ODLUKA KOMISIJE (EU, Euratom) 2021/259

od 10. veljače 2021.

o utvrđivanju provedbenih pravila o gospodarskoj sigurnosti u pogledu klasificiranih bespovratnih sredstava

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 Uredbu (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 ([1]),

uzimajući u obzir Odluku Komisije (EU, Euratom) 2015/443 od 13. ožujka 2015. o sigurnosti u Komisiji ([2]),

uzimajući u obzir Odluku Komisije (EU, Euratom) 2015/444 od 13. ožujka 2015. o sigurnosnim propisima za zaštitu klasificiranih podataka EU-a ([3]),

uzimajući u obzir Odluku Komisije (EU, Euratom) 2017/46 od 10. siječnja 2017. o sigurnosti komunikacijskih i informacijskih sustava u Europskoj komisiji ([4]),

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. te Odluke utvrditi u provedbenim pravilima o gospodarskoj sigurnosti, kojima će se urediti pitanja kao što su dodjeljivanje klasificiranih sporazuma o dodjeli bespovratnih sredstava, 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 sporazume o dodjeli bespovratnih sredstava potrebno provesti u bliskoj suradnji s nacionalnim sigurnosnim tijelom, zaduženim sigurnosnim tijelom ili bilo kojim drugim nadležnim tijelom predmetne države članice. Države članice dogovorile 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 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) ([5]).

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

(3) Vijeće, Komisija i Visoki predstavnik Unije za vanjske poslove i sigurnosnu politiku dogovorili 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 ([6]) o sigurnosnim propisima za zaštitu klasificiranih podataka EU-a.

(4) Stoga bi se Komisijinim provedbenim pravilima o gospodarskoj sigurnosti u pogledu klasificiranih bespovratnih sredstava trebala osigurati najveća moguća usklađenost i uzeti u obzir smjernice o gospodarskoj sigurnosti koje je Sigurnosni odbor Vijeća odobrio 13. prosinca 2016.

(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,

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 bespovratnih sredstava u smislu Odluke (EU, Euratom) 2015/444, a posebno njezina poglavlja 6.

2. Ovom Odlukom utvrđuju se posebni zahtjevi kako bi se osigurala zaštita klasificiranih podataka EU-a (EUCI) u objavi pozivâ te pri dodjeli bespovratnih sredstava i provedbi klasificiranih sporazuma o dodjeli bespovratnih sredstava koje je sklopila Europska komisija.

3. Ova Odluka odnosi se na bespovratna sredstva koja uključuju podatke klasificirane stupnjevima tajnosti u nastavku:

(a) RESTREINT UE/EU RESTRICTED;

(b) CONFIDENTIEL UE/EU CONFIDENTIAL;

(c) SECRET UE/EU SECRET.

4. Ova se Odluka primjenjuje ne dovodeći u pitanje posebna pravila utvrđena u drugim pravnim aktima, kao što su ona koja se odnose na Europski program industrijskog razvoja u području obrane.

Članak 2.

Odgovornosti unutar Komisije

1. U okviru odgovornosti dužnosnika za ovjeravanje tijela koje dodjeljuje bespovratna sredstva iz Uredbe (EU, Euratom) 2018/1046 Europskog parlamenta i Vijeća, dužnosnik za ovjeravanje osigurava da je klasificirana dodjela bespovratnih sredstava u skladu s Odlukom (EU, Euratom) 2015/444 i njezinim provedbenim pravilima.

([6]) 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.).

([7]) Odluka Komisije od 4. svibnja 2016. o ovlaštenju povezanom sa sigurnošću [C(2016) 2797 final].

2. U tu svrhu taj se dužnosnik za ovjeravanje u svim fazama savjetuje sa sigurnosnim tijelom Komisije o pitanjima sigurnosnih elemenata klasificiranog sporazuma o dodjeli bespovratnih sredstava, programa ili projekta te o potpisanim klasificiranim sporazumima o dodjeli bespovratnih sredstava obavještava lokalnog službenika za sigurnost. Odluku o stupnju tajnosti određenih tema donosi tijelo koje dodjeljuje bespovratna sredstva uzimajući u obzir vodič za stupnjeve tajnosti.

3. Ako se primjenjuju sigurnosne upute za program ili projekt iz članka 5. stavka 3., tijelo koje dodjeljuje bespovratna sredstva i sigurnosno tijelo Komisije ispunjavaju dužnosti koje su im dodijeljene u tim uputama.

4. Poštujući zahtjeve iz ovih provedbenih pravila sigurnosno tijelo Komisije blisko surađuje s nacionalnim sigurnosnim tijelima („NST”) i zaduženim sigurnosnim tijelima („ZST”) predmetne države članice, posebno u pogledu uvjerenja o sigurnosnoj provjeri pravne osobe („USPPO”) i uvjerenja o sigurnosnoj provjeri osobe („USP”), postupaka za posjete i planova prijevoza.

5. Ako bespovratnim sredstvima upravljaju izvršne agencije EU-a ili druga tijela za financiranje, i ne primjenjuju se posebna pravila iz drugih pravnih akata iz članka 1. stavka 4.:

(a) služba Komisije koja delegira upravljanje ostvaruje prava koja ima autor klasificiranih podataka EU-a nastalih u kontekstu bespovratnih sredstava ako je to omogućeno u dogovoru o delegiranju;

(b) služba Komisije koja delegira upravljanje odgovorna je za određivanje stupnja tajnosti;

(c) zahtjevi za informacije o uvjerenju o sigurnosnoj provjeri i obavijesti nacionalnim sigurnosnim tijelima i/ili zaduženim sigurnosnim tijelima šalju se preko sigurnosnog tijela Komisije.

POGLAVLJE 2.

POSTUPANJE S POZIVIMA ZA KLASIFICIRANU DODJELU BESPOVRATNIH SREDSTAVA

Članak 3.

Osnovna načela

1. Klasificirane dijelove dodjele bespovratnih sredstava provode samo korisnici koji su registrirani u državi članici ili korisnici koji su registrirani u trećoj zemlji ili ih je osnovala međunarodna organizacija ako je ta treća zemlja ili međunarodna organizacija sklopila sporazum o sigurnosti podataka s Unijom ili administrativni dogovor s Komisijom ([8]).

2. Prije objave poziva za klasificiranu dodjelu bespovratnih sredstava tijelo koje dodjeljuje bespovratna sredstva određuje stupanj tajnosti svih podataka koji se mogu dostaviti podnositeljima zahtjeva. Tijelo koje dodjeljuje bespovratna sredstva određuje i najviši stupanj tajnosti svih podataka koji se upotrebljavaju ili nastaju tijekom izvršenja sporazuma o dodjeli bespovratnih sredstava, 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).

3. Tijelo koje dodjeljuje bespovratna sredstva osigurava da se u pozivima za dodjelu klasificiranih bespovratnih sredstava navode informacije o posebnim sigurnosnim obvezama povezanima s klasificiranim podacima. Dokumentacija poziva uključuje pojašnjenja o vremenskom rasporedu za korisnike za stjecanje USPPO-a, ako su potrebni. U prilozima I. i II. nalaze se primjeri predložaka za informacije o uvjetima poziva.

([8]) 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.

4. Tijelo koje dodjeljuje bespovratna sredstva osigurava da se podaci klasificirani stupnjem tajnosti RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET podnositeljima zahtjeva otkrivaju tek nakon što potpišu ugovor o povjerljivosti podataka kojim se podnositelji zahtjeva obvezuju da s klasificiranim podacima EU-a postupaju i štite ih u skladu s Odlukom (EU, Euratom) 2015/444, njezinim provedbenim pravilima i primjenjivim nacionalnim propisima.

5. Ako se podnositeljima zahtjeva dostavljaju podaci stupnja tajnosti RESTREINT UE/EU RESTRICTED, minimalni zahtjevi iz članka 5. stavka 7. ove Odluke uvrštavaju se u poziv ili ugovore o povjerljivosti podataka sklopljene u fazi prijedloga.

