupci kojih se potrebno pridržavati moraju biti dokumentirani te ih korisnici moraju potvrditi u pisanom obliku.

19. SecOP-i moraju biti dostupni korisnicima i administratorima te moraju sadržavati opis sigurnosnih uloga i povezani popis zadaća, uputa i planova.

Evidencija, revizija i odgovori na incidente

20. Svaki pristup CIS-u potrebno je zabilježiti.

21. Sljedeći događaji moraju biti zabilježeni:

    (a) svi pokušaji prijave, bez obzira na to je li prijava bila uspješna ili neuspješna;

    (b) odjave (uključujući zbog neaktivnosti, ako je primjenjivo);

    (c) stvaranje, brisanje ili izmjene prava pristupa i povlastica;

    (d) stvaranje, brisanje ili izmjene lozinki.

22. Za sve prethodno navedene događaje potrebno je dostaviti barem sljedeće informacije:

    (a) vrstu događaja;

    (b) korisničko ime;

    (c) datum i vrijeme;

    (d) identifikacijsku oznaku uređaja.

23. Zapisi iz evidencije trebali bi pomoći službeniku za sigurnost u ispitivanju potencijalnih sigurnosnih incidenata. Mogu se upotrijebiti i za potporu sudskim istragama u slučaju sigurnosnog incidenta. Trebalo bi redovito provjeravati sve zapise o sigurnosti kako bi se utvrdili potencijalni sigurnosni incidenti. Zapisi iz evidencije moraju biti zaštićeni od neovlaštenog brisanja ili izmjene.

24. Ugovaratelj mora imati utvrđenu strategiju za odgovor na sigurnosne incidente. Korisnicima i administratorima treba dati upute o tome kako odgovoriti na incidente, kako ih prijaviti i što učiniti u slučaju izvanredne situacije.

25. Ugroženost podataka klasificiranih stupnjem tajnosti RESTREINT UE/EU RESTRICTED ili sumnja na takvu ugroženost mora se prijaviti javnom naručitelju. Izvješće mora sadržavati opis obuhvaćenih podataka i opis okolnosti ugroženosti ili sumnje na ugroženost. Svi korisnici CIS-a moraju znati kako službeniku za sigurnost prijaviti stvaran sigurnosni incident ili sumnju na takav incident.

Umrežavanje i međusobno povezivanje

26. Ako je CIS ugovaratelja koji postupa s podacima klasificiranima stupnjem tajnosti RESTREINT UE/EU RESTRICTED međusobno povezan s CIS-om koji nije akreditiran, time se znatno povećava prijetnja sigurnosti CIS-a i podataka klasificiranih stupnjem tajnosti RESTREINT UE/EU RESTRICTED s kojima taj CIS postupa. To obuhvaća internet i ostale javne ili privatne CIS-ove, kao što su drugi CIS-ovi u vlasništvu ugovaratelja ili podugovaratelja. U tom slučaju ugovaratelj mora provesti procjenu rizika kako bi utvrdio dodatne sigurnosne zahtjeve koje treba provesti u okviru postupka sigurnosne akreditacije. Ugovaratelj javnom naručitelju i, ako se to zahtijeva nacionalnim zakonima i propisima, nadležnom tijelu za sigurnosnu akreditaciju podnosi izjavu o sukladnosti kojom potvrđuje da su CIS ugovaratelja i povezana međusobna povezivanja akreditirana za postupanje s klasificiranim podacima EU-a stupnja tajnosti RESTREINT UE/EU RESTRICTED.

27. Daljinski pristup LAN uslugama s drugih sustava (npr. daljinski pristup e-pošti i daljinska podrška sustavu) zabranjen je osim ako je javni naručitelj proveo i dogovorio posebne sigurnosne mjere i ako ih je, u skladu s nacionalnim zakonima i propisima, odobrilo nadležno tijelo za sigurnosnu akreditaciju.

Upravljanje konfiguracijama

28. Detaljna konfiguracija hardvera i softvera, kako je navedeno u dokumentaciji za akreditaciju/odobrenje (uključujući dijagrame sustava i mreže), mora biti dostupna i redovito se održavati.

29. Službenik za sigurnost ugovaratelja mora provjeriti konfiguracije na hardveru i softveru kako bi se osiguralo da nisu ugrađeni neovlašteni hardver ili softver.

30. Potrebno je procijeniti kako promjene u konfiguraciji CIS-a ugovaratelja utječu na sigurnost, a te promjene mora odobriti službenik za sigurnost i, ako se to zahtijeva nacionalnim zakonima i propisima, tijelo za sigurnosnu akreditaciju.

