SKLEP KOMISIJE (EU, Euratom) 2021/259

z dne 10. februarja 2021

o določitvi izvedbenih pravil za industrijsko varnost v zvezi s tajnimi donacijami

EVROPSKA KOMISIJA JE –

ob upoštevanju Pogodbe o delovanju Evropske unije in zlasti člena 249 Pogodbe,

ob upoštevanju Pogodbe o ustanovitvi Evropske skupnosti za atomsko energijo in zlasti člena 106 Pogodbe,

ob upoštevanju Uredbe (EU, Euratom) 2018/1046 Evropskega parlamenta in Sveta z dne 18. julija 2018 o finančnih pravilih, ki se uporabljajo za splošni proračun Unije, spremembi uredb (EU) št. 1296/2013, (EU) št. 1301/2013, (EU) št. 1303/2013, (EU) št. 1304/2013, (EU) št. 1309/2013, (EU) št. 1316/2013, (EU) št. 223/2014, (EU) št. 283/2014 in Sklepa št. 541/2014/EU ter razveljavitvi Uredbe (EU, Euratom) št. 966/2012 ([1]),

ob upoštevanju Sklepa Komisije (EU, Euratom) 2015/443 z dne 13. marca 2015 o varnosti v Komisiji ([2]),

ob upoštevanju Sklepa Komisije (EU, Euratom) 2015/444 z dne 13. marca 2015 o varnostnih predpisih za varovanje tajnih podatkov EU ([3]),

ob upoštevanju Sklepa Komisije (EU, Euratom) 2017/46 z dne 10. januarja 2017 o varnosti komunikacijskih in informacijskih sistemov v Evropski komisiji ([4]),

po posvetovanju s strokovno skupino Komisije za varnost v skladu s členom 41(5) Sklepa (EU, Euratom) 2015/444,

ob upoštevanju naslednjega:

(1) Členi 41, 42, 47 in 48 Sklepa (EU, Euratom) 2015/444 določajo, da je treba v izvedbenih pravilih za industrijsko varnost določiti podrobnejše določbe za dopolnitev in podporo poglavja 6 navedenega sklepa, ki ureja vprašanja, kot so tajni sporazumi o donacijah, varnostna dovoljenja organizacij, dovoljenja za dostop do tajnih podatkov, obiski ter razpošiljanje in prenašanje tajnih podatkov Evropske unije.

(2) Sklep (EU, Euratom) 2015/444 določa, da se tajni sporazumi o donacijah izvajajo v tesnem sodelovanju z nacionalnim varnostnim organom, imenovanim varnostnim organom ali katerim koli drugim pristojnim organom zadevnih držav članic. Države članice so se dogovorile, da bodo zagotovile, da je vsak subjekt pod njihovo jurisdikcijo, ki lahko prejema ali ustvarja tajne podatke, ki izvirajo od Komisije, ustrezno varnostno preverjen in je zmožen zagotavljati ustrezno raven varovanja, enakovredno ravni, ki jo zagotavljajo varnostni predpisi Sveta Evropske unije za varovanje tajnih podatkov EU z ustrezno oznako stopnje tajnosti, kot je določeno v Sporazumu med državami članicami Evropske unije, ki so se sestale v okviru Sveta, o varovanju tajnih podatkov, ki se izmenjujejo v interesu Evropske unije (2011/C 202/05) ([5]).

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

(3) Svet, Komisija in visoki predstavnik Unije za zunanje zadeve in varnostno politiko so se dogovorili, da bodo zagotovili kar največjo doslednost pri uporabi varnostnih predpisov v zvezi z varovanjem tajnih podatkov EU, pri tem pa upoštevali svoje posebne institucionalne in organizacijske potrebe v skladu z izjavami, priloženimi k zapisniku seje Sveta, na kateri je bil sprejet Sklep Sveta 2013/488/EU ([6]) o varnostnih predpisih za varovanje tajnih podatkov EU.

(4) Izvedbena pravila Komisije za industrijsko varnost, kar zadeva tajne donacije, bi morala zato prav tako zagotoviti največjo možno doslednost in upoštevati Smernice za industrijsko varnost, ki jih je 13. decembra 2016 odobril Varnostni odbor Sveta.

(5) Komisija je 4. maja 2016 sprejela sklep ([7]), ki člana Komisije, pristojnega za varnostne zadeve, pooblašča, da v imenu Komisije in na njeno odgovornost sprejme izvedbena pravila iz člena 60 Sklepa (EU, Euratom) 2015/444 –

SPREJELA NASLEDNJI SKLEP:

POGLAVJE 1

SPLOŠNE DOLOČBE

Člen 1

Predmet urejanja in področje uporabe

1. Ta sklep določa izvedbena pravila za industrijsko varnost v zvezi s tajnimi donacijami v smislu Sklepa (EU, Euratom) 2015/444 in zlasti poglavja 6 navedenega sklepa.

2. Ta sklep določa posebne zahteve za zagotovitev varstva tajnih podatkov EU pri objavi razpisov, dodelitvi donacij in izvajanju tajnih sporazumov o donacijah, ki jih sklene Evropska komisija.

3. Ta sklep se uporablja za donacije, pri katerih gre za tajne podatke naslednjih stopenj tajnosti:

(a) RESTREINT UE/EU RESTRICTED;

(b) CONFIDENTIEL UE/EU CONFIDENTIAL;

(c) SECRET UE/EU SECRET.

4. Uporaba tega sklepa ne posega v posebna pravila, določena v drugih pravnih aktih, kot so tisti v zvezi z evropskim programom za razvoj obrambne industrije.

Člen 2

Pristojnosti znotraj Komisije

1. Odredbodajalec organa, ki dodeljuje donacije, iz Uredbe (EU, Euratom) 2018/1046 Evropskega parlamenta in Sveta v okviru svojih pristojnosti zagotovi, da je tajna donacija skladna s Sklepom (EU, Euratom) 2015/444 in njegovimi izvedbenimi pravili.

([6]) Sklep Sveta 2013/488/EU z dne 23. septembra 2013 o varnostnih predpisih za varovanje tajnih podatkov EU (UL L 274, 15.10.2013, str. 1).

([7]) Sklep Komisije z dne 4. maja 2016 o pooblastitvi v zvezi z varnostjo [C(2016) 2797 final].

2. V ta namen se zadevni odredbodajalec v vseh fazah posvetuje z varnostnim organom Komisije glede vprašanj v zvezi z varnostnimi elementi tajnega sporazuma o donaciji, programa ali projekta in obvesti lokalnega uradnika za varnost o podpisanih tajnih sporazumih o donacijah. Odločitev o stopnji tajnosti posameznih vsebin sprejme organ, ki dodeli donacijo, pri čemer ustrezno upošteva Vodič po stopnjah tajnosti.

3. Če se uporabljajo varnostna navodila za program ali projekt iz člena 5(3), organ, ki dodeli donacijo, in Varnostni organ Komisije izpolnita dolžnosti, ki so jima naložene v navedenih navodilih.

4. Ob upoštevanju zahtev teh izvedbenih pravil Varnostni organ Komisije tesno sodeluje z nacionalnimi varnostnimi organi in imenovanimi varnostnimi organi zadevnih držav članic, zlasti glede varnostnih dovoljenj organizacij in dovoljenj za dostop do tajnih podatkov, postopkov za obiske in načrtov prevoza.

5. Če donacije upravljajo izvajalske agencije EU ali drugi organi financiranja in se ne uporabljajo posebna pravila iz drugih pravnih aktov iz člena 1(4):

(a) služba Evropske komisije, ki prenese pooblastila, uveljavlja pravice, ki jih ima tvorec tajnih podatkov EU, ustvarjenih v zvezi z donacijami, če je tako določeno v dogovoru o prenosu pooblastil;

(b) je služba Evropske komisije, ki prenese pooblastila, odgovorna za določitev stopnje tajnosti;

(c) se zahteve za varnostno dovoljenje in obvestila nacionalnih varnostnih organov in/ali imenovanih varnostnih organov pošljejo preko Varnostnega organa Komisije.

POGLAVJE 2

OBRAVNAVANJE RAZPISOV ZA TAJNE SPORAZUME O DONACIJI

Člen 3

Osnovna načela

1. Tajne dele donacij izvajajo samo upravičenci, ki so registrirani v državi članici, ali upravičenci, ki so registrirani v tretji državi ali ki jih ustanovi mednarodna organizacija, če je ta tretja država ali mednarodna organizacija sklenila sporazum o varovanju tajnosti podatkov z Unijo ali sklenila upravni dogovor s Komisijo ([8]).

2. Pred objavo razpisa za tajni sporazum o donaciji organ, ki dodeli donacijo, določi stopnjo tajnosti vseh podatkov, ki bi se lahko sporočili prosilcem. Organ, ki dodeli donacijo, določi tudi najvišjo stopnjo tajnosti vseh podatkov, ki se uporabljajo ali nastanejo pri izvajanju sporazuma o donaciji ali programa ali projekta, ali vsaj pričakovani obseg in vrsto podatkov, ki jih je treba predložiti ali obravnavati, ter potrebo po tajnem komunikacijskem in informacijskem sistemu.

3. Organ, ki dodeli donacijo, zagotovi, da razpisi za tajne donacije vsebujejo informacije o posebnih varnostnih obveznostih, povezanih s tajnimi podatki. Razpisna dokumentacija zajema pojasnila o časovnem razporedu, v katerem upravičenci pridobijo varnostno dovoljenje organizacije, če se zahteva. Vzorčne predloge za informacije v zvezi z razpisnimi pogoji so v Prilogi I in Prilogi II.

([8]) Seznam sporazumov, ki jih je sklenila EU, in upravnih dogovorov, ki jih je sklenila Evropska komisija, v skladu s katerimi se lahko tajni podatki EU izmenjujejo s tretjimi državami in mednarodnimi organizacijami, je na voljo na spletišču Komisije.