6. Svi podnositelji zahtjeva i korisnici koji moraju postupati s podacima klasificiranima stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET ili ih čuvati u svojim objektima, u fazi prijedloga ili tijekom izvršenja samog klasificiranog sporazuma o dodjeli bespovratnih sredstava moraju imati USPPO potrebne razine, osim u slučajevima iz stavka 9. U nastavku su utvrđena tri scenarija do kojih može doći u fazi prijedloga za klasificiranu dodjelu bespovratnih sredstava koji obuhvaćaju klasificirane podatke EU-a stupnja tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET:

(a) bez pristupa klasificiranim podacima EU-a stupnja tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET u fazi prijedloga:

ako se poziv odnosi na bespovratna sredstva koja će obuhvaćati klasificirane podatke EU-a stupnja tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET, ali podnositelj zahtjeva u fazi prijedloga ne mora postupati s tim podacima, podnositelj zahtjeva koji nema USPPO potrebne razine ne isključuje se iz postupka podnošenja zahtjeva zato što nema USPPO;

(b) pristup klasificiranim podacima EU-a stupnja tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET u prostorima tijela koje dodjeljuje bespovratna sredstva u fazi prijedloga:

pristup se odobrava osoblju podnositelja zahtjeva koje ima USP potrebne razine i za koje je utvrđena nužnost pristupa podacima;

(c) postupanje s klasificiranim podacima EU-a stupnja tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET ili njihovo čuvanje u prostorima podnositelja zahtjeva u fazi prijedloga:

ako se u pozivu od podnositelja zahtjeva zahtijeva da postupa s klasificiranim podacima EU-a ili ih čuva u svojim prostorima, on mora imati USPPO potrebne razine. U takvim okolnostima, prije nego što se podnositelju zahtjeva omogući pristup klasificiranim podacima EU-a, tijelo koje dodjeljuje bespovratna sredstva preko sigurnosnog tijela Komisije dobiva od nadležnog NST-a ili ZST-a potvrdu da je podnositelju zahtjeva odobren odgovarajući USPPO. Pristup se odobrava osoblju podnositelja zahtjeva koje ima USP potrebne razine i za koje je utvrđena nužnost pristupa podacima.

7. USPPO ili USP u načelu nije potreban za pristup podacima stupnja tajnosti RESTREINT UE/EU RESTRICTED, ni u fazi prijedloga ni za izvršenje sporazuma o dodjeli bespovratnih sredstava. Ako države članice zahtijevaju USPPO ili USP za sporazume o dodjeli bespovratnih sredstava 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 sporazuma o dodjeli bespovratnih sredstava ili podugovora ili nadmetanja za njih isključuju podnositelji zahtjeva, korisnici ili podugovaratelji iz država članica koje nemaju takve zahtjeve u pogledu USPPO-a za pristup podacima stupnja tajnosti RESTREINT UE/EU RESTRICTED. Ti se sporazumi o dodjeli bespovratnih sredstava izvršavaju u državama članicama u skladu s njihovim nacionalnim zakonima i propisima.

8. Ako je USPPO potreban za postupak poziva i izvršenje klasificiranog sporazuma o dodjeli bespovratnih sredstava, tijelo koje dodjeljuje bespovratna sredstva preko sigurnosnog tijela Komisije podnosi zahtjev NST-u ili ZST-u korisnika upotrebljavajući informativni obrazac o uvjerenju o sigurnosnoj provjeri pravne osobe ili bilo koji utvrđeni istovrijedni elektronički oblik. Dodatak D Prilogu III. sadržava primjer informativnog obrasca o uvjerenju o sigurnosnoj provjeri pravne osobe ([9]). Odgovor na informativni obrazac o uvjerenju o sigurnosnoj provjeri pravne osobe dostavlja se u roku od deset radnih dana od datuma podnošenja zahtjeva.

9. Ako vladine ustanove ili ustanove pod nadzorom vlade u državama članicama sudjeluju u klasificiranim bespovratnim sredstvima za koje se zahtijevaju USPPO-i te ako USPPO-i nisu izdani za te ustanove na temelju nacionalnih zakona, tijelo koje dodjeljuje bespovratna sredstva preko sigurnosnog tijela Komisije provjerava kod predmetnog NST-a ili ZST-a mogu li te vladine ustanove postupati s klasificiranim podacima EU-a potrebne razine.

([9]) Drugi obrasci koji se upotrebljavaju mogu se razlikovati od primjera iz ovih provedbenih pravila.

10. Ako je USP potreban za izvršenje klasificiranog sporazuma o dodjeli bespovratnih sredstava i ako je prema nacionalnim zakonima USPPO potreban prije odobravanja USP-a, tijelo koje dodjeljuje bespovratna sredstva s pomoću informativnog obrasca o uvjerenju o sigurnosnoj provjeri pravne osobe preko sigurnosnog tijela Komisije provjerava kod NST-a ili ZST-a korisnika posjeduje li on USPPO ili je postupak za USPPO u tijeku. U tom slučaju Komisija ne izdaje zahtjeve za USP-e upotrebom informativnog obrasca o uvjerenju o sigurnosnoj provjeri osobe.

Članak 4.

Podugovaranje pri klasificiranoj dodjeli bespovratnih sredstava

1. Uvjeti pod kojima korisnik može podugovarati zadaće djelovanja koje obuhvaćaju klasificirane podatke EU-a utvrđuju se u pozivu i sporazumu o dodjeli bespovratnih sredstava Ti uvjeti uključuju zahtjev da se svi informativni obrasci o uvjerenju o sigurnosnoj provjeri pravne osobe podnose preko sigurnosnog tijela Komisije. Podugovaranje podliježe prethodnoj pisanoj suglasnosti tijela koje dodjeljuje bespovratna sredstva. Prema potrebi, podugovaranje mora biti u skladu s temeljnim aktom o uspostavi programa.

2. Klasificirani dijelovi dodjele bespovratnih sredstava daju se u podugovor samo subjektima koji su registrirani u državi članici ili 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 Unijom ili administrativni dogovor s Komisijom ([10]).

POGLAVLJE 3.

POSTUPANJE S KLASIFICIRANIM BESPOVRATNIM SREDSTVIMA

Članak 5.

Osnovna načela

1. Pri dodjeli klasificiranih bespovratnih sredstava tijelo koje dodjeljuje bespovratna sredstva zajedno sa sigurnosnim tijelom Komisije osigurava da sporazum o dodjeli bespovratnih sredstava obuhvaća obveze korisnika u pogledu zaštite klasificiranih podataka EU-a koji su upotrijebljeni ili nastali pri izvršenju sporazuma o dodjeli bespovratnih sredstava. Sigurnosni zahtjevi povezani s pojedinim bespovratnim sredstvima u obliku su pisma o sigurnosnim aspektima („SAL”). Primjer predloška pisma o sigurnosnim aspektima nalazi se u Prilogu III.

2. Prije potpisivanja klasificiranog sporazuma o dodjeli bespovratnih sredstava tijelo koje dodjeljuje bespovratna sredstva odobrava vodič za stupnjeve tajnosti („SCG”) za zadaće koje će se obavljati i podatke nastale pri izvršenju sporazuma o dodjeli bespovratnih sredstava 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 u obliku su 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 postupku savjetovanja podnosi Komisijinoj stručnoj skupini za sigurnost. Ako je sporazum o dodjeli bespovratnih sredstava dio programa ili projekta s vlastitim SUP-om, pismo o sigurnosnim aspektima sporazuma o dodjeli bespovratnih sredstava ima pojednostavnjeni oblik te se u njemu upućuje na sigurnosne odredbe utvrđene u SUP-u programa ili projekta.

4. Osim u slučajevima iz članka 3. stavka 9., klasificirani sporazum o dodjeli bespovratnih sredstava ne potpisuje se sve dok NST ili ZST podnositelja zahtjeva ne potvrdi USPPO podnositelja zahtjeva ili, ako se klasificirani sporazum o dodjeli bespovratnih sredstava dodjeljuje konzorciju, sve dok NST ili ZST barem jednog podnositelja zahtjeva iz konzorcija, ili više ako je potrebno, ne potvrdi USPPO tog podnositelja zahtjeva.

5. U načelu, ako drugačije nije predviđeno drugim relevantnim propisima, tijelo koje dodjeljuje bespovratna sredstva smatra se autorom klasificiranih podataka EU-a koji su nastali pri izvršenju sporazuma o dodjeli bespovratnih sredstava

([10]) 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.

6. Tijelo koje dodjeljuje bespovratna sredstva preko sigurnosnog tijela Komisije obavještava NST-e i/ili ZST-e svih korisnika i podugovaratelja o potpisivanju klasificiranih sporazuma o dodjeli bespovratnih sredstava ili podugovora te o produljenju ili prijevremenom raskidu takvih sporazuma o dodjeli bespovratnih sredstava ili podugovora. Popis zahtjeva po zemljama naveden je u Prilogu IV.