31. Potrebno je barem jedanput tromjesečno provjeriti sadržava li sustav sigurnosne nedostatke. Potrebno je instalirati softver za otkrivanje zlonamjernih programa i redovito ga ažurirati. Takav bi softver po mogućnosti trebao biti priznat na nacionalnoj ili međunarodnoj razini ili barem općepriznat industrijski standard.

32. Ugovaratelj mora izraditi plan neprekidnosti poslovanja. Potrebno je utvrditi postupke za sigurnosno kopiranje koji bi obuhvaćali sljedeće:

a) učestalost sigurnosnog kopiranja;

b) zahtjevi za pohranu na lokaciji (vatrootporni spremnici) ili izvan nje;

c) kontrolu ovlaštenog pristupa sigurnosnim kopijama.

Čišćenje i uništavanje

33. Za CIS ili medije za pohranu podataka koji su u bilo kojem trenutku sadržavali podatke stupnja tajnosti RESTREINT UE/EU RESTRICTED potrebno je prije odlaganja provesti u nastavku opisano čišćenje cijelog sustava ili medija za pohranu:

a) izbrisivu memoriju (npr. USB-ovi, SD kartice, SSD diskovi, hibridni tvrdi diskovi) treba prebrisati najmanje tri puta i zatim provjeriti da se izvorni sadržaj ne može vratiti ili ih treba izbrisati upotrebom odobrenog softvera za brisanje;

b) magnetske medije (npr. tvrdi diskovi) treba prebrisati ili demagnetizirati;

c) optičke medije (npr. CD-ovi, DVD-ovi) treba trajno uništiti ili dezintegrirati;

d) za sve ostale medije za pohranu potrebno je savjetovati se s javnim naručiteljem ili, po potrebi, NST-om/ZST-om/SAA-om u pogledu sigurnosnih zahtjeva koje treba ispuniti.

34. Podaci klasificirani stupnjem tajnosti RESTREINT UE/EU RESTRICTED moraju se očistiti na svim medijima za pohranu podataka prije nego što se daju bilo kojem subjektu koji nije ovlašten pristupiti podacima klasificiranima stupnjem tajnosti RESTREINT UE/EU RESTRICTED (npr. radi održavanja).

PRILOG IV.

Uvjerenja o sigurnosnoj provjeri pravne osobe i sigurnosnoj provjeri osobe za ugovaratelje koja obuhvaća podatke stupnja tajnosti RESTREINT UE/EU RESTRICTED i NST-ovi/ZST-ovi koji zahtijevaju obavijest o klasificiranim ugovorima stupnja tajnosti RESTREINT UE/EU RESTRICTED ([1])

Država članica	USPPO		Obavijest NST-a/ZST-a o ugovoru ili podugovoru koji obuhvaća podatke stupnja tajnosti R-UE/EU-R		USP	
	DA	NE	DA	NE	DA	NE
Belgija		X		X		X
Bugarska		X		X		X
Češka		X		X		X
Danska	X		X		X	
Njemačka		X		X		X
Estonija	X		X			X
Irska		X		X		X
Grčka	X			X	X	
Španjolska		X	X			X
Francuska		X		X		X
Hrvatska		X	X			X
Italija		X	X			X
Cipar		X	X			X
Latvija		X		X		X

([1]) Tim se nacionalnim zahtjevima za USPPO/USP i obavijestima o ugovorima koji obuhvaćaju podatke stupnja tajnosti RESTREINT UE/EU RESTRICTED ne smiju određivatinikakve dodatne obveze ostalim državama članicama ili ugovarateljima u njihovoj nadležnosti.

Napomena: Obavezno je obavijestiti o ugovorima koji obuhvaćaju podatke stupnja tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET.

Država članica	USPPO		Obavijest NST-a/ZST-a o ugovoru ili podugovoru koji obuhvaća podatke stupnja tajnosti R-UE/EU-R		USP	
	DA	NE	DA	NE	DA	NE
Litva	X		X			X
Luksemburg	X		X		X	
Mađarska		X		X		X
Malta		X		X		X
Nizozemska	X (samo za ugovore povezane s obranom)		X (samo za ugovore povezane s obranom)			X
Austrija		X		X		X
Poljska		X		X		X
Portugal		X		X		X
Rumunjska		X		X		X
Slovenija	X		X			X
Slovačka	X		X			X
Finska		X		X		X
Švedska	X (samo za ugovore povezane s obranom)		X (samo za ugovore povezane s obranom)		X (samo za ugovore povezane s obranom)	
Ujedinjena Kraljevina		X		X		X

PRILOG V.