4. Organ, ki dodeli donacijo, zagotovi, da se tajni podatki stopnje tajnosti RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL in SECRET UE/EU SECRET razkrijejo prosilcem šele po tem, ko so podpisali sporazum o nerazkrivanju podatkov, ki prosilce obvezuje, da tajne podatke EU obravnavajo in jih varujejo v skladu s Sklepom (EU, Euratom) 2015/444, njegovimi izvedbenimi pravili in veljavnimi nacionalnimi pravili.

5. Kadar se podatki stopnje tajnosti RESTREINT UE/EU RESTRICTED dajo na razpolago prosilcem, se minimalne zahteve iz člena 5(7) tega sklepa vključijo v razpis ali dogovore o nerazkrivanju informacij, sklenjene v fazi predloga.

6. Vsi prosilci in upravičenci, ki morajo obravnavati podatke stopnje tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ali SECRET UE/EU SECRET ali tovrstne podatke hraniti v svojih prostorih bodisi v fazi predloga bodisi med izvajanjem tajnega sporazuma o donaciji, morajo imeti varnostno dovoljenje organizacije za zahtevano stopnjo, razen v primerih iz odstavka 9. V nadaljevanju so navedeni trije možni scenariji, do katerih lahko pride v fazi predloga za tajni sporazum o donaciji, ki vključuje tajne podatke EU stopnje tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ali SECRET UE/EU SECRET:

(a) brez dostopa do tajnih podatkov EU stopnje tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ali SECRET UE/EU SECRET v fazi predloga:

kadar se razpis nanaša na donacijo, ki bo vključevala tajne podatke EU stopnje tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ali SECRET UE/EU SECRET, vendar od prosilca ne zahteva, da take informacije obravnava v fazi predloga, se prosilec, ki nima varnostnega dovoljenja organizacije za zahtevano stopnjo, ne izključi iz postopka vlaganja prošnje iz razloga, da nima tovrstnega dovoljenja;

(b) dostop do tajnih podatkov EU stopnje tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ali SECRET UE/EU SECRET v prostorih organa. ki dodeljuje donacijo, v fazi predloga:

dostop se odobri osebju prosilca, ki ima dovoljenje za dostop do tajnih podatkov za zahtevano stopnjo in za katero velja potreba po seznanitvi;

(c) obravnavanje tajnih podatkov EU stopnje tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ali SECRET UE/EU SECRET ali njihovo shranjevanje v prostorih prosilca v fazi predloga:

kadar se v razpisu od prosilcev zahteva obravnavanje tajnih podatkov EU ali shranjevanje tovrstnih podatkov v njihovih prostorih, mora imeti prosilec varnostno dovoljenje organizacije za zahtevano stopnjo. V takih okoliščinah organ, ki dodeli donacijo, preden se prosilcu dajo na razpolago tajni podatki EU, preko varnostnega organa Komisije pridobi zagotovilo zadevnega nacionalnega varnostnega organa ali imenovanega varnostnega organa, da je bilo prosilcu podeljeno ustrezno varnostno dovoljenje organizacije. Dostop se odobri osebju prosilca, ki ima dovoljenje za dostop do tajnih podatkov za zahtevano stopnjo in za katero velja potreba po seznanitvi;

7. Za dostop do podatkov stopnje tajnosti RESTREINT UE/EU RESTRICTED se niti v fazi predloga niti za izvajanje sporazuma o donaciji načeloma ne zahteva varnostno dovoljenje organizacije ali dovoljenje za dostop do tajnih podatkov. Kadar države članice po nacionalnih zakonih in predpisih, kot so navedeni v Prilogi IV, za sporazume o donacijah oziroma podizvajalske pogodbe na stopnji tajnosti RESTREINT UE/EU RESTRICTED zahtevajo varnostno dovoljenje organizacije ali dovoljenje za dostop do tajnih podatkov, te nacionalne zahteve ne nalagajo nobenih dodatnih obveznosti drugim državam članicam, niti iz povezanih sporazumov o donacijah ali podizvajalskih pogodb ali razpisov za take pogodbe ne izključujejo prosilcev, upravičencev oziroma podizvajalcev iz držav članic, ki za dostop do podatkov stopnje tajnosti RESTREINT UE/EU RESTRICTED varnostnega dovoljenja organizacije ne zahtevajo. Ti sporazumi o donacijah se izvajajo v državah članicah v skladu z njihovimi nacionalnimi zakoni in predpisi.

8. Kadar se za upravljanje razpisa in izvajanje tajnega sporazuma o donacijah zahteva varnostno dovoljenje organizacije, organ, ki dodeli donacijo, preko Varnostnega organa Komisije predloži zahtevo nacionalnemu varnostnemu organu ali imenovanemu varnostnemu organu upravičenca z uporabo informacijskega lista za varnostno dovoljenje organizacije (FSCIS) ali kakšnega drugega uveljavljenega enakovrednega elektronskega obrazca. Vzorec informacijskega lista za varnostno dovoljenje organizacije je v Dodatku D Priloge III ([9]). Odgovor na informacijski list za varnostno dovoljenje organizacije se, kolikor je mogoče, zagotovi v desetih delovnih dneh od datuma zahtevka.

9. Kadar pri tajnih donacijah, za katere je potrebno varnostno dovoljenje organizacije, sodelujejo ustanove vlad držav članic ali ustanove pod nadzorom njihove vlade, za katere se po nacionalni zakonodaji ne izdajajo varnostna dovoljenja organizacije, organ, ki dodeljuje donacije, preko Varnostnega organa Komisije pri zadevnem nacionalnem varnostnemu organu ali imenovanem varnostnemu organu preveri, ali so te vladne ustanove sposobne obravnavati tajne podatke EU na zahtevani stopnji tajnosti.

([9]) Drugi uporabljeni obrazci se lahko po zasnovi razlikujejo od vzorca iz teh izvedbenih pravil.

10. Kadar se za izvajanje tajnega sporazuma o donacijah zahteva dovoljenje za dostop do tajnih podatkov, po nacionalnih pravilih pa je pred podelitvijo dovoljenja za dostop do tajnih podatkov potrebno varnostno dovoljenje organizacije, organ, ki dodeljuje donacije, preko Varnostnega organa Komisije z uporabo informacijskega lista za varnostno dovoljenje organizacije pri nacionalnem varnostnemu organu ali imenovanem varnostnemu organu upravičenca preveri, ali ima upravičenec varnostno dovoljenje organizacije oziroma ali je postopek za izdajo varnostnega dovoljenja organizacije v teku. Komisija v tem primeru za izdajo zahtevkov za dovoljenje za dostop do tajnih podatkov ne uporabi informacijskega lista za dovoljenje za dostop do tajnih podatkov (PSCIS).

Člen 4

Oddaja v podizvajanje pri tajnih sporazumih o donacijah

1. Pogoji, pod katerimi lahko upravičenci oddajo v podizvajanje opravljanje nalog, ki vključujejo tajne podatke EU, se opredelijo v razpisu in sporazumu o donaciji. Med temi pogoji mora biti tudi zahteva, da se vsi informacijski listi za varnostno dovoljenje organizacije vložijo preko Varnostnega organa Komisije. Za oddajo v podizvajanje je potrebno predhodno pisno dovoljenje organa, ki dodeljuje donacije. Če je ustrezno, mora biti oddaja v podizvajanje skladna z osnovnim aktom o vzpostavitvi programa.

2. Tajni deli donacij se dajo v podizvajanje samo subjektom, ki so registrirani v državi članici, ali subjektom, ki so registrirani v tretji državi ali ki jih ustanovi mednarodna organizacija, če je ta tretja država ali mednarodna organizacija sklenila sporazum o varovanju tajnosti podatkov z Unijo ali sklenila upravni dogovor s Komisijo ([10]).

POGLAVJE 3

OBRAVNAVANJE TAJNIH DONACIJ

Člen 5

Osnovna načela

1. Organ, ki dodeli tajno donacijo, pri dodelitvi tajne donacije skupaj z Varnostnim organom Komisije zagotovi, da so obveznosti upravičenca v zvezi z varovanjem tajnih podatkov EU, ki se uporabijo ali nastanejo pri izvajanju sporazuma o donaciji, sestavni del sporazuma o donaciji. Varnostne zahteve, povezane s posamezno donacijo, so v obliki listine o varnostnih vidikih. Vzorčna predloga listine o varnostnih vidikih je določena v Prilogi III.

2. Organ, ki dodeli donacijo, pred podpisom tajnega sporazuma o donaciji odobri vodič po stopnjah tajnosti za naloge, ki jih je treba opraviti, in podatke, ki nastanejo pri izvajanju sporazuma o donaciji ali, kadar je to ustrezno, na ravni programa ali projekta. Vodič po stopnjah tajnosti je sestavni del listine o varnostnih vidikih.

3. Varnostne zahteve, povezane s posameznim programom ali projektom, so v obliki varnostnega navodila za program (ali projekt) (v nadaljnjem besedilu: varnostno navodilo). Varnostno navodilo se lahko pripravi z uporabo določb predloge listine o varnostnih vidikih, kot je določena v Prilogi III. Sestavi ga služba Komisije, ki upravlja program ali projekt, v tesnem sodelovanju z varnostnim organom Komisije ter ga predloži v posvet strokovni skupini Komisije za varnost. Kadar je sporazum o donaciji del programa ali projekta z lastnim varnostnim navodilom, je listina o varnostnih vidikih v zvezi s sporazumom o donaciji v poenostavljeni obliki in vključuje sklicevanje na varnostne določbe, določene v varnostnem navodilu za program ali projekt.

4. Razen v primerih iz člena 3(9) se tajni sporazum o donaciji podpiše šele, ko je nacionalni varnostni organ ali imenovani varnostni organ prosilca potrdil varnostno dovoljenje organizacije prosilca ali, če se tajni sporazum o donaciji sklepa s konzorcijem, ko je potrjeno varnostno dovoljenje organizacije vsaj enega prosilca iz konzorcija s strani zadevnega nacionalnega varnostnega organa ali imenovanega varnostnega organa tega prosilca.

5. Načeloma in, če ni drugače določeno v drugih upoštevnih pravilih, se organ, ki dodeli donacijo, šteje za tvorca tajnih podatkov EU, ustvarjenih pri izvajanju sporazuma o donaciji.