7. Sporazumi o dodjeli bespovratnih sredstava koji obuhvaćaju podatke klasificirane stupnjem tajnosti RESTREINT UE/EU RESTRICTED sadržavaju odredbu o sigurnosti kojom odredbe utvrđene u Dodatku E Prilogu III. postaju obvezujuće za korisnike. Ti sporazumi o dodjeli bespovratnih sredstava obuhvaćaju pismo o sigurnosnim aspektima u kojem se utvrđuju najmanje zahtjevi za postupanje s podacima stupnja tajnosti RESTREINT UE/EU RESTRICTED, među ostalim aspekti o informacijskoj sigurnosti i posebni zahtjevi koje korisnici trebaju ispuniti u svrhu akreditacije CIS-a korisnika koji postupa s podacima stupnja tajnosti RESTREINT UE/EU RESTRICTED.

8. Ako se to zahtijeva nacionalnim zakonima i propisima država članica, NST-i ili ZST-i osiguravaju da korisnici ili podugovaratelji u njihovoj nadležnosti postupaju u skladu s primjenjivim sigurnosnim odredbama za zaštitu podataka stupnja tajnosti RESTREINT UE/EU RESTRICTED te provode posjete radi provjere objekata korisnika ili podugovaratelja koji se nalaze na njihovu državnom području. Ako NST ili ZST nema takvu obvezu, tijelo koje dodjeljuje bespovratna sredstva osigurava da korisnici provode potrebne sigurnosne odredbe navedene u Dodatku E Prilogu III.

Članak 6.

Pristup osoblja korisnika i podugovaratelja klasificiranim podacima EU-a

1. Tijelo koje dodjeljuje bespovratna sredstva osigurava da klasificirani sporazumi o dodjeli bespovratnih sredstava uključuju odredbe u kojima se navodi da se osoblju korisnika ili podugovaratelja kojima je za potrebe izvršenja klasificiranog sporazuma o dodjeli bespovratnih sredstava 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) relevantni NST ili ZST ili drugo nadležno sigurnosno tijelo proveo je nad njima sigurnosne provjere 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 preuzelo odgovornost za zaštitu takvih podataka.

2. Ako je primjenjivo, pristup klasificiranim podacima EU-a u skladu je i s temeljnim aktom o uspostavi programa te se u obzir uzimaju sve dodatne oznake definirane u SCG-u.

3. Ako korisnik 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 korisnika 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.

Članak 7.

Pristup stručnjaka koji sudjeluju u provjerama, pregledima i revizijama klasificiranim podacima EU-a

1. Ako su vanjske osobe („stručnjaci”) uključene u provjere, preglede ili revizije koje provodi tijelo koje dodjeljuje bespovratna sredstva ili u preglede uspješnosti korisnika kojima je potreban pristup podacima klasificiranima stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET, ugovor im se dostavlja samo ako je relevantni NST ili ZST ili drugo nadležno sigurnosno tijelo provelo nad njima sigurnosne provjere odgovarajuće razine. Tijelo koje dodjeljuje bespovratna sredstva preko sigurnosnog tijela Komisije provjerava stručnjake i, prema potrebi, traži od NST-a ili ZST-a da pokrenu postupak provjere stručnjaka najmanje šest mjeseci prije početka njihovih ugovora.

2. Prije potpisivanja ugovora stručnjaci su upućeni u primjenjiva sigurnosna pravila za zaštitu klasificiranih podataka EU-a te preuzimaju odgovornost za zaštitu takvih podataka.

POGLAVLJE 4.

POSJETI POVEZANI S KLASIFICIRANIM SPORAZUMIMA O DODJELI BESPOVRATNIH SREDSTAVA

Članak 8.

Osnovna načela

1. Ako je tijelu koje dodjeljuje bespovratna sredstva, stručnjacima, korisnicima ili podugovarateljima u kontekstu izvršenja klasificiranog sporazuma o dodjeli bespovratnih sredstava 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 predmetnim NST-ima ili ZST-ima ili drugim nadležnim sigurnosnim tijelima.

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

(a) posjeti se obavljaju u službene svrhe povezane s klasificiranim sporazumom o dodjeli bespovratnih sredstava;

(b) kako bi pristupili klasificiranim podacima EU-a koji su upotrijebljeni ili nastali pri izvršenju klasificirane dodjele bespovratnih sredstava, svi posjetitelji moraju imati USP potrebne razine i utvrđenu nužnost pristupa podacima.

Članak 9.

Zahtjevi za posjete

1. Posjeti korisnika ili podugovaratelja objektima drugih korisnika ili podugovaratelja ili prostorima tijela koje dodjeljuje bespovratna sredstva koji uključuju 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 ili ZST-u objekta. Predložak obrasca zahtjeva za posjet nalazi se u Dodatku C Prilogu III.;

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

(c) službenik za sigurnost objekta koji šalje posjetitelja zatim od svojeg NST-a ili ZST-a dobiva odgovor NST-a ili 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 dana posjeta nije uložen prigovor.

2. Posjeti službenika tijela koje dodjeljuje bespovratna sredstva, stručnjaka ili revizora objektima korisnika ili podugovaratelja koji uključuju 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 ili ZST-u objekta koji prima posjetitelja podnese zahtjev za posjet;

(c) sigurnosno tijelo Komisije dobiva od NST-a ili 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 dana posjeta nije uložen 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 godinu dana 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 dana posjeta.

Članak 10.

Postupci za posjete

1. Prije nego što posjetiteljima odobri pristup klasificiranim podacima EU-a, ured za sigurnost objekta koji prima posjetitelja postupa u skladu sa svim sigurnosnim postupcima i pravilima koji se odnose na posjet koje je utvrdio NST ili 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 zastupaju, datum isteka USP-a, datum posjeta i imena osoba koje su posjetili. Evidencija se čuva najmanje pet godina ili dulje ako se to zahtijeva nacionalnim pravilima i propisima zemlje u kojoj se nalazi objekt koji prima posjetitelja.

Članak 11.

Izravno organizirani posjeti

1. U kontekstu posebnih projekata, relevantni NST ili ZST i sigurnosno tijelo Komisije mogu se dogovoriti o postupku prema kojem se posjeti za konkretnu klasificiranu dodjelu bespovratnih sredstava mogu organizirati izravno 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 9. i članku 10. stavku 1.

2. Posjeti koji uključuju pristup podacima klasificiranima stupnjem tajnosti RESTREINT UE/EU RESTRICTED organiziraju se izravno između subjekta koji šalje i subjekta koji prima posjetitelja te nije potrebno slijediti postupke iz članka 9. i članka 10. stavka 1.

POGLAVLJE 5.

SLANJE I PRIJENOS KLASIFICIRANIH PODATAKA EU-A PRI IZVRŠENJU KLASIFICIRANIH SPORAZUMA O DODJELI BESPOVRATNIH SREDSTAVA

Članak 12.

Osnovna načela

Tijelo koje dodjeljuje bespovratna sredstva 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 sporazuma o dodjeli bespovratnih sredstava, među ostalim sa suglasnosti autora podatka.

Članak 13.

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 korisnika i koji se upotrebljavaju za postupanje s klasificiranim podacima EU-a za izvršenje sporazuma o dodjeli bespovratnih sredstava(„CIS korisnika”) 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. Sigurnosne mjere TEMPEST provode se u skladu s člankom 36. stavkom 6. te odluke.

2. Sigurnosna akreditacija CIS-a korisnika koji postupa s klasificiranim podacima EU-a stupnja tajnosti RESTREINT UE/EU RESTRICTED i svako njihovo međusobno povezivanje mogu se delegirati službeniku za sigurnost korisnika ako je to u skladu s nacionalnim zakonima i propisima. Ako se ta zadaća delegira, korisnik 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-i ili ZST-i te SAA-i i dalje su odgovorni za zaštitu podataka stupnja tajnosti RESTREINT UE/EU RESTRICTED s kojima korisnik postupa i zadržavaju pravo na inspekciju sigurnosnih mjera koje je korisnik poduzeo. Nadalje, korisnik tijelu koje dodjeljuje bespovratna sredstva i, ako se to zahtijeva nacionalnim zakonima i propisima, nadležnom nacionalnom tijelu za sigurnosnu akreditaciju podnosi izjavu o sukladnosti kojom potvrđuje da su CIS korisnika i međusobna povezivanja akreditirana za postupanje s klasificiranim podacima EU-a stupnja tajnosti RESTREINT UE/EU RESTRICTED ([11]).