POPIS SLUŽBI NACIONALNIH SIGURNOSNIH TIJELA/ZADUŽENIH SIGURNOSNIH TIJELA KOJE SU ODGOVORNE ZA POSTUPKE POSTUPANJA POVEZANE S GOSPODARSKOM SIGURNOŠĆU

BELGIJA

National Security Authority
FPS Foreign Affairs
Rue des Petits Carmes 15
1000 Bruxelles
Tel. +32 25014542 (tajništvo)
Faks +32 25014596
E-pošta: nvo-ans@diplobel.fed.be

BUGARSKA

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

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

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

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

   (Prethodno navedena nadležna tijela provode postupke provjere za izdavanje USPPO-ova pravnim subjektima koji se prijavljuju za sklapanje klasificiranog ugovora, kao i za izdavanje USP-ova pojedincima koji provode klasificirani ugovor za potrebe tih tijela.)

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

   (Prethodno navedena sigurnosna služba provodi postupke provjere za izdavanje USPPO-ova i USP-ova svim ostalim pravnim subjektima i osobama u zemlji koji se prijavljuju za sklapanje klasificiranog ugovora ili provode klasificirani ugovor.)

ČEŠKA

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

DANSKA

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

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

NJEMAČKA

1. Za pitanja o politici gospodarske sigurnosti, USPPO-ovima, planovima prijevoza (osim za kriptomaterijal/CCI):
Federal Ministry of Economic Affairs and Energy
Industrial Security Division - ZB3
Villemombler Str. 76
53123 Bonn
Tel. +49 228996154028
Faks +49 228996152676
E-pošta: dsagermany-zb3@bmwi.bund.de (adresa e-pošte ureda)

2. For standard visit requests from/to German companies:
Federal Ministry of Economic Affairs and Energy
Industrial Security Division – ZB2
Villemombler Str. 76
53123 Bonn
Tel. +49 228996152401
Faks +49 228996152603
E-pošta: zb2-international@bmwi.bund.de (adresa e-pošte ureda)

3. Planovi prijevoza za kriptomaterijal:
Federal Office for Information Security (BSI)
National Distribution Agency/NDA-EU DEU
Mainzer Str. 84
53179 Bonn
Tel. +49 2289995826052
Faks +49 228991095826052
E-pošta: NDAEU@bsi.bund.de

ESTONIJA

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

IRSKA

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

GRČKA

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
Faks +30 2106527612
E-pošta: daa.industrial@hndgs.mil.gr

ŠPANJOLSKA

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Calle Argentona 30
28023 Madrid
Tel. +34 913725000
Faks +34 913725808
E-pošta: nsa-sp@areatec.com
Za pitanja o uvjerenju o sigurnosnoj provjeri osobe: asip@areatec.com
Za planove prijevoza i međunarodne posjete: sp-ivtco@areatec.com

FRANCE

National Security Authority (NSA) (za politiku i provedbu u područjima koja nisu obrambena industrija)
Secrétariat général de la défense et de la sécurité nationale
Sous-direction Protection du secret (SGDSN/PSD)
51 boulevard de la Tour-Maubourg
75700 Pariz 07 SP
Tel. +33 171758193
Faks +33 171758200
E-pošta: ANSFrance@sgdsn.gouv.fr

Designated Security Authority (za provedbu u obrambenoj industriji)
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 Pariz Cedex 15
Tel. +33 988670421
E-pošta: za obrasce i poslane zahtjeve za posjet: dga-ssdi.ai.fct@intradef.gouv.fr
za zaprimljene zahtjeve za posjet: dga-ssdi.visit.fct@intradef.gouv.fr

HRVATSKA

Ured Vijeća za nacionalnu sigurnost
Croatian NSA
Jurjevska 34
10000 Zagreb
Tel. +385 14681222
Faks +385 14686049
E-pošta: NSACroatia@uvns.hr

ITALIJA

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

CIPAR

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

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

LATVIJA

National Security Authority
Constitution Protection Bureau of the Republic of Latvia
P.O. Box 286
Riga LV-1001
Tel. +371 67025418, +371 67025463
Faks +371 67025454
E-pošta: 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
Faks +370 70666700
E-pošta: nsa@vsd.lt

LUKSEMBURG

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

MAĐARSKA

National Security Authority of Hungary
H-1399 Budapest P.O. Box 710/50
H-1024 Budapest, Szilágyi Erzsébet fasor 11/B
Tel. +36 13911862
Faks +36 13911889
E-pošta: 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
Faks +356 21242406
E-pošta: certification@mccaa.org.mt

NIZOZEMSKA

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

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

AUSTRIJA

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

2. ZST u vojnom području:
BMLVS/Abwehramt
Postfach 2000
1030 Vienna
E-pošta: abwa@bmlvs.gv.at

POLJSKA

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

PORTUGAL

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

RUMUNJSKA

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
Faks +40 212245830
E-pošta: relatii.publice@orniss.ro, nsa.romania@nsa.ro

SLOVENIJA

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

SLOVAČKA

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

FINSKA

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

ŠVEDSKA

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

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

UJEDINJENA KRALJEVINA

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