([10]) Seznam sporazumov, ki jih je sklenila EU, in upravnih dogovorov, ki jih je sklenila Evropska komisija, v skladu s katerimi se lahko tajni podatki EU izmenjujejo s tretjimi državami in mednarodnimi organizacijami, je na voljo na spletišču Komisije.

6. Organ, ki dodeli donacijo, preko Varnostnega organa Komisije obvesti nacionalne varnostne organe in/ali imenovane varnostne organe vseh upravičencev in podizvajalcev o podpisu tajnih sporazumov o donacijah ali oddaji v podizvajanje in o vsakem podaljšanju ali predčasnem prenehanju takšnih pogodb oziroma podizvajalskih pogodb. Seznam zahtev po državah je naveden v Prilogi IV.

7. Sporazumi o donacijah, ki vključujejo tajne podatke stopnje tajnosti RESTREINT UE/EU RESTRICTED, vključujejo klavzulo o pogodbeni varnosti, ki določa, da so določbe iz Dodatka E Priloge III za upravičenca zavezujoče. Ti sporazumi o donacijah vključujejo listino o varnostnih vidikih, ki določa vsaj zahteve za obravnavanje podatkov stopnje tajnosti RESTREINT UE/EU RESTRICTED, vključno z vidiki informacijske varnosti in posebnimi zahtevami, ki jih morajo upravičenci izpolniti za akreditacijo svojega komunikacijskega in informacijskega sistema, s katerim se obravnavajo podatki stopnje tajnosti RESTREINT UE/EU RESTRICTED.

8. Če to zahtevajo nacionalni zakoni in predpisi držav članic, nacionalni varnostni organi ali imenovani varnostni organi zagotovijo, da upravičenci ali podizvajalci pod njihovo jurisdikcijo upoštevajo veljavne varnostne določbe za varovanje podatkov stopnje tajnosti RESTREINT UE/EU RESTRICTED in opravljajo preveritvene obiske v objektih upravičencev ali podizvajalcev, ki so na njihovem ozemlju. Kadar nacionalni varnostni organ ali imenovani varnostni organ nima take obveznosti, organ, ki dodeli donacijo, zagotovi, da upravičenci izvedejo potrebne varnostne določbe iz Dodatka E Priloge III.

Člen 6

Dostop osebja upravičencev in podizvajalcev do tajnih podatkov EU

1. Organ, ki dodeli donacijo, zagotovi, da tajni sporazumi o donacijah vključujejo določbe, v skladu s katerimi se lahko osebju upravičencev ali podizvajalcev, ki za izvajanje sporazuma oziroma podizvajalske pogodbe s tajnimi podatki potrebuje dostop do tajnih podatkov EU, tak dostop odobri le, če:

(a) je bilo ugotovljeno, da za osebje velja potreba po seznanitvi;

(b) ga je v primeru podatkov stopnje tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ali SECRET UE/EU SECRET varnostno preveril zadevni nacionalni varnostni organ ali imenovani varnostni organ ali kateri koli drug pristojni varnostni organ;

(c) je bilo osebje poučeno o varnostnih pravilih za varovanje tajnih podatkov EU, ki se uporabljajo, ter je sprejelo odgovornost za varovanje teh podatkov.

2. Če je ustrezno, mora biti dostop do tajnih podatkov EU tudi skladen s temeljnim aktom o vzpostavitvi programa in mora upoštevati dodatne oznake, opredeljene v vodiču po stopnjah tajnosti.

3. Če želi upravičenec ali podizvajalec na položaju, ki zahteva dostop do tajnih podatkov EU stopnje tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ali SECRET UE/EU SECRET, zaposliti državljana tretje države, je v skladu z nacionalnimi zakoni in predpisi, ki se uporabljajo na kraju, kjer se odobri dostop do tajnih podatkov EU, je upravičenec ali podizvajalec pristojen za začetek postopka varnostnega preverjanja take osebe.

Člen 7

Dostop strokovnjakov, ki sodelujejo pri preverjanjih, pregledih ali revizijah, do tajnih podatkov EU

1. Če pri preverjanjih, pregledih ali revizijah, ki jih izvaja organ, ki dodeljuje donacije, ali pri pregledih uspešnosti upravičencev, pri katerih je potreben dostop do podatkov s stopnjo tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ali SECRET UE/EU SECRET, sodelujejo zunanje osebe (v nadaljnjem besedilu: strokovnjaki), se z njimi sklene pogodba samo, če jih je na ustrezni stopnji varnostno preveril nacionalni varnostni organ ali imenovani varnostni organ ali kateri koli drug pristojni varnostni organ. Organ, ki dodeli donacijo, preko Varnostnega organa Komisije preveri strokovnjake in po potrebi zaprosi nacionalni varnostni organ ali imenovani varnostni organ, da začne postopek njihovega preverjanja najmanj šest mesecev pred začetkom veljavnosti njihove pogodbe.

2. Strokovnjaki morajo biti pred podpisom pogodbe poučeni o varnostnih pravilih za varovanje tajnih podatkov EU, ki se uporabljajo, ter sprejeti odgovornost za varovanje teh podatkov.

POGLAVJE 4

OBISKI V ZVEZI S TAJNIMI SPORAZUMI O DONACIJI

Člen 8

Osnovna načela

1. Če morajo imeti organ, ki dodeli donacijo, strokovnjaki, upravičenci ali podizvajalci za izvajanje tajnega sporazuma o donaciji dostop do podatkov stopnje tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ali SECRET UE/EU SECRET v prostorih enih ali drugih, se obiski organizirajo v sodelovanju z zadevnimi nacionalnimi varnostnimi organi ali imenovanimi varnostnimi organi ali katerimi koli drugimi pristojnimi varnostnimi organi.

2. Za obiske iz odstavka 1 veljajo naslednje zahteve:

(a) obisk ima uraden namen, povezan s tajnim sporazumom o donaciji;

(b) vsak obiskovalec mora imeti dovoljenje za dostop do tajnih podatkov za zahtevano stopnjo in potrebo po seznanitvi, da bi imel dostop do tajnih podatkov EU, ki se ustvarijo ali nastanejo pri izvajanju tajnega sporazuma o donaciji.

Člen 9

Zaprosila za najavo obiska

1. Obiski upravičencev ali podizvajalcev v prostorih drugih upravičencev ali podizvajalcev ali v prostorih organa, ki dodeli donacijo, ki vključujejo dostop do podatkov stopnje tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ali SECRET UE/EU SECRET, se organizirajo v skladu z naslednjim postopkom:

(a) uradnik za varnost objekta pošiljatelja obiskovalca izpolni vse ustrezne dele obrazca zaprosila za najavo obiska in ga predloži nacionalnemu varnostnemu organu ali imenovanemu varnostnemu organu objekta. Predloga obrazca zaprosila za najavo obiska je določena v Dodatku C Priloge III;

(b) nacionalni varnostni organ ali imenovani varnosti organ objekta pošiljatelja mora dovoljenje obiskovalca za dostop do tajnih podatkov potrditi, preden zaprosilo za najavo obiska predloži nacionalnemu varnostnemu organu ali imenovanemu varnostnemu organu objekta gostitelja (ali varnostnemu organu Komisije, če je obisk v prostorih organa, ki dodeli donacijo);

(c) uradnik za varnost objekta pošiljatelja nato od svojega nacionalnega varnostnega organa ali imenovanega varnostnega organa pridobi odgovor nacionalnega varnostnega organa ali imenovanega varnostnega organa objekta gostitelja (ali varnostnega organa Komisije), o bodisi odobritvi bodisi zavrnitvi zaprosila za najavo obiska;

(d) zaprosilo za najavo obiska se šteje za odobreno, če do petih delovnih dni pred datumom obiska ni ugovorov.

2. Obiski uradnikov organa, ki dodeli donacijo, strokovnjakov ali revizorjev v prostorih upravičencev ali podizvajalcev, ki vključujejo dostop do podatkov stopnje tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ali SECRET UE/EU SECRET, se organizirajo v skladu z naslednjim postopkom:

(a) obiskovalec izpolni vse ustrezne dele obrazca zaprosila za najavo obiska in ga predloži varnostnemu organu Komisije;

(b) varnostni organ Komisije pred predložitvijo zaprosila za najavo obiska nacionalnemu varnostnemu organu ali imenovanemu varnostnemu organu objekta gostitelja potrdi dovoljenje obiskovalca za dostop do tajnih podatkov;

(c) varnostni organ Komisije od nacionalnega varnostnega organa ali imenovanega varnostnega organa objekta gostitelja pridobi odgovor o bodisi odobritvi bodisi zavrnitvi zaprosila za najavo obiska;

(d) zaprosilo za najavo obiska se šteje za odobreno, če do petih delovnih dni pred datumom obiska ni ugovorov.

3. Zaprosilo za najavo obiska lahko velja za en sam obisk ali za ponavljajoče se obiske. V primeru ponavljajočih se obiskov je lahko zaprosilo za najavo obiska veljavno do največ enega leta od datuma začetka veljavnosti zaprosila.

4. Veljavnost posameznega zaprosila za najavo obiska ne presega veljavnosti dovoljenja obiskovalca za dostop do tajnih podatkov.

5. Praviloma bi bilo treba zaprosilo za najavo obiska predložiti pristojnemu varnostnemu organu objekta gostitelja najpozneje 15 delovnih dni pred datumom obiska.

Člen 10

Postopki za obiske

1. Preden se obiskovalcem dovoli dostop do tajnih podatkov EU, mora varnostna služba objekta gostitelja izpolniti vse z obiskom povezane varnostne postopke in pravila, ki jih je določil nacionalni varnostni organ ali imenovani varnostni organ.

2. Obiskovalci dokažejo svojo istovetnost ob prihodu v objekt gostitelja s predložitvijo veljavne osebne izkaznice ali potnega lista. Ti identifikacijski podatki ustrezajo podatkom iz zaprosila za najavo obiska.