Članak 14.

Prijevoz komercijalnom kurirskom službom

Pri prijevozu klasificiranih podataka EU-a komercijalnom kurirskom službom poštuju se relevantne odredbe Odluke Komisije (EU, Euratom) 2019/1962 ([12]) o provedbenim pravilima za postupanje s podacima stupnja tajnosti RESTREINT UE/EU RESTRICTED i Odluke Komisije (EU, Euratom) 2019/1961 ([13]) o provedbenim pravilima za postupanje s podacima stupnja tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET.

Članak 15.

Ručni prijenos

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

2. Osoblje korisnika može podatke stupnja tajnosti RESTREINT UE/EU RESTRICTED ručno prenositi unutar Unije ako su ispunjeni zahtjevi u nastavku:

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

(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 korisnika obavlja unutar države članice dogovara 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, među ostalim o referentnoj oznaci, stupnju tajnosti, očekivanom vremenu dolaska i imenu kurirske službe. Takav ručni prijenos dopušten je ako su ispunjeni zahtjevi u nastavku:

(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 čitavo 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 ono ovlašćuje za prijenos utvrđene klasificirane pošiljke.

([11]) 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.

([12]) Odluka Komisije (EU, Euratom) 2019/1962 od 17. listopada 2019. o provedbenim pravilima za postupanje s podacima stupnja tajnosti RESTREINT UE/EU RESTRICTED (SL L 311, 2.12.2019., str. 21.).

([13]) Odluka Komisije (EU, Euratom) 2019/1961 od 17. listopada 2019. o provedbenim pravilima za postupanje s podacima stupnja tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET (SL L 311, 2.12.2019., str. 1.).

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 korisnika primjenjuju se dodatna pravila u nastavku:

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

(b) u slučaju povrede sigurnosti NST ili 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 ili 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 njezinih dijelova koji su dovoljni da se utvrdi da pošiljka 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 korisnika podliježe odredbama sporazuma o sigurnosti podataka ili administrativnog dogovora koji su Unija ili Komisija sklopile s trećom zemljom ili međunarodnom organizacijom.

POGLAVLJE 6.

PLANIRANJE KONTINUITETA POSLOVANJA

Članak 16.

Krizni planovi i mjere oporavka

Tijelo koje dodjeljuje bespovratna sredstva osigurava da klasificirani sporazum o dodjeli bespovratnih sredstava obvezuje korisnika da donese krizne poslovne planove za zaštitu klasificiranih podataka EU-a s kojima se postupa u kontekstu izvršenja klasificiranog sporazuma o dodjeli bespovratnih sredstava u izvanrednim situacijama i da u kontekstu planiranja kontinuiteta poslovanja uspostavi preventivne mjere i mjere oporavka kako bi nepredviđeni događaji što manje utjecali na postupanje s klasificiranim podacima EU-a i njihovo čuvanje. Korisnici tijelu koje dodjeljuje bespovratna sredstva potvrđuju da imaju krizne poslovne planove.

Članak 17.

Stupanje na snagu

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

Sastavljeno u Bruxellesu 10. veljače 2021.

Za Komisiju,
u ime predsjednice,
Johannes HAHN
Član Komisije

PRILOG I.

STANDARDNE INFORMACIJE U POZIVU

(prilagoditi upotrijebljenom pozivu)

Sigurnost

Projekti koji uključuju klasificirane podatke EU-a moraju se sigurnosno pregledati prije odobrenja financiranja i na njih se mogu primjenjivati posebna sigurnosna pravila (detaljno opisana u pismu o sigurnosnim aspektima (SAL) koje je priloženo sporazumu o dodjeli bespovratnih sredstava).

Tim se pravilima (koja su uređena Odlukom Komisije (EU, Euratom) 2015/444 ([1]) i/ili nacionalnim propisima) predviđa, na primjer, sljedeće:

— projekti koji uključuju podatke klasificirane stupnjem tajnosti TRES SECRET UE/EU TOP SECRET (ili istovrijedni) **NE MOGU** se financirati,

— klasificirani podaci moraju se označiti u skladu s primjenjivim sigurnosnim uputama u pismu o sigurnosnim aspektima,

— za podatke stupnja tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili višeg stupnja tajnosti (i stupnja tajnosti RESTREINT UE/EU RESTRICTED ako se to zahtijeva nacionalnim propisima) vrijedi sljedeće:

  — mogu nastati ili im se pristupiti isključivo u prostorima za koje je nadležno nacionalno sigurnosno tijelo, u skladu s nacionalnim propisima, dalo sigurnosno odobrenje,

  — s njima se može postupati isključivo u sigurnosnoj zoni koju je akreditiralo nadležno nacionalno sigurnosno tijelo,

  — mogu im pristupati s njima postupati isključivo osobe s valjanim uvjerenjem o sigurnosnoj provjeri osobe za koje je utvrđena nužnost pristupa podacima,

— po isteku sporazuma o dodjeli bespovratnih sredstava klasificirani podaci moraju se vratiti ili ih se mora nastaviti štititi u skladu s primjenjivim pravilima,

— zadaće djelovanja koje uključuju klasificirane podatke EU-a mogu se podugovarati samo uz prethodno pisano odobrenje tijela koje dodjeljuje bespovratna sredstva i samo subjektima s poslovnim nastanom u državi članici ili sa sjedištem u trećoj zemlji koja je sklopila sporazum o sigurnosti podataka s EU-om (ili administrativni dogovor s Komisijom),

— otkrivanje klasificiranih podataka EU-a trećoj strani podliježe prethodnom pisanom odobrenju tijela koje dodjeljuje bespovratna sredstva.

Napominje se da, ovisno o vrsti djelatnosti, prije potpisivanja sporazuma o dodjeli bespovratnih sredstava može biti potrebno dostaviti sigurnosno odobrenje. Tijelo koje dodjeljuje bespovratna sredstva procijenit će potrebu za sigurnosnim odobrenjem u svakom pojedinom slučaju i tijekom pripreme dodjele bespovratnih sredstava odlučiti kada ih je potrebno dostaviti. Napominje se da **ni u kojem slučaju** nije moguće potpisati sporazum o dodjeli bespovratnih sredstava dok barem jedan od korisnika u konzorciju nema sigurnosno odobrenje.

Dodatne sigurnosne preporuke mogu se dodati sporazumu o dodjeli bespovratnih sredstava u obliku sigurnosnih rezultata (*npr. osnivanje savjetodavne skupine za sigurnost, ograničavanje razine detalja, upotreba lažnih scenarija, isključivanje upotrebe klasificiranih podataka itd.*).

Korisnici moraju osigurati da njihovi projekti ne podliježu nacionalnim sigurnosnim zahtjevima/sigurnosnim zahtjevima treće zemlje koji bi mogli utjecati na provedbu ili dovesti u pitanje dodjelu bespovratnih sredstava (*npr. tehnološka ograničenja, nacionalne oznake stupnjeva tajnosti itd.*). Tijelo koje dodjeljuje bespovratna sredstva mora se bez odgode obavijestiti o svim potencijalnim sigurnosnim problemima.

[Dodatna OPCIJA za okvirne sporazume o partnerstvu: za okvirne sporazume o partnerstvu može biti potrebno sigurnosnom pregledu podvrgnuti i zahtjeve za okvirne sporazume o partnerstvu i zahtjeve za dodjelu bespovratnih sredstava.]

([1]) Vidjeti Odluku Komisije (EU, Euratom) 2015/444 od 13. ožujka 2015. o sigurnosnim propisima za zaštitu klasificiranih podataka EU-a (SL L 72, 17.3.2015., str. 53.).

PRILOG II.

ODREDBE STANDARDNOG SPORAZUMA O DODJELI BESPOVRATNIH SREDSTAVA

(prilagoditi upotrijebljenom sporazumu o dodjeli bespovratnih sredstava)

13.2. Sigurnost – klasificirani podaci

Stranke moraju postupati s klasificiranim podacima (EU-a ili nacionalnim) u skladu s primjenjivim pravom EU-a ili nacionalnim pravom o klasificiranim podacima (posebno Odlukom Komisije (EU, Euratom) 2015/444 ([1]) i njezinim provedbenim pravilima).

Posebna sigurnosna pravila (ako postoje) navedena su u Prilogu 5.

PRILOG 5.

Sigurnost – klasificirani podaci EU-a

[OPCIJA za djelovanja s klasificiranim podacima EU-a (standardna): Ako se klasificirani podaci EU-a upotrebljavaju u djelovanju ili nastanu djelovanjem, moraju se obrađivati u skladu s vodičem za stupnjeve tajnosti (SCG) i pismom o sigurnosnim aspektima (SAL) navedenima u Prilogu 1. i Odluci (EU, Euratom) 2015/444 i njezinim provedbenim pravilima, dok se ne deklasificiraju.

Rezultati koji sadržavaju klasificirane podatke EU-a moraju se podnijeti u skladu s posebnim postupcima dogovorenima s tijelom koje dodjeljuje bespovratna sredstva.

Zadaće djelovanja koje uključuju klasificirane podatke EU-a mogu se podugovarati samo uz prethodno izričito pisano odobrenje tijela koje dodjeljuje bespovratna sredstva i samo subjektima s poslovnim nastanom u državi članici ili sa sjedištem u trećoj zemlji koja je sklopila sporazum o sigurnosti podataka s EU-om (ili administrativni dogovor s Komisijom).

Klasificirani podaci EU-a ne smiju se otkrivati trećim stranama (među ostalim sudionicima uključenima u provedbu djelovanja) bez prethodnog izričitog pisanog odobrenja tijela koje dodjeljuje bespovratna sredstva.]

([1]) Odluka Komisije (EU, Euratom) 2015/444 od 13. ožujka 2015. o sigurnosnim propisima za zaštitu klasificiranih podataka EU-a (SL L 72, 17.3.2015., str. 53.).

PRILOG III.

[Prilog IV. (……)]

PISMO O SIGURNOSNIM ASPEKTIMA (SAL) [1]

[model]

[1] Ovaj model pisma o sigurnosnim aspektima primjenjuje se ako se smatra da je Komisija autor klasificiranih podataka koji su nastali ili s kojima se postupa radi izvršenja sporazuma o dodjeli bespovratnih sredstava. Ako Komisija nije autor klasificiranih podataka koji nastanu ili s kojima se postupa radi izvršenja sporazuma o dodjeli bespovratnih sredstava i ako države članice koje sudjeluju u dodjeli bespovratnih sredstava uspostave poseban sigurnosni okvir, mogu se primjenjivati drugi modeli pisma o sigurnosnim aspektima.

Dodatak A

SIGURNOSNI ZAHTJEVI

Tijelo koje dodjeljuje bespovratna sredstva mora u pismo o sigurnosnim aspektima (SAL) uvrstiti sljedeće sigurnosne zahtjeve. Neke se odredbe možda ne primjenjuju na sporazum o dodjeli bespovratnih sredstava. One se nalaze u uglatim zagradama.

Popis odredbi nije iscrpan. Mogu se dodati dodatne odredbe ovisno o prirodi klasificiranih bespovratnih sredstava.

OPĆI UVJETI*[Napomena: primjenjuju se na sve klasificirane sporazume o dodjeli bespovratnih sredstava*]

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

2. Korisnici bespovratnih sredstava podliježu svim obvezama navedenima u Odluci Komisije (EU, Euratom) 2015/444 ([2]) (dalje u tekstu „CD 2015/444") i njezinim provedbenim pravilima ([3]). Ako korisnik bespovratnih sredstava ima poteškoća s primjenom primjenjivog pravnog okvira u državi članici, mora se obratiti sigurnosnom tijelu Komisije i nacionalom sigurnosnom tijelu (NST) ili zaduženom sigurnosnom tijelu (ZST).

3. Klasificirani podaci koji su stvoreni pri izvršenju sporazuma o dodjeli bespovratnih sredstava moraju se označiti kao klasificirani podaci EU-a stupnja tajnosti koji je utvrđen u vodiču za stupnjeve tajnosti (SCG) u Dodatku B tom pismu. Odstupanje od stupnja tajnosti propisanog SCG-om dopušteno je samo uz pisano odobrenje tijela koje dodjeljuje bespovratna sredstva.

4. Komisija, kao tijelo koje dodjeljuje bespovratna sredstva, ostvaruje prava koja pripadaju autoru bilo kojeg klasificiranog podatka EU-a koji je nastao i s kojim se postupa radi izvršenja klasificiranog sporazuma o dodjeli bespovratnih sredstava.

5. Korisnik ili podugovaratelj ne smije bez pisane suglasnosti tijela koje dodjeljuje bespovratna sredstva upotrebljavati podatke ni materijale koje je primio od tijela koje dodjeljuje bespovratna sredstva ili koji su nastali u ime tog tijela ni u koju svrhu osim za potrebe sporazuma o dodjeli bespovratnih sredstava.

6. Ako je za izvršenje sporazuma o dodjeli bespovratnih sredstava potrebno uvjerenje o sigurnosnoj provjeri pravne osobe (USPPO), korisnik od tijela koje dodjeljuje bespovratna sredstva mora zatražiti da nastavi sa zahtjevom za USPPO.

7. Korisnik mora ispitati sve povrede sigurnosti povezane s klasificiranim podacima EU-a te ih što prije prijaviti tijelu koje dodjeljuje bespovratna sredstva. Korisnik ili podugovaratelj svojem NST-u ili ZST-u te, ako je to u skladu s nacionalnim zakonima i propisima, sigurnosnom tijelu Komisije mora odmah prijaviti sve slučajeve u kojima se zna ili postoji razlog za sumnju da su klasificirani podaci EU-a koji su dostavljeni ili nastali u skladu sa sporazumom o dodjeli bespovratnih sredstava izgubljeni ili otkriveni neovlaštenim osobama.

([2]) Odluka Komisije (EU, Euratom) 2015/444 od 13. ožujka 2015. o sigurnosnim propisima za zaštitu klasificiranih podataka EU-a (SL L 72, 17.3.2015., str. 53.).

([3]) Tijelo koje dodjeljuje bespovratna sredstva treba umetnuti upućivanja nakon što se ta provedbena pravila donesu.

8. Nakon isteka sporazuma o dodjeli bespovratnih sredstava korisnik ili podugovaratelj mora tijelu koje dodjeljuje bespovratna sredstva čim prije vratiti sve klasificirane podatke EU-a koje posjeduje. Ako je izvedivo, korisnik ili podugovaratelj može uništiti klasificirane podatke EU-a umjesto da ih vrati. To se mora izvršiti u skladu s nacionalnim zakonima i propisima zemlje u kojoj je sjedište korisnika, 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.

9. Ako je korisnik ili podugovaratelj nakon raskida ili sklapanja sporazuma o dodjeli bespovratnih sredstava ovlašten zadržati klasificirane podatke EU-a, oni se moraju nastaviti štititi u skladu s Odlukom CD 2015/444 i njezinim provedbenim pravilima ([4]).

10. 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 uključuju, među ostalim, zahtjev da komunikacijski i informacijski sustavi koje korisnik posjeduje i koje koristi za postupanje s klasificiranim podacima EU-a za potrebe sporazuma o dodjeli bespovratnih sredstava(dalje u tekstu: „CIS korisnika”) moraju biti akreditirani ([5]), da elektroničko slanje klasificiranih podataka EU-a mora biti zaštićeno kriptografskim proizvodima odobrenima u skladu s člankom 36. stavkom 4. Odluke Vijeća 2015/444 i da se sigurnosne mjere TEMPEST moraju provoditi u skladu s člankom 36. stavkom 6. Odluke 2015/444.

11. Korisnik ili podugovaratelj dužan je imati krizni poslovni plan za zaštitu svih klasificiranih podataka EU-a s kojima se postupa pri izvršenju klasificiranog sporazuma o dodjeli bespovratnih sredstava 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. Korisnik ili podugovaratelj o svojem kriznom poslovnom planu mora obavijestiti tijelo koje dodjeljuje bespovratna sredstva.

SPORAZUMI O DODJELI BESPOVRATNIH SREDSTAVA ZA KOJE JE POTREBAN PRISTUP PODACIMA KLASIFICIRANIMA STUPNJEM TAJNOSTI RESTREINT UE/EU RESTRICTED

12. U načelu, uvjerenje o sigurnosnoj provjeri osobe (USP) nije potrebno za ispunjavanje sporazuma o dodjeli bespovratnih sredstava ([6]). Međutim, podaci ili materijal klasificirani stupnjem tajnosti RESTREINT UE/EU RESTRICTED moraju biti dostupni samo osoblju korisnika kojima su ti podaci potrebni za izvršenje sporazuma o dodjeli bespovratnih sredstava(*načelo nužnosti pristupa podacima*), koje je službenik za sigurnost korisnika 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.