3. Objekt gostitelja zagotovi, da se vodi evidenca vseh obiskovalcev, vključno z njihovimi imeni, organizacijo, ki jo zastopajo, datumom izteka veljavnosti dovoljenja za dostop do tajnih podatkov, datumom obiska in imeni obiskanih oseb. Take evidence se hranijo najmanj pet let ali dlje, če tako zahtevajo nacionalni predpisi države, v kateri se nahaja objekt gostitelja.

Člen 11

Neposredno organizirani obiski

1. V okviru posebnih projektov se lahko ustrezni nacionalni varnostni organi ali imenovani varnostni organi in varnostni organ Komisije dogovorijo o postopku, po katerem se lahko obiski za določeno tajno donacijo organizirajo neposredno med obiskovalčevim uradnikom za varnost in uradnikom za varnost objekta, ki bo obiskan. Predloga obrazca, ki se uporabi za ta namen, je določena v Dodatku C Priloge III. Tak izredni postopek se določi v varnostnem navodilu ali z drugo posebno ureditvijo. V takem primeru se postopki iz člena 9 in člena 10(1) ne uporabljajo.

2. Obiski, ki vključujejo dostop do podatkov stopnje tajnosti RESTREINT UE/EU RESTRICTED, se organizirajo neposredno med pošiljateljem in gostiteljem, ne da bi bilo treba upoštevati postopke iz člena 9 in člena 10(1).

POGLAVJE 5

RAZPOSILJANJE IN PRENASANJE TAJNIH PODATKOV EU PRI IZVAJANJU TAJNIH SPORAZUMOV O DONACIJI

Člen 12

Osnovna načela

Organ, ki dodeli donacijo, zagotovi, da so vse odločitve v zvezi z razpošiljanjem in prenašanjem tajnih podatkov EU skladne s Sklepom (EU, Euratom) 2015/444 in njegovimi izvedbenimi pravili ter pogoji tajnega sporazuma o donaciji, vključno s privolitvijo tvorca.

Člen 13

Elektronsko obravnavanje

1. Elektronsko obravnavanje in razpošiljanje tajnih podatkov EU se izvajata v skladu s poglavjema 5 in 6 Sklepa (EU, Euratom) 2015/444 in njegovimi izvedbenimi pravili.

Komunikacijske in informacijske sisteme, ki so v lasti upravičenca in se uporabljajo za obravnavanje tajnih podatkov EU za izvajanje sporazuma o donaciji (v nadaljnjem besedilu: komunikacijski in informacijski sistemi upravičenca), mora akreditirati pristojni organ za varnostno akreditacijo. Vsako elektronsko razpošiljanje tajnih podatkov EU se zaščiti s šifrirnimi izdelki, odobrenimi v skladu s členom 36(4) Sklepa (EU, Euratom) 2015/444. Varnostni ukrepi TEMPEST se izvajajo v skladu s členom 36(6) navedenega sklepa.

2. Za varnostno akreditacijo komunikacijskih in informacijskih sistemov upravičenca, s katerimi se obravnavajo tajni podatki EU stopnje tajnosti RESTREINT UE/EU RESTRICTED, in kakršno koli njihovo medsebojno povezovanje se lahko pooblasti upravičenčevega uradnika za varnost, če to dovoljujejo nacionalni zakoni in predpisi. Kadar se pooblastilo za nalogo prenese na upravičenca, je slednji pristojen za izvajanje minimalnih varnostnih zahtev, ki so opisane v listini o varnostnih vidikih, pri obravnavanju podatkov stopnje tajnosti RESTREINT UE/EU RESTRICTED z njegovimi komunikacijskimi in informacijskimi sistemi. Vendar ustrezni nacionalni varnostni organi ali imenovani varnostni organi in organ za varnostno akreditacijo ohranijo pristojnost za varovanje podatkov stopnje tajnosti RESTREINT UE/EU RESTRICTED, ki jih obravnava upravičenec, in pravico do pregleda varnostnih ukrepov, ki jih sprejme upravičenec. Poleg tega upravičenec organu, ki dodeli donacijo, in, če tako zahtevajo nacionalni zakoni in drugi predpisi, pristojnemu nacionalnemu organu za varnostno akreditacijo predloži izjavo o skladnosti, ki potrjuje, da so bili komunikacijski in informacijski sistemi upravičenca in povezane medsebojne povezave akreditirani za obravnavanje tajnih podatkov EU stopnje tajnosti RESTREINT UE/EU RESTRICTED ([11]).

Člen 14

Prevozi, ki jih izvajajo komercialne kurirske službe

Za prevoz tajnih podatkov EU s komercialnimi kurirskimi službami veljajo ustrezne določbe Sklepa Komisije (EU, Euratom) 2019/1962 ([12]) o izvedbenih pravilih za obravnavanje podatkov stopnje RESTREINT UE/EU RESTRICTED in Sklepa Komisije (EU, Euratom) 2019/1961 ([13]) o izvedbenih pravilih za obravnavanje podatkov stopnje CONFIDENTIEL UE/EU CONFIDENTIAL in SECRET UE/EU SECRET.

Člen 15

Ročni prenos

1. Za ročni prenos tajnih podatkov veljajo stroge varnostne zahteve.

2. Podatke stopnje tajnosti RESTREINT UE/EU RESTRICTED lahko ročno prenaša osebje upravičenca znotraj Unije, če so izpolnjene naslednje zahteve:

(a) uporabljena ovojnica ali pakiranje je neprosojno in na njem ni označena stopnja tajnosti njegove vsebine;

(b) tajni podatki se ne dajo iz rok prenašalca;

(c) ovojnica ali pakiranje se ne odpre na poti.

3. Pri tajnih podatkih stopnje tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL in SECRET UE/EU SECRET se pošiljatelj in prejemnik vnaprej dogovorita o ročnem prenosu, ki ga izvaja osebje upravičenca znotraj države članice. Organ oziroma subjekt za razpošiljanje obvesti organ oziroma subjekt za prejemanje o podrobnostih pošiljke, vključno s sklicem, stopnjo tajnosti, pričakovanim časom prihoda in imenom kurirja. Tak ročni prenos je dovoljen, če so izpolnjene naslednje zahteve:

(a) tajni podatki se prenašajo v dvojni ovojnici ali pakiranju;

(b) zunanja ovojnica ali pakiranje je dobro zaprto in na njem ni označena stopnja tajnosti njegove vsebine, na notranji ovojnici pa je stopnja tajnosti označena;

(c) tajni podatki EU se ne dajo iz rok prenašalca;

(d) ovojnica ali pakiranje se ne odpre na poti;

(e) ovojnica ali pakiranje se prenaša v aktovki, ki jo je mogoče zakleniti, ali v podobni odobreni embalaži take velikosti in teže, da jo lahko prenašalec vedno nosi pri sebi in se ne izroči v oddano prtljago;

(f) kurir ima pri sebi kurirsko potrdilo, ki ga je izdal njegov pristojni varnostni organ, ki mu omogoča prenašanje tako identificirane tajne pošiljke.

([11]) Minimalne zahteve za komunikacijske in informacijske sisteme, s katerimi se obravnavajo tajni podatki EU stopnje tajnosti RESTREINT UE/EU RESTRICTED, so določene v Dodatku E Priloge III.

([12]) Sklep Komisije (EU, Euratom) 2019/1962 z dne 17. oktobra 2019 o izvedbenih pravilih za obravnavanje podatkov stopnje RESTREINT UE/EU RESTRICTED (UL L 311, 2.12.2019, str. 21).

([13]) Sklep Komisije (EU, Euratom) 2019/1961 z dne 17. oktobra 2019 o izvedbenih pravilih za obravnavanje podatkov stopnje CONFIDENTIEL UE/EU CONFIDENTIAL in SECRET UE/EU SECRET (UL L 311, 2.12.2019, str. 1).

4. Za ročno prenašanje podatkov stopnje tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL in SECRET UE/EU SECRET, ki ga izvaja osebje upravičenca, iz ene države članice v drugo se uporabljajo naslednja dodatna pravila:

(a) kurir je odgovoren za varno hrambo tajnega gradiva, ki se prenaša, dokler ni izročeno prejemniku;

(b) v primeru kršitve varovanja tajnosti lahko nacionalni varnostni organ ali imenovani varnostni organ pošiljatelja zahteva, da organi v državi, v kateri je prišlo do kršitve, izvedejo preiskavo, poročajo o svojih ugotovitvah in po potrebi sprejmejo pravne ali druge ukrepe;

(c) kurir je bil poučen o vseh varnostnih obveznostih, ki jih je treba spoštovati med prenosom, in je podpisal ustrezno potrdilo o seznanjenosti;

(d) navodila za kurirja se priložijo kurirskemu potrdilu;

(e) kurirju sta zagotovljena opis pošiljke in načrt poti;

(f) dokumenti se po opravljenem prevozu vrnejo nacionalnemu varnostnemu organu ali imenovanemu varnostnemu organu, ki jih je izdal, ali pa jih prejemnik hrani za namene spremljanja;

(g) če carinski organi, organi za priseljevanje ali mejni policisti zahtevajo preveritev in podroben pregled pošiljke, se jim dovoli, da odprejo in opazujejo zadostne dele pošiljke, da ugotovijo, ali pošiljka ne vsebuje nobenega drugega gradiva razen prijavljenega;

(h) carinske organe je treba pozvati, naj spoštujejo uradno veljavo odpremne listine in pooblastil, ki jih ima pri sebi kurir.

Če carinski organi odprejo pošiljko, je treba to opraviti zunaj vidnega polja nepooblaščenih oseb in po možnosti v prisotnosti kurirja. Kurir zahteva, da se pošiljka ponovno zapakira, in od organov, ki izvajajo pregled, zahteva, da pošiljko ponovno zapečatijo in pisno potrdijo, da so jo odprli.

5. Za ročni prenos podatkov stopnje tajnosti RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL in SECRET UE/EU SECRET, ki ga izvaja osebje upravičenca, v tretjo državo ali mednarodno organizacijo veljajo določbe sporazuma o varovanju tajnosti podatkov ali upravnega dogovora, sklenjenega med Unijo oziroma Komisijo in to tretjo državo ali mednarodno organizacijo.