13. Ako tijelo koje dodjeljuje bespovratna sredstva nije dalo pisanu suglasnost, korisnik 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.

14. Korisnik ili podugovaratelj mora zadržati oznake stupnja tajnosti klasificiranih podataka stvorenih ili dostavljenih tijekom izvršenja sporazuma o dodjeli bespovratnih sredstava i ne smije deklasificirati podatke bez pisane suglasnosti tijela koje dodjeljuje bespovratna sredstva.

15. Kada se ne koriste, podaci ili materijal klasificiran oznakom stupnja tajnosti RESTREINT UE/EU RESTRICTED moraju se čuvati u zaključanom uredskom ormariću. Kada se prenose, dokumente treba nositi u neprozirnoj omotnici. Dokumenti stalno moraju biti uz nositelja i ne smiju se putem otvarati.

([4]) Tijelo koje dodjeljuje bespovratna sredstva treba umetnuti upućivanja nakon što se ta provedbena pravila donesu.

([5]) Stranka koja provodi akreditaciju morat će tijelu koje dodjeljuje bespovratna sredstva preko sigurnosnog tijela Komisije i u suradnji s nadležnim tijelom za sigurnosnu akreditaciju (SAA) dostaviti izjavu o sukladnosti.

([6]) Ako su korisnici iz država članica u kojima se za bespovratna sredstva klasificirana oznakom tajnosti RESTREINT UE/EU RESTRICTED zahtijevaju USP-i i/ili USPPO-i, tijelo koje dodjeljuje bespovratna sredstva u SAL-u navodi zahtjeve tih USP-a ili USPPO-a za te korisnike.

16. Korisnik ili podugovaratelj može dokumente klasificirane oznakom tajnosti RESTREINT UE/EU RESTRICTED tijelu koje dodjeljuje bespovratna sredstva poslati komercijalnom kurirskom službom, poštanskom službom, ručnim prijenosom ili elektroničkim putem. Korisnik 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 bespovratnih sredstava ([7]).

17. 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.

18. Sigurnosna akreditacija CIS-a korisnika koji postupa s klasificiranim podacima EU-a stupnja tajnosti RESTREINT UE/EU RESTRICTED i svako njihovo međusobno povezivanje mogu se delegirati službeniku za sigurnost korisnika ako to dopuštaju nacionalni zakoni i propisi. U slučaju tako delegirane akreditacije, NST-i, ZST-i ili tijela za sigurnosnu akreditaciju (SAA) i dalje su odgovorni za zaštitu svih podataka stupnja tajnosti RESTREINT UE/EU RESTRICTED s kojima korisnik postupa te zadržavaju pravo na inspekciju sigurnosnih mjera koje je korisnik poduzeo. Osim toga, korisnik tijelu koje dodjeljuje bespovratna sredstva i, ako se to zahtijeva nacionalnim zakonima i propisima, nadležnom nacionalnom tijelu za sigurnosnu akreditaciju podnosi izjavu o sukladnosti kojom potvrđuje da su CIS korisnika 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)

19. Minimalni zahtjevi za komunikacijske i informacijske sustave koji postupaju s podacima klasificiranima stupnjem tajnosti RESTREINT UE/EU RESTRICTED utvrđeni su u Dodatku E tom pismu o sigurnosnim aspektima.

UVJETI POD KOJIMA KORISNIK MOŽE SKLAPATI PODUGOVORE

20. Korisnik mora prije podugovaranja bilo kojeg dijela klasificiranog sporazuma o dodjeli bespovratnih sredstava dobiti dopuštenje tijela koje dodjeljuje bespovratna sredstva.

21. Subjektu registriranom u trećoj zemlji ili subjektu koji pripada međunarodnoj organizaciji ne može se dati podugovor ako ta treća zemlja ili međunarodna organizacija nije sklopila sporazum o sigurnosti podataka s EU-om ili administrativni dogovor s Komisijom.

22. Ako je korisnik sklopio podugovor, sigurnosne odredbe sporazuma o dodjeli bespovratnih sredstava primjenjuju se *mutatis mutandis* na podugovaratelja (podugovaratelje) i njegovo (njihovo) osoblje. U tom je slučaju odgovornost korisnika osigurati da svi podugovaratelji ta načela primjenjuju na vlastite podugovore. Kako bi se osigurao primjeren nadzor sigurnosti, sigurnosno tijelo Komisije obavještava NST-e i/ili ZST-e korisnika i podugovaratelja o dodjeli svih povezanih klasificiranih podugovora stupnja tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET. Po potrebi se NST-ima i/ili ZST-ima korisnika i podugovaratelja dostavlja preslika sigurnosnih odredbi povezanih s konkretnim podugovorom. NST-i i ZST-i koji zahtijevaju obavijest o sigurnosnim odredbama klasificiranih sporazuma o dodjeli bespovratnih sredstava stupnja tajnosti RESTREINT UE/EU RESTRICTED navedeni su u prilogu Komisijinim provedbenim pravilima o gospodarskoj sigurnosti u pogledu klasificiranih sporazuma o dodjeli bespovratnih sredstava ([8]).

23. Korisnik ne smije podugovaratelju otkriti nijedan klasificirani podatak EU-a bez prethodnog pisanog odobrenja tijela koje dodjeljuje bespovratna sredstva. Ako se klasificirani podaci EU-a podugovarateljima šalju često ili rutinski, tada tijelo koje dodjeljuje bespovratna sredstva može dati svoje odobrenje na određeni rok (npr. 12 mjeseci) ili za razdoblje trajanja podugovora.

([7]) Tijelo koje dodjeljuje bespovratna sredstva treba umetnuti upućivanja nakon što se ta provedbena pravila donesu.
([8]) Tijelo koje dodjeljuje bespovratna sredstva treba umetnuti upućivanja nakon što se ta provedbena pravila donesu.

POSJETI

Ako se na posjete koji uključuju podatke klasificirane stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET primjenjuje standardni postupak zahtjeva za posjet, tijelo koje dodjeljuje bespovratna sredstva mora uvrstiti stavke 24., 25. i 26. te izbrisati stavak 27. Ako su posjeti koji uključuju podatke klasificirane stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET organizirani izravno između ustanova koje šalju i primaju posjetitelje, tijelo koje dodjeljuje bespovratna sredstva mora izbrisati stavke 25. i 26. i uvrstiti samo stavak 27.

24. Posjeti koji uključuju pristup ili potencijalni pristup podacima klasificiranima stupnjem tajnosti RESTREINT UE/EU RESTRICTED organiziraju se izravno između ustanova koje šalju i primaju posjetitelje, pri čemu nije potrebno slijediti postupak iz stavaka od 25. do 27. u nastavku.

[25. Posjeti koji uključuju pristup ili potencijalni pristup podacima klasificiranima stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET podliježu postupku u nastavku:

a) službenik za sigurnost objekta koji šalje posjetitelja ispunjava sve relevantne dijelove obrasca zahtjeva za posjet (Dodatak C) i podnosi zahtjev NST-u ili 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 prostorije tijela koje dodjeljuje bespovratna sredstva) podnese zahtjev za posjet;

c) službenik za sigurnost objekta koji šalje posjetitelja zatim od svojeg NST-a ili ZST-a dobiva odgovor NST-a ili 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 dana posjeta nije uložen prigovor.]

[26. 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 ili ZST-a.]

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

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

29. Objekt koji prima posjetitelja mora osigurati da se vodi evidencija svih posjetitelja. Evidencija mora sadržavati njihova imena, organizacije koje zastupaju, 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 nacionalnim zakonima i propisima.

POSJETI RADI PROCJENE STANJA

30. Sigurnosno tijelo Komisije može u suradnji s nadležnim NST-om ili ZST-om provoditi posjete objektima korisnika ili podugovaratelja radi provjere toga poštuju li se sigurnosni zahtjevi za postupanje s klasificiranim podacima EU-a.

VODIČ ZA STUPNJEVE TAJNOSTI

31. Popis svih elemenata sporazuma o dodjeli bespovratnih sredstava koji su klasificirani ili će biti klasificirani tijekom izvršenja sporazuma o dodjeli bespovratnih sredstava, pravila klasifikacije i specifikacija primjenjivih stupnjeva tajnosti nalaze se u vodiču za stupnjeve tajnosti (SCG). SCG je sastavni dio ovog sporazuma o dodjeli bespovratnih sredstava i nalazi se u Dodatku B ovom Prilogu.

Dodatak B

VODIČ ZA STUPNJEVE TAJNOSTI

[poseban tekst koji treba prilagoditi predmetu sporazuma o dodjeli bespovratnih sredstava]

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 navedite 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 (prema potrebi), broj telefona i e-adresu. Navedite ime i broj telefona/telefaksa te e-adresu glavne točke za kontakt ili osobe s kojom ste dogovorili posjet. Napomene: 1. Važno je navesti točan poštanski broj jer poduzeće može imati više različitih objekata. 2. Pri ručnom ispunjavanju zahtjeva Prilog 1. može se koristiti ako je potrebno posjetiti dva ili više objekta u vezi s istim predmetom. Ako se koristi Prilog u stavci 3. treba 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 uključuje više od dva posjetitelja, potrebno je koristiti Prilog 2.
13. **THE SECURITY OFFICER OF THE REQUESTING ENTITY**	U ovoj stavci potrebno je navesti ime, broj telefona, broj telefaksa i e-adresu 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-adresu (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-adresu (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 ([9]).

REQUEST FOR VISIT

(MODEL)

TO: _____

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

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

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

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

NAME:

POSTAL ADDRESS:

E-MAIL ADDRESS:

FAX NO: TELEPHONE NO:

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

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

8. **TYPE OF INITIATIVE:**

☐ Initiated by requesting organisation or facility

☐ By invitation of the facility to be visited

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

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

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

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

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

NAME:

TELEPHONE NO:

E-MAIL ADDRESS:

SIGNATURE:

14. CERTIFICATION OF SECURITY CLEARANCE LEVEL:

NAME:

ADDRESS:

TELEPHONE NO:

E-MAIL ADDRESS:

SIGNATURE:

STAMP

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

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

NAME:

ADDRESS:

TELEPHONE NO:

E-MAIL ADDRESS:

STAMP

SIGNATURE:

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

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

<Mjesto za upućivanje na primjenjivo zakonodavstvo o osobnim podacima i poveznica na obvezne informacije za ispitanika, npr. kako se provodi članak 13. Opće uredbe o zaštiti podataka ([10]).>

([10]) 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(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)***

<Mjesto za upućivanje na primjenjivo zakonodavstvo o osobnim podacima i poveznica na obvezne informacije za ispitanika, npr. kako se provodi članak 13. Opće uredbe o zaštiti podataka ([11]).>

([11]) 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 ispitanika, npr. kako se provodi članak 13. Opće uredbe o zaštiti podataka ([12]).>

([12]) 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 (MODEL)

1. **UVOD**

1.1. Primjer informativnog obrasca o uvjerenju o sigurnosnoj provjeri pravne osobe priložen je radi brze razmjene informacija između nacionalnog sigurnosnog tijela (NST) ili zaduženog sigurnosnog tijela (ZST), ostalih nadležnih nacionalnih sigurnosnih tijela i sigurnosnog tijela Komisije (koje djeluju u ime tijela koja dodjeljuju bespovratna sredstva) u pogledu uvjerenja o sigurnosnoj provjeri pravne osobe (USPPO) objekta uključenog u prijave za klasificirana bespovratna sredstva ili podugovore ili njihovo izvršenje.

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-ima/ZST-ima/Komisiji e-poštom.

1.5. NST-i/ZST-i trebali bi nastojati 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 ili podugovor o bespovratnim sredstvima, NST ili ZST koji daje odgovor o tome mora biti obaviješten.

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

Ove detaljne upute vrijede za NST ili ZST ili tijelo koje dodjeljuje bespovratna sredstva i sigurnosno tijelo Komisije, koji ispunjavaju informativni obrazac o uvjerenju o sigurnosnoj provjeri pravne osobe. Zahtjev bi trebalo ispuniti velikim tiskanim slovima.

ZAGLAVLJE	Podnositelj zahtjeva unosi puni naziv NST-a/ZST-a i naziv zemlje.
1. **VRSTA ZAHTJEVA**	Tijelo koje dodjeljuje bespovratna sredstva koje 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 kratice u nastavku: 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**	Za polja od 1. do 6. nisu potrebni posebni razlozi. U polju 4. treba koristiti standardnu dvoslovnu oznaku zemlje. Polje 5. nije obavezno.
3. **RAZLOG ZA ZAHTJEV**	Navedite konkretan razlog za zahtjev, pokazatelje projekta, broj poziva ili dodjele bespovratnih sredstava. Navedite potrebe za pohranu podataka, stupanj tajnosti CIS-a itd. Trebalo bi uvrstiti sve rokove/datume isteka/datume dodjele kojima bi se moglo 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 korisnik ili podugovaratelj odgovoran je za podnošenje zahtjeva za produljenje USPPO-a.
6. **NAPOMENE**	Ovdje se mogu navesti dodatne informacije o USPPO-u, objekua ili prethodno navedenim stavkama.
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 (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 korisnika 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 objekta navedenog u nastavku 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 sporazuma (odabir prijedloga), sporazumu o dodjeli bespovratnih sredstava ili podugovoru, programu/projektu itd.)

.....

NST/ZST/tijelo koje dodjeljuje bespovratna sredstva koje podnosi zahtjev: Ime: .....

Datum: (dd/mm/gggg) .....

ODGOVOR (u roku od deset radnih dana)

Potvrđuje se da:

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

   [ ] C-UE/EU-C.

2. Prethodno navedeni objekt ima kapacitete za zaštitu klasificiranih podataka/materijala:

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

3. Prethodno navedeni objekt ima akreditirani/ovlašteni CIS:

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

4. [ ] u vezi s prethodno navedenim zahtjevom, pokrenut je postupak za USPPO. Obavijestit ćemo vas kad USPPO bude izdan ili odbijen.

5. [ ] prethodno navedeni objekt nema USPPO.

6. Ova potvrda o USPPO-u prestaje važiti: ..... (*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 ispitanika, npr. kako se provodi članak 13. Opće uredbe o zaštiti podataka ([13]).>

([13]) 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 korisnika

Općenito

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

2. Korisnik je odgovoran za primjenu sigurnosnih zahtjeva utvrđenih 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, među ostalim radne stanice, pisače, kopirne uređaje, telefaks uređaje, poslužitelje, sustave za upravljanje mrežom, upravljače mrežom i upravljače komunikacijom, prijenosna računala, *notebook*računala, tablete, pametne telefone i prijenosne uređaje za pohranu podataka kao što su USB-i, CD-i, kartice SD itd.

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

5. Korisnici 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 predmetni objekt.

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

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

8. Samo se s podacima klasificiranima stupnjem tajnosti RESTREINT UE/EU RESTRICTED koji su kodirani odobrenim kriptografskim proizvodima može postupati, odnosno može ih se čuvati ili slati (žično ili bežično) kao s bilo kojim drugim neklasificiranim podacima u okviru sporazuma o dodjeli bespovratnih sredstava. Te kriptografske proizvode mora odobriti EU ili država članica.

9. Vanjski subjekti koji sudjeluju u radovima održavanja/popravka moraju se ugovorno obvezati da će postupati u skladu s primjenjivim odredbama za postupanje s podacima klasificiranima stupnjem tajnosti RESTREINT UE/EU RESTRICTED, kako je utvrđeno u ovom dokumentu.

10. Na zahtjev tijela koje dodjeljuje bespovratna sredstva ili nadležnog NST-a, ZST-a ili SAA-a korisnik mora dostaviti dokaz o poštovanju odredbe o sigurnosti sporazuma o dodjeli bespovratnih sredstava. Ako je za osiguranje poštovanja tih zahtjeva ujedno potrebno provesti reviziju i inspekciju postupaka i objekata korisnika, korisnici predstavnicima javnog naručitelja, NST-a, ZST-a i/ili SAA-a ili relevantnog sigurnosnog tijela EU-a, dopuštaju provođenje takve revizije i inspekcije.

Fizička sigurnost

11. Zone u 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 trebale bi biti odvojene i kontrolirane zone s primjerenim sustavom za kontrolu pristupa. Pristup tim odvojenim i kontroliranim zonama mora se ograničiti na osobe s posebnim odobrenjem. Ne dovodeći u pitanje stavak 8., oprema opisana u stavku 3. mora se čuvati u takvim odvojenim i kontroliranim zonama.

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-i, uređaji za masovnu pohranu ili CD-RW-i) s komponentama CIS-a.