POGLAVJE 6

NACRTOVANJE NEPREKINJENEGA POSLOVANJA

Člen 16

Načrti za izredne razmere in obnovitveni ukrepi

Organ, ki dodeli donacijo, zagotovi, da tajni sporazum o donaciji od upravičencev zahteva, da pripravijo načrte poslovanja za izredne razmere za zaščito tajnih podatkov EU, ki se obravnavajo v zvezi z izvajanjem tajnega sporazuma o donaciji v izrednih razmerah, in vzpostavi preventivne in obnovitvene ukrepe v okviru načrtovanja neprekinjenega poslovanja, da se čim bolj zmanjša učinek incidentov v zvezi z obravnavo in hrambo tajnih podatkov EU. Upravičenci organu, ki dodeli donacijo, potrdijo, da so njihovi načrti poslovanja za izredne razmere sprejeti.

Člen 17

Začetek veljavnosti

Ta sklep začne veljati dvajseti dan po objavi v *Uradnem listu Evropske unije*.

V Bruslju, 10. februarja 2021

Za Komisijo
V imenu predsednice
Johannes HAHN
Član Komisije

PRILOGA I

STANDARDNE INFORMACIJE V RAZPISU

(se prilagodi glede na uporabljeni razpis)

Varnost

Projekte, ki vključujejo tajne podatke EU, je treba za odobritev financiranja varnostno pregledati, zanje lahko veljajo posebna varnostna pravila (podrobno opisana v listini o varnostnih vidikih, ki je priložena sporazumu o donaciji).

Ta pravila (urejena s Sklepom Komisije (EU, Euratom) 2015/444 ([1]) in/ali nacionalnimi pravili) npr. določajo:

— da projektov, ki vključujejo informacije stopnje tajnosti TRES SECRET UE/EU TOP SECRET (ali enakovredne) **NI** mogoče financirati;

— da morajo biti tajni podatki označeni v skladu z veljavnimi varnostnimi navodili v listini o varnostnih vidikih;

— da se podatki stopnje tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ali višje (in RESTREINT UE/EU RESTRICTED, če tako zahtevajo nacionalna pravila):

  — lahko ustvarjajo ali se do njih dostopa samo v prostorih z varnostnim dovoljenjem organizacije, ki ga je izdal pristojni nacionalni varnostni organ v skladu z nacionalnimi pravili;

  — lahko obravnavajo samo v varnostnem območju, ki ga je akreditiral pristojni nacionalni varnostni organ;

  — lahko obravnavajo in je do njih mogoč dostop samo s strani oseb z veljavnim dovoljenjem za dostop do tajnih podatkov in s potrebo po seznanitvi;

— da je treba tajne podatke ob izteku donacije vrniti ali jih še naprej varovati v skladu z veljavnimi pravili;

— da se lahko opravljanje nalog, ki vključujejo tajne podatke EU, odda v podizvajanje samo po predhodnem pisnem dovoljenju organa, ki dodeli donacijo, in samo subjektom s sedežem v državi članici EU ali državi nečlanici, ki ima z EU sklenjen sporazum o varnosti podatkov (ali dogovor o izvajanju s Komisijo);

— da je za razkritje tajnih podatkov EU potrebno predhodno pisno dovoljenje organa, ki dodeli donacijo.

Opozarjamo, da je glede na vrsto dejavnosti morda treba predložiti varnostno dovoljenje organizacije pred podpisom tajnega sporazuma o donaciji. Organ, ki dodeli donacijo, za vsak primer posebej oceni, ali je potrebno dovoljenje, in med pripravo donacije določi, kdaj ga je treba predložiti. Opozarjamo, da **v nobenem primeru** ne moremo podpisati sporazuma o donaciji, dokler nima vsaj eden od upravičencev varnostnega dovoljenja organizacije.

Sporazumu o donaciji se lahko dodajo še nadaljnja varnostna priporočila v obliki varnostnih rezultatov (*npr. ustanovitev svetovalne skupine za varnost, omejitev stopnje podrobnosti, uporaba namišljenega scenarija, izključitev uporabe tajnih podatkov itd.*).

Upravičenci morajo zagotoviti, da za njihove projekte ne veljajo nacionalne varnostne zahteve ali varnostne zahteve tretje države, ki bi lahko vplivale na izvajanje ali ogrozile dodelitev donacije (*npr. omejitve glede tehnologije, nacionalna stopnja tajnosti itd.*). O možnih varnostnih vprašanjih je treba takoj obvestiti organ, ki dodeljuje donacijo.

[Dodatna MOŽNOST za okvirne sporazume o partnerstvu: pri okvirnih sporazumih o partnerstvu je morda treba varnostno pregledati tako vloge za okvirni sporazum o partnerstvu kot tudi prošnje za donacijo.]

([1]) Gl. Sklep Komisije (EU, Euratom) 2015/444 z dne 13. marca 2015 o varnostnih predpisih za varovanje tajnih podatkov EU (UL L 72, 17.3.2015, str. 53).

PRILOGA II

DOLOČBE STANDARDNEGA SPORAZUMA O DONACIJI

(se prilagodi glede na uporabljeni sporazum o donaciji)

13.2 Varnost – tajni podatki

Pogodbenice morajo obravnavati tajne podatke (tajne podatke EU ali nacionalne) skladno z veljavno zakonodajo EU ali nacionalno zakonodajo o tajnih podatkih (zlasti s Sklepom Komisije (EU, Euratom) 2015/444 ([1]) in njegovimi izvedbenimi pravili).

Morebitna posebna varnostna pravila so določena v Prilogi 5.

PRILOGA 5

Varnost – tajni podatki EU

[MOŽNOST za ukrepe s tajnimi podatki EU (standardna): Če se pri ukrepu uporabljajo ali ustvarjajo tajni podatki EU, jih je treba obravnavati skladno z vodičem po stopnjah tajnosti in listino o varnostnih vidikih iz Priloge 1 ter Sklepom (EU, Euratom) 2015/444 in njegovimi izvedbenimi pravili, dokler se stopnja tajnosti ne prekliče.

Vse rezultate, ki vključujejo tajne podatke EU, je treba predložiti v skladu s posebnimi postopki, dogovorjenimi z organom, ki dodeli donacijo.

Opravljanje nalog, ki vključujejo tajne podatke EU, odda v podizvajanje samo po predhodnem izrecnem pisnem dovoljenju organa, ki dodeli donacijo, in samo subjektom s sedežem v državi članici EU ali državi nečlanici, ki ima z EU sklenjen sporazum o varnosti podatkov (ali dogovor o izvajanju s Komisijo);

Tajni podatki EU se ne smejo razkriti nobeni tretji osebi (vključno z udeleženci, ki sodelujejo pri izvajanju ukrepa) brez predhodnega izrecnega pisnega dovoljenja organa, ki dodeli donacijo.]

([1]) Sklep Komisije (EU, Euratom) 2015/444 z dne 13. marca 2015 o varnostnih predpisih za varovanje tajnih podatkov EU (UL L 72, 17.3.2015, str. 53).

PRILOGA III

[Priloga IV (k ……)]

LISTINA O VARNOSTNIH VIDIKIH [1]

[Vzorec]

[1] Ta vzorec listine o varnostnih vidikih se uporablja, kadar se Komisija šteje za tvorca tajnih podatkov, ki se ustvarjajo ali obravnavajo pri izvajanju sporazuma o donaciji. Kadar tvorec tajnih podatkov, ki se ustvarjajo ali obravnavajo pri izvajanju sporazuma o donaciji, ni Komisija in kadar imajo države članice, ki sodelujejo pri donaciji, vzpostavljen poseben varnostni okvir, se lahko uporabljajo druge vrste listine o varnostnih vidikih.

Dodatek A

VARNOSTNE ZAHTEVE

Organ, ki dodeljuje donacijo, mora v listino o varnostnih vidikih vključiti naslednje varnostne zahteve. Nekatere klavzule se za sporazum o donaciji morda ne uporabljajo. Te so prikazane v oglatih oklepajih.

Seznam klavzul ni izčrpen. Glede na naravo tajnega sporazuma o donaciji se lahko dodajo dodatne klavzule.

SPOŠNI POGOJI [*Opomba: uporabljajo se za vse tajne sporazume o donaciji.*]

1. Ta listina o varnostnih vidikih je sestavni del sporazuma o donaciji [oziroma podizvajalske pogodbe] in opisuje varnostne zahteve, povezane s posameznim sporazumom o donaciji. Neizpolnjevanje teh zahtev je lahko zadosten razlog za odpoved sporazuma o donaciji.

2. Za upravičence donacije veljajo vse obveznosti iz Sklepa Komisije (EU, Euratom) 2015/444 ([2]) (v nadaljnjem besedilu: Sklep 2015/444) in njegovih izvedbenih pravil ([3]). Če ima upravičenec donacije težave z uporabo veljavnega pravnega okvira v državi članici, se mora obrniti na Varnostni organ Komisije in nacionalni varnostni organ ali imenovani varnostni organ.

3. Tajni podatki, ki nastanejo pri izvajanju sporazuma o donaciji, morajo biti označeni kot tajni podatki EU stopnje tajnosti, kot je določena v vodiču po stopnjah tajnosti iz Dodatka B k tej listini. Odstopanje od stopnje tajnosti, ki jo določa vodič po stopnjah tajnosti, je dovoljeno samo s pisnim dovoljenjem organa, ki dodeli donacijo.

4. Komisija kot organ, ki dodeli donacijo, uveljavlja pravice, ki pripadajo tvorcu vseh tajnih podatkov EU, ki so bili ustvarjeni in obravnavani za izvajanje tajnega sporazuma o donaciji.

5. Upravičenec oziroma podizvajalec ne sme nobenih podatkov ali gradiva, ki mu jih zagotovi organ, ki dodeli donacijo, ali se mu predložijo v imenu tega organa, brez pisnega soglasja naročnika uporabiti za noben drug namen, kot je izvajanje sporazuma o donaciji.

6. Če je za izvajanje sporazuma o donaciji potrebno varnostno dovoljenje organizacije, mora upravičenec zaprositi organ, ki dodeli donacijo, da opravi postopek zahteve za varnostno dovoljenje organizacije.

7. Upravičenec mora preiskati vse kršitve varnosti v zvezi s tajnimi podatki EU in o njih takoj, ko je mogoče, poročati organu, ki dodeli donacijo. Upravičenec oziroma podizvajalec mora pristojnemu nacionalnemu varnostnemu organu ali imenovanemu varnostnemu organu ter, če to dopuščajo nacionalni zakoni in drugi predpisi, Varnostnemu organu Komisije nemudoma poročati o vseh primerih, v katerih je znano ali pa obstaja razlog za sum, da so bili tajni podatki EU, ki so bili predloženi ali so nastali na podlagi sporazuma o donaciji, izgubljeni ali razkriti nepooblaščenim osebam.

([2]) Sklep Komisije (EU, Euratom) 2015/444 z dne 13. marca 2015 o varnostnih predpisih za varovanje tajnih podatkov EU (UL L 72, 17.3.2015, str. 53).

([3]) Organ, ki dodeli donacijo, po sprejetju izvedbenih pravil vstavi sklice nanje.

8. Po izteku sporazuma o donaciji mora upravičenec oziroma podizvajalec organu, ki dodeli donacijo, čim prej vrniti vse tajne podatke EU, ki jih ima. Če je izvedljivo, lahko upravičenec oziroma podizvajalec uniči tajne podatke EU, namesto da bi jih vrnil. To je treba storiti v skladu z nacionalnimi zakoni in predpisi države, v kateri ima upravičenec sedež, s predhodnim soglasjem Varnostnega organa Komisije in po njegovih navodilih. Tajni podatki EU morajo biti uničeni tako, da jih ni mogoče niti v celoti niti delno rekonstruirati.

9. Če ima upravičenec ali podizvajalec dovoljenje, da po prenehanju veljavnosti ali izteku sporazuma o donaciji obdrži tajne podatke EU, je treba tajne podatke EU še naprej varovati v skladu s Sklepom 2015/444 in njegovimi izvedbenimi pravili ([4]).

10. Pri elektronski obravnavi, obdelavi in prenosu tajnih podatkov EU je treba upoštevati določbe poglavja 5 in 6 Sklepa 2015/444. Med njim so med drugim zahteve: da je za komunikacijske in informacijske sisteme v lasti upravičenca, ki se uporabljajo za obravnavo tajnih podatkov EU za namene sporazuma o donaciji (v nadaljnjem besedilu: upravičenčevi komunikacijski in informacijski sistemi), potrebna akreditacija ([5]); da je treba vsako elektronsko razpošiljanje tajnih podatkov EU zaščititi s šifrirnimi izdelki, odobrenimi v skladu s členom 36(4) Sklepa 2015/444, in da je treba varnostne ukrepe TEMPEST izvajati v skladu s členom 36(6) Sklepa 2015/444.

11. Upravičenec oziroma podizvajalec pripravi načrte neprekinjenega poslovanja za zaščito vseh tajnih podatkov EU, ki jih obravnava pri izvajanju tajnega sporazuma o donaciji, v izrednih razmerah in uvede preventivne in obnovitvene ukrepe, da se čim bolj zmanjša učinek incidentov, povezanih z obravnavo in hrambo tajnih podatkov EU. Upravičenec oziroma podizvajalec mora obvestiti organ, ki dodeli donacijo, o svojih načrtih neprekinjenega poslovanja.

SPORAZUMI O DONACIJI, KI ZAHTEVAJO DOSTOP DO PODATKOV STOPNJE TAJNOSTI RESTREINT UE/EU RESTRICTED

12. Dovoljenje za dostop do tajnih podatkov načeloma ni potrebno za izpolnjevanje sporazuma o donaciji ([6]). Vendar morajo biti podatki ali gradivo stopnje tajnosti RESTREINT UE/EU RESTRICTED dostopni samo osebju upravičenca, ki tovrstne podatke potrebuje za izvedbo sporazuma o donaciji (načelo potrebe po seznanitvi) in ga je upravičenčev uradnik za varstvo poučil o njihovih odgovornostih in posledicah kakršnega koli nepooblaščenega razkritja ali kršitve varnosti teh podatkov ter ki je pisno potrdilo svojo seznanitev s posledicami nevarovanja tajnih podatkov EU.

13. Razen če je organ, ki dodeli donacijo, dal pisno soglasje, upravičenec oziroma podizvajalec ne sme zagotoviti dostopa do podatkov ali gradiva stopnje tajnosti RESTREINT UE/EU RESTRICTED nobenemu subjektu ali osebi, ki ni član njegovega osebja, za katero velja potreba po seznanitvi.

14. Upravičenec oziroma podizvajalec mora ohraniti oznake stopnje tajnosti tajnih podatkov, ki so nastali med izvajanjem sporazuma o donaciji ali so bili med izvajanjem sporazuma o donaciji zagotovljeni, in ne sme preklicati stopnje tajnosti podatkov brez pisnega soglasja organa, ki dodeli donacijo.

15. Kadar se podatki ali gradivo stopnje tajnosti RESTREINT UE/EU RESTRICTED ne uporabljajo, jih je treba hraniti v zaklenjenih pisarniških omarah. Med prevozom morajo biti dokumenti v neprosojnem ovoju. Dokumenti se ne smejo dati iz rok prenašalca in jih ni dovoljeno odpreti na poti.

([4]) Organ, ki dodeli donacijo, po sprejetju izvedbenih pravil vstavi sklice nanje.

([5]) Pogodbenica, ki bo izvedla akreditacijo, bo morala organu, ki dodeli donacijo, predložiti izjavo o skladnosti, in sicer prek varnostnega organa Komisije in v sodelovanju z ustreznim nacionalnim organom za varnostno akreditacijo.

([6]) Če so upravičenci iz držav članic, ki za donacije s stopnjo tajnosti RESTREINT UE/EU RESTRICTED zahtevajo dovoljenje za dostop do tajnih podatkov in/ali varnostno dovoljenje organizacije, organ, ki dodeli donacijo, v listini o varnostnih vidikih navede te zahteve glede dovoljenja za dostop do tajnih podatkov in varnostnega dovoljenja organizacije za zadevne upravičence.

16. Upravičenec oziroma podizvajalec lahko dokumente stopnje tajnosti RESTREINT UE/EU RESTRICTED pošlje organu, ki dodeli donacijo, tako, da uporabi komercialne kurirske službe, poštne storitve, ročni prenos ali elektronska sredstva. Pri tem mora upravičenec oziroma podizvajalec upoštevati varnostno navodilo programa (ali projekta), ki ga je izdala Komisija, in/ali izvedbena pravila Komisije za industrijsko varnost v zvezi s tajnimi donacijami ([7]).

17. Ko dokumenti stopnje tajnosti RESTRAINT UE/EU RESTRICTED niso več potrebni, jih je treba uničiti tako, da jih ni mogoče niti v celoti niti delno rekonstruirati.

18. Za varnostno akreditacijo upravičenčevih komunikacijskih in informacijskih sistemov, s katerimi se obravnavajo tajni podatki EU stopnje tajnosti RESTREINT UE/EU RESTRICTED, in za kakršno koli njihovo medsebojno povezovanje se lahko pooblasti upravičenčevega uradnika za varnost, če to dopuščajo nacionalni zakoni in predpisi. Kadar se tako prenese pooblastilo za akreditacijo, nacionalni varnostni organi, imenovani varnostni organi ali organi za varnostno akreditacijo ohranijo pristojnost za varovanje vseh podatkov stopnje tajnosti RESTREINT UE/EU RESTRICTED, ki jih obravnava upravičenec, in pravico do pregleda varnostnih ukrepov, ki jih sprejme upravičenec. Poleg tega upravičenec organu, ki dodeli donacijo, in, če tako zahtevajo nacionalni zakoni in drugi predpisi, pristojnemu nacionalnemu organu za varnostno akreditacijo predloži izjavo o skladnosti, ki potrjuje, da so bili upravičenčevi komunikacijski in informacijski sistemi in povezane medsebojne povezave akreditirani za obravnavanje tajnih podatkov EU stopnje tajnosti RESTREINT UE/EU RESTRICTED.

OBRAVNAVANJE PODATKOV STOPNJE TAJNOSTI RESTREINT UE/EU RESTRICTED V KOMUNIKACIJSKIH IN INFORMACIJSKIH SISTEMIH

19. Minimalne zahteve za komunikacijske in informacijske sisteme, s katerimi se obravnavajo podatki stopnje RESTREINT UE/EU RESTRICTED, so določene v Dodatku E k tej listini o varnostnih vidikih.

POGOJI, POD KATERIMI LAHKO UPRAVIČENEC ODDA NAROČILO V PODIZVAJANJE

20. Preden odda upravičenec kateri koli del tajnega sporazuma o donaciji v podizvajanje, mora od organa, ki dodeli donacijo, pridobiti dovoljenje.

21. S subjektom, ki je registriran v tretji državi, ali subjektom, ki je član mednarodne organizacije, se ne sme skleniti nobena podizvajalska pogodba, če ta tretja država ali mednarodna organizacija ni sklenila sporazuma o varovanju tajnosti podatkov z EU ali upravnega dogovora s Komisijo.

22. Če je upravičenec sklenil podizvajalsko pogodbo, se varnostne določbe sporazuma o donaciji smiselno uporabljajo za podizvajalca in njegovo osebje. V takem primeru je upravičenec odgovoren za zagotovitev, da vsi podizvajalci v svojih podizvajalskih pogodbenih razmerjih uporabljajo ta načela. Za zagotovitev ustreznega varnostnega nadzora Varnostni organ Komisije uradno obvesti vse nacionalne varnostne organe in/ali imenovane varnostne organe upravičenca in podizvajalca o sklenitvi vseh povezanih podizvajalskih pogodb s tajnimi podatki stopnje tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL in SECRET UE/EU SECRET. Po potrebi se nacionalnim varnostnim organom in/ali imenovanim varnostnim organom upravičenca in podizvajalca predložijo kopije varnostnih določb, povezanih s posamezno podizvajalsko pogodbo. Nacionalni varnostni organi in imenovani varnostni organi, ki jih je treba uradno obvestiti o varnostnih določbah tajnih sporazumov o donaciji stopnje tajnosti RESTREINT UE/EU RESTRICTED, so navedeni v prilogi k izvedbenim pravilom Komisije za industrijsko varnost v zvezi tajnimi sporazumi o donaciji ([8]).

23. Upravičenec brez predhodnega pisnega dovoljenja organa, ki dodeli donacijo, tajnih podatkov EU ne sme razkriti podizvajalcu. Če je treba tajne podatke EU podizvajalcem pošiljati pogosto ali rutinsko, lahko organ, ki dodeli donacijo, da dovoljenje za določeno obdobje (npr. 12 mesecev) ali za čas trajanja podizvajalske pogodbe.

([7]) Organ, ki dodeli donacijo, po sprejetju izvedbenih pravil vstavi sklice nanje.
([8]) Organ, ki dodeli donacijo, po sprejetju izvedbenih pravil vstavi sklice nanje.

OBISKI

Če se za obiske, ki vključujejo podatke stopnje tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ali SECRET UE/EU SECRET, uporablja standardni postopek za predložitev zaprosila za najavo obiska, mora organ, ki dodeli donacijo, vključiti odstavke 24, 25 in 26 ter črtati odstavek 27. Če se obiski, ki vključujejo podatke stopnje tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ali SECRET UE/EU SECRET, organizirajo neposredno med pošiljateljem in gostiteljem, mora organ, ki dodeli donacijo, črtati odstavka 25 in 26 ter vključiti samo odstavek 27.

24. Obiski, ki vključujejo dostop ali potencialni dostop do podatkov stopnje tajnosti RESTREINT UE/EU RESTRICTED, se organizirajo neposredno med pošiljateljem in gostiteljem, ne da bi bilo treba upoštevati postopke iz odstavkov 25 do 27 v nadaljevanju.

[25. Za obiske, ki vključujejo dostop ali potencialni dostop do podatkov stopnje tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ali SECRET UE/EU SECRET, se uporablja naslednji postopek:

(a) uradnik za varnost objekta pošiljatelja izpolni vse ustrezne dele obrazca zaprosila za najavo obiska (Dodatek C) in zaprosilo predloži nacionalnemu varnostnemu organu ali imenovanemu varnostnemu organu objekta;

(b) nacionalni varnostni organ ali imenovani varnostni organ objekta pošiljatelja mora dovoljenje obiskovalca za dostop do tajnih podatkov potrditi, preden zaprosilo za najavo obiska predloži nacionalnemu varnostnemu organu ali imenovanemu varnostnemu organu objekta gostitelja (ali varnostnemu organu Komisije, če je obisk v prostorih organa, ki dodeli donacijo);

(c) uradnik za varnost objekta pošiljatelja nato od svojega nacionalnega varnostnega organa ali imenovanega varnostnega organa pridobi odgovor nacionalnega varnostnega organa ali imenovanega varnostnega organa objekta gostitelja (ali varnostnega organa Komisije), o bodisi odobritvi bodisi zavrnitvi zaprosila za najavo obiska;

(d) zaprosilo za najavo obiska se šteje za odobreno, če do petega delovnega dne pred datumom obiska ni ugovorov.]

[26. Preden se obiskovalcu omogoči dostop do podatkov stopnje tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ali SECRET UE/EU SECRET, mora objekt gostitelja prejeti dovoljenje svojega nacionalnega varnostnega organa ali imenovanega varnostnega organa.]

[27. Obiski, ki vključujejo dostop ali potencialni dostop do podatkov stopnje tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ali SECRET UE/EU SECRET, se organizirajo neposredno med pošiljateljem in gostiteljem (primer obrazca, ki se lahko uporabi za ta namen, je v Dodatku C).]

[28. Obiskovalci morajo dokazati svojo istovetnost ob prihodu v objekt gostitelja s predložitvijo veljavne osebne izkaznice ali potnega lista.

[29. Objekt, ki gosti obiskovalca, mora zagotoviti, da se vodi evidenca vseh obiskovalcev. Ta mora vključevati njihova imena, organizacijo, ki jo zastopajo, datum izteka veljavnosti dovoljenja za dostop do tajnih podatkov (če je ustrezno), datum obiska in imena obiskanih oseb. Ne glede na pravila EU v zvezi z varstvom podatkov se take evidence hranijo najmanj pet let ali v skladu z nacionalnimi pravili in predpisi, kot je ustrezno.

OCENJEVALNI OBISKI

30. Varnostni organ Komisije lahko v sodelovanju z ustreznimi nacionalnimi varnostnimi organi ali imenovanimi varnostnimi organi vodi obiske prostorov upravičencev ali podizvajalcev, da preveri, ali so varnostne zahteve za obravnavo tajnih podatkov EU izpolnjene.

VODIČ PO STOPNJAH TAJNOSTI

31. Seznam vseh elementov sporazuma o donaciji, ki so označeni za tajne ali jih je treba za tajne označiti med izvajanjem sporazuma o donaciji, pravila za to in določitev stopenj tajnosti, ki se uporabljajo, so vključeni v vodiču po stopnjah tajnosti. Vodič po stopnjah tajnosti je sestavni del tega sporazuma o donaciji in je na voljo v Dodatku B te priloge.

Dodatek B

VODIČ PO STOPNJAH TAJNOSTI

[specifično besedilo, ki se prilagodi glede na predmet sporazuma o donaciji]

Dodatek C

ZAPROSILO ZA NAJAVO OBISKA (VZOREC)

PODROBNA NAVODILA ZA IZPOLNJEVANJE ZAPROSILA ZA NAJAVO OBISKA

(Zaprosilo se vloži samo v angleškem jeziku.)

HEADING	Obkljukajte polja za vrsto obiska in vrsto podatkov ter navedite število lokacij, ki se obiščejo, in število obiskovalcev.
4. **ADMINISTRATIVE DATA**	Izpolni nacionalni varnostni organ / imenovani varnostni organ, ki je vložil zahtevek.
5. **REQUESTING ORGANISATION OR INDUSTRIAL FACILITY**	Navedite polno ime in poštni naslov. Po potrebi vključite mesto, državo in poštno številko.
6. **ORGANISATION OR INDUSTRIAL FACILITY TO BE VISITED**	Navedite polno ime in poštni naslov. Vključite mesto, državo, poštno številko, številko teleksa ali telefaksa (če je primerno), telefonsko številko in elektronski naslov. Navedite ime in telefonsko številko / številko telefaksa ter elektronski naslov vaše glavne kontaktne točke ali osebe, s katero ste se dogovorili za obisk. Pripombe: 1) Navedba pravilne poštne številke je pomembna, saj ima lahko podjetje več objektov. 2) Pri ročni vložitvi zahtevka se lahko Priloga 1 uporabi, če se v zvezi z isto zadevo obiščeta dva ali več objektov. Če se uporabi priloga, je treba v točki 3 navesti: „GLEJ PRILOGO 1, ŠT. OBJEKTOV“ (navedite število objektov).
7. **DATES OF VISIT**	Navedite dejanski datum ali obdobje (od–do) obiska v obliki „dan - mesec - leto“. Če je primerno, v oklepajih navedite nadomesten datum ali obdobje.
8. **TYPE OF INITIATIVE**	Navedite, ali je pobudo za obisk dala organizacija oziroma objekt, ki je vložil zahtevek, ali pa je podlaga za obisk vabilo objekta, ki se obišče.
9. **THE VISIT RELATES TO:**	Navedite polno ime projekta, pogodbe ali razpisa za zbiranje ponudb, pri čemer uporabite samo okrajšave v splošni uporabi.
10. **SUBJECT TO BE DISCUSSED/ JUSTIFICATION**	Na kratko opišite razloge za obisk. Ne uporabljajte nepojasnjenih okrajšav. Pripombe: V primeru ponavljajočih se obiskov bi morala ta postavka vsebovati navedbo „Ponavljajoči se obiski“ kot prve besede v podatkovnem elementu (npr. Ponavljajoči se obiski za razpravo o___).
11. **ANTICIPATED LEVEL OF CLASSIFIED INFORMATION TO BE INVOLVED**	Navedite SECRET UE/EU SECRET (S-UE/EU-S) ali CONFIDENTIEL UE/EU CONFIDENTIAL (C-UE/EU-C), kot je ustrezno.

12. **PARTICULARS OF VISITOR**	Pripomba: če se obiska udeležita več kot dva obiskovalca, je treba uporabiti Prilogo 2.
13. **THE SECURITY OFFICER OF THE REQUESTING ENTITY**	V tej postavki se navedejo ime, telefonska številka, številka telefaksa in elektronski naslov uradnika za varnost objekta, ki je vložil zahtevek.
14. **CERTIFICATION OF SECURITY CLEARANCE**	To polje izpolni organ za potrjevanje. Opombe za organ za potrjevanje: a. navedite ime, naslov, telefonsko številko, številko telefaksa in elektronski naslov (lahko predhodno natisnete); b. to postavko je treba podpisati in žigosati (če je primerno).
15. **REQUESTING SECURITY AUTHORITY**	To polje izpolni nacionalni varnostni organ / imenovani varnostni organ. Opomba za nacionalni varnostni organ / imenovani varnostni organ: a. navedite ime, naslov, telefonsko številko, številko telefaksa in elektronski naslov (lahko predhodno natisnete); b. to postavko je treba podpisati in žigosati (če je primerno).

Izpolniti je treba vsa polja in obrazec predložiti prek medvladnih kanalov ([9]).

ZAPROSILO ZA NAJAVO OBISKA

(VZOREC)

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]) Če je bilo dogovorjeno, da se lahko obiski, ki vključujejo dostop ali potencialen dostop do tajnih podatkov EU stopnje tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL in SECRET UE/EU SECRET, organizirajo neposredno, se lahko izpolnjeni obrazec predloži neposredno varnostnemu uradniku objekta, ki se obišče.

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):**

<Vstavi se sklic na veljavno zakonodajo o osebnih podatkih in povezava na obvezne informacije, ki jih je treba predložiti posamezniku, na katerega se nanašajo podatki, npr. kako se izvaja člen 13 Splošne uredbe o varstvu podatkov ([10]).>

([10]) Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL L 119, 4.5.2016, str. 1).

PRILOGA 1 k OBRAZCU ZAPROSILA ZA NAJAVO OBISKA

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)***

<Vstavi se sklic na veljavno zakonodajo o osebnih podatkih in povezava na obvezne informacije, ki jih je treba predložiti posamezniku, na katerega se nanašajo podatki, npr. kako se izvaja člen 13 Splošne uredbe o varstvu podatkov ([11]).>

([11]) Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL L 119, 4.5.2016, str. 1).

PRILOGA 2 k OBRAZCU ZAPROSILA ZA NAJAVO OBISKA

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)***

<Vstavi se sklic na veljavno zakonodajo o osebnih podatkih in povezava na obvezne informacije, ki jih je treba predložiti posamezniku, na katerega se nanašajo podatki, npr. kako se izvaja člen 13 Splošne uredbe o varstvu podatkov ([12]).>

([12]) Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL L 119, 4.5.2016, str. 1).

Dodatek D

INFORMACIJSKI LIST ZA VARNOSTNO DOVOLJENJE ORGANIZACIJE (FSCIS) (VZOREC)

1. **UVOD**

1.1 Priložen je vzorec informacijskega lista za varnostno dovoljene organizacije za hitro izmenjavo informacij med nacionalnim varnostnim organom ali imenovanim varnostnim organom, drugimi pristojnimi nacionalnimi varnostnimi organi in Varnostnim organom Komisije (v imenu organov, ki dodelijo donacijo) v zvezi z varnostnim dovoljenjem organizacije za objekt, ki sodeluje pri prošnjah za tajne donacije ali podizvajanje in pri njihovem izvajanju.

1.2 Informacijski list za varnostno dovoljenje organizacije je veljaven le, če je opremljen z žigom ustreznega nacionalnega varnostnega organa, imenovanega varnostnega organa ali drugega pristojnega organa.

1.3 Informacijski list za varnostno dovoljenje organizacije je razdeljen na oddelka za zahtevke in odgovore ter se lahko uporablja za zgoraj opredeljene namene ali katere koli druge namene, za katere se za določen objekt zahteva varnostno dovoljenje organizacije. Razlog za poizvedbo mora nacionalni varnostni organ ali imenovani varnostni organ, ki je vložil zahtevek, navesti v polju 7 oddelka za zahtevke.

1.4 Podatki, navedeni v informacijskem listu za varnostno dovoljene organizacije, običajno niso tajni; če je treba informacijski list pošiljati med zadevnimi nacionalnimi varnostnimi organi, imenovanimi varnostnimi organi in Komisijo, se to po možnosti izvaja prek elektronskih sredstev.

1.5 Nacionalni varnostni organi / imenovani varnostni organi morajo storiti vse, kar je v njihovi moči, da na zahtevo iz informacijskega lista za varnostno dovoljenje organizacije odgovorijo v desetih delovnih dneh.

1.6 V primeru prenosa tajnih podatkov, dodelitve donacije ali oddaje v podizvajanje v zvezi s tem zagotovilom, je treba o tem obvestiti nacionalni varnostni organ ali imenovani varnostni organ.

Postopki in navodila za uporabo informacijskega lista za varnostno dovoljenje organizacije

Ta podrobna navodila so namenjena nacionalnemu varnostnemu organu ali imenovanemu varnostnemu organu ali organu, ki dodeli donacijo, in Varnostnemu organu Komisije, ki izpolnjuje informacijski list za varnostno dovoljenje organizacije. Zaželeno je, da se zahtevek izpolni z velikimi tiskanimi črkami.

GLAVA	Vložnik zahtevka vpiše polni naziv nacionalnega varnostnega organa / imenovanega varnostnega organa in ime države.
1. **VRSTA ZAHTEVKA**	Organ, ki dodeli donacijo in vlaga zahtevo, izbere ustrezno potrditveno polje za vrsto zahtevka FSCIS. Vključi se zahtevana stopnja tajnosti varnostnega dovoljenja. Uporabiti je treba naslednje okrajšave: SECRET UE/EU SECRET = S-UE/EU-S CONFIDENTIEL UE/EU CONFIDENTIAL = C-UE/EU-C KIS = komunikacijski in informacijski sistemi za obdelavo tajnih podatkov
2. **PODROBNOSTI O TEMI**	Polja od 1 do 6 ne zahtevajo posebne razlage. V polju 4 se uporabi standardna dvočrkovna koda države. Polje 5 ni obvezno.
3. **RAZLOG ZA ZAHTEVEK**	Navedite specifični razlog za zahtevek, kazalnike projekta, številko razpisa ali donacije. Navedite potrebo po zmogljivosti za hrambo, stopnjo tajnosti KIS itd. Vključiti bi bilo treba vse roke / datume izteka / datume sklenitve, ki bi lahko vplivali na izdajo varnostnega dovoljenja organizacije.

4. **NACIONALNI VARNOSTNI ORGAN / IMENOVANI VARNOSTNI ORGAN, KI JE VLOŽIL ZAHTEVEK**	Navedite ime dejanskega vložnika zahtevka (v imenu NVO/IVO) in datum zahtevka (s številkami) (dd/mm/llll).
5. **ODDELEK ZA ODGOVOR**	Polja 1–5: izberite ustrezna polja. Polje 2: če poteka postopek za izdajo varnostnega dovoljenja organizacije, se priporoča, da se vložniku zahtevka okvirno navede zahtevani čas obdelave (če je znan). Polje 6: a) čeprav se potrditev razlikuje po državah ali celo po objektu, se priporoča, da se navede datum izteka veljavnosti varnostnega dovoljenja organizacije; b) če je datum izteka veljavnosti zagotovila za varnostno dovoljenje organizacije nedoločen, se lahko to polje prečrta; c) v skladu z ustreznimi nacionalnimi pravili in predpisi je za zahtevek za podaljšanje varnostnega dovoljenja organizacije odgovoren naročnik ali upravičenec oziroma podizvajalec.
6. **PRIPOMBE**	Na tem mestu se lahko navedejo dodatne informacije v zvezi z varnostnim dovoljenjem organizacije, objektom ali prej navedenimi postavkami.
7. **NVO/IVO, KI JE IZDAL DOVOLJENJE**	Navedite ime organa izdajatelja (v imenu NVO/IVO) in datum odgovora (s številkami) (dd/mm/llll).

INFORMACIJSKI LIST ZA VARNOSTNO DOVOLJENJE ORGANIZACIJE (FSCIS) (VZOREC)

Izpolniti je treba vsa polja in obrazec predložiti prek medvladnih kanalov oziroma kanalov med vladami in mednarodnimi organizacijami.

ZAHTEVEK ZA ZAGOTOVILO ZA VARNOSTNO DOVOLJENJE ORGANIZACIJE

PRI/V: _____

(ime države NVO/IVO)

Izpolnite polja za odgovor, če je primerno:

[...] Potrdite zagotovilo za varnostno dovoljenje organizacije na stopnji tajnosti: [ ] S-UE/EU-S [ ] C-UE/EU-C

za spodaj navedeni objekt

[...] vključno z varovanjem tajnega gradiva/podatkov

[...] vključno s komunikacijskimi in informacijski sistemi (KIS) za obdelavo tajnih podatkov

[...] Neposredno ali na ustrezno zahtevo upravičenca ali podizvajalca začnite postopek pridobivanja FSC do vključno stopnje tajnosti ....., pri čemer sta zagotovljeni stopnja varovanja ..... in stopnja KIS ....., če objekt trenutno nima zmožnosti na teh stopnjah.

Potrdite točnost podatkov spodaj navedenega objekta in po potrebi zagotovite popravke/dodatke.

1. Polno ime objekta:	Popravki/dodatki:
.....	.....
2. Polni naslov objekta:	
.....	.....
3. Poštni naslov (če je različen od naslova v točki 2)	
.....	.....
4. Poštna številka / mesto / država	
.....	.....
5. Ime uradnika za varnost	
.....	
.....	
6. Telefon/Telefaks/E-naslov uradnika za varnost	
.....	.....

7. Ta zahtevek je podan iz naslednjih razlogov: (navedite podrobnosti o fazi pred sklenitvijo pogodbe (zbiranje predlogov), sporazumu o donaciji ali podizvajalski pogodbi, programu/projektu itd.)

.....

Naročnik v okviru NVO/PVO/organa, ki dodeli donacijo, ki je vložil zahtevek: Ime: .....

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

ODGOVOR (v desetih delovnih dneh)

S tem potrjujemo, da:

1. [...] ima zgoraj navedeni objekt varnostno dovoljenje organizacije do vključno stopnje tajnosti [...] S-UE/EU-S.

   [ ] C-UE/EU-C.

2. Zgoraj navedeni objekt ima zmožnost varovanja tajnih podatkov/gradiva:

   [ ] da, stopnja tajnosti: ..... [ ] ne.

3. Zgoraj navedeni objekt ima akreditiran/potrjen KIS:

   [ ] da, stopnja tajnosti: ..... [ ] ne.

4. [...] v zvezi z zgoraj navedenim zahtevkom se je začel postopek pridobitve varnostnega dovoljenja organizacije. Obvestili vas bomo, ko bo varnostno dovoljenje organizacije izdano ali zavrnjeno.

5. [...] zgoraj navedeni objekt nima varnostnega dovoljenja organizacije.

6. To zagotovilo za varnostno dovoljenje organizacije preneha veljati: ..... (*dd/mm/llll*) ali kakor sicer svetuje NVO/IVO. V primeru predhodne razveljavitve ali sprememb zgoraj navedenih informacij boste obveščeni.

7. Pripombe:
   .....

NVO/IVO, ki je izdal dovoljenje Ime:..... *Datum:(dd/mm/llll)* .....

<Vstavi se sklic na veljavno zakonodajo o osebnih podatkih in povezava