Pristup komunikacijskom i informacijskom sustavu (CIS)

13. Pristup CIS-u korisnika 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 autentifikaciju.

15. Lozinke, koje su dio većine sigurnosnih mjera identifikacije i autentifikacije, moraju se sastojati od najmanje devet znakova i sadržavati numeričke znakove te „posebne" znakove (ako sustav to dopušta) i abecedne znakove. Lozinke se moraju mijenjati najmanje svakih 180 dana. Moraju se promijeniti čim 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 sustav i sigurnosne kontrole. Odjava korisnika iz CIS-a mora biti 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 barem pet uzastopnih pokušaja prijave 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. Sigurnosno-operativni postupci moraju biti dostupni korisnicima i administratorima te sadržavati opis sigurnosnih uloga i povezani popis zadaća, uputa i planova.

Evidencija, revizija i odgovori na incidente

20. Svaki pristup CIS-u treba zabilježiti.

21. Moraju se evidentirati sljedeći događaji:

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

    b) odjave (među ostalim 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 mora se 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 koristiti i za potporu sudskim istragama u slučaju sigurnosnog incidenta. Sve evidencije o sigurnosti treba bi redovito provjeravati kako bi se utvrdili potencijalni sigurnosni incidenti. Zapisi iz evidencije moraju biti zaštićeni od neovlaštenog brisanja ili izmjene.

24. Korisnik 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 tijelu koje dodjeljuje bespovratna sredstva 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 njega.

Umrežavanje i međusobno povezivanje

26. Ako je CIS korisnika 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 korisnika ili podugovaratelja. U tom slučaju korisnik mora provesti procjenu rizika kako bi utvrdio dodatne sigurnosne zahtjeve koje treba provesti u okviru postupka sigurnosne akreditacije. Korisnik tijelu koje dodjeljuje bespovratna sredstva 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 tijelo koje dodjeljuje bespovratna sredstva provelo i dogovorilo 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 (među ostalim dijagrami sustava i mreže), mora biti dostupna i redovito se održavati.

29. Službenik za sigurnost korisnika mora provesti provjere konfiguracije na hardveru i softveru kako bi se osiguralo da nije ugrađen neovlašteni hardver ili softver.

30. Potrebno je procijeniti kako promjene u konfiguraciji CIS-a korisnika 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 svaka tri mjeseca provjeriti sadržava li sustav sigurnosne slabe točke. 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. Korisnik mora izraditi plan kontinuiteta poslovanja. Potrebno je utvrditi postupke za sigurnosno kopiranje koji bi obuhvaćali:

    a) učestalost sigurnosnog kopiranja;

    b) zahtjeve 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 čitavog sustava ili medija za pohranu:

    a) izbrisiva memorija (npr. USB-i, kartice SD, SSD diskovi, hibridni tvrdi diskovi) mora se prebrisati najmanje tri puta i zatim provjeriti da se izvorni sadržaj ne može vratiti ili se mora izbrisati korištenjem odobrenog softvera za brisanje;

    b) magnetski mediji (npr. tvrdi diskovi) moraju se prebrisati ili demagnetizirati;

    c) optički mediji (npr. CD-i, DVD-i) moraju se trajno uništiti ili dezintegrirati;

    d) za sve ostale medije za pohranu potrebno je savjetovati se s tijelom koje dodjeljuje bespovratna sredstva ili, po potrebi, NST-om, ZST-om ili 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 korisnike ili podugovaratelje koja uključuju podatke stupnja tajnosti RESTREINT UE/EU RESTRICTED i NST-i/ZST-i koji zahtijevaju obavijest o klasificiranim sporazumima o dodjeli bespovratnih sredstava stupnja tajnosti RESTREINT UE/EU RESTRICTED ([1])

Država članica	USPPO		Obavijest NST-u i/ili ZST-u o sporazumu o dodjeli bespovratnih sredstava ili podugovoru koji uključuje 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**
Litva	**X**		**X**			**X**
Luksemburg	**X**		**X**		**X**	
Mađarska		**X**		**X**		**X**
Malta		**X**		**X**		**X**
Nizozemska	**X** (samo za sporazume o dodjeli bespovratnih sredstava i podugovore koji se odnose na obranu)		**X** (samo za sporazume o dodjeli bespovratnih sredstava i podugovore koji se odnose na obranu)			**X**
Austrija		**X**		**X**		**X**
Poljska		**X**		**X**		**X**

([1]) Tim se nacionalnim zahtjevima za USPPO/USP i obavijestima o sporazumima o dodjeli bespovratnih sredstava koji uključuju podatke stupnja tajnosti RESTREINT UE/EU RESTRICTED ne smiju određivati dodatne obveze ostalim državama članicama ili korisnicima ili podugovarateljima u njihovoj nadležnosti.
Napomena: obavezno je dostaviti obavijest o sporazumima o dodjeli bespovratnih sredstava koji uključuju podatke stupnja tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET.

Portugal		**X**		**X**		**X**
Rumunjska		**X**		**X**		**X**
Slovenija	**X**		**X**			**X**
Slovačka	**X**		**X**			**X**
Finska		**X**		**X**		**X**
Švedska		**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 Sofija
   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 Sofija
   Tel. +359 29227002
   Faks +359 29885211
   E-pošta: office@iksbg.org

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

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

(Navedena nadležna tijela provode postupke provjere za izdavanje USPPO-a pravnim subjektima koji se prijavljuju za sklapanje klasificiranog sporazuma, kao i za izdavanje USP-a pojedincima koji provode klasificirani sporazum za potrebe tih tijela.)

5. State Agency National Security (security service)

   45 Cherni Vrah Blvd.
   1407 Sofija

   Tel. +359 28147109

   Faks +359 29632188, +359 28147441

   E-pošta: dans@dans.bg

(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 klasificiranog sporazuma o dodjeli bespovratnih sredstava ili provode klasificirani ugovor ili klasificirani ugovor o bespovratnim sredstvima.)

ČEŠKA

National Security Authority
Industrial Security Department
PO BOX 49
150 06 Prag 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 Kopenhagen Ø

   Tel. +45 33325566

   Faks +45 33931320

NJEMAČKA

1. Za pitanja o politici gospodarske sigurnosti, USPPO-ima, planovima prijevoza (osim za kriptomaterijal/CCI):
   Federal Ministry for Economic Affairs and Energy
   Industrial Security Division – RS3
   Villemombler Str. 76
   53123 Bonn

   Tel. +49 228996154028

   Faks +49 228996152676

   E-pošta: dsagermany-rs3@bmwi.bund.de (e-pošta ureda)

2. Za standardne zahtjeve za posjet njemačkih poduzeća/njemačkim poduzećima:

Federal Ministry for Economic Affairs and Energy

Industrial Security Division – RS2
Villemombler Str. 76
53123 Bonn

Tel. +49 228996152401

Faks +49 228996152603

E-pošta: rs2-international@bmwi.bund.de (e-pošta 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, Atena

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 912832583, +34 912832752, +34 913725928

Faks +34 913725808

E-pošta: nsa-sp@areatec.com

Za informacije o klasificiranim programima: programas.ons@areatec.com

Za pitanja o uvjerenju o sigurnosnoj provjeri osobe: hps.ons@areatec.com

Za planove prijevoza i međunarodne posjete: sp-ivtco@areatec.com

FRANCUSKA

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
10 000 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.lv, ndi@zd.gov.lv

LITVA

Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija
(The Commission for Secrets Protection Coordination of the Republic of Lithuania)
National Security Authority
Pilaitės pr. 19
LT-06264 Vilnius

Tel. +370 70666128

E-pošta: nsa@vsd.lt

LUKSEMBURG

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

Tel. +352 24782210

E-pošta: ans@me.etat.lu

MAĐARSKA

National Security Authority of Hungary
H-1399 Budimpešta P.O. Box 710/50
H-1024 Budimpešta, 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 Hag

   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 Hag

   Tel. +31 704419407

   Faks +31 703459189

   E-pošta: indussec@mindef.nl

AUSTRIJA

1. Federal Chancellery of Austria

   Department I/10, Federal Office for Information Security

   Ballhausplatz 2
   10104 Beč

   Tel. +43 153115202594

   E-pošta: isk@bka.gv.at

2. ZST u vojnom području:
   BMLV/Abwehramt

   Postfach 2000
   1030 Beč

   E-pošta: abwa@bmlvs.gv.at

POLJSKA

Internal Security Agency
Department for the Protection of Classified Information
Rakowiecka 2A
00-993 Varšava

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 Lisabon

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 Bukurešt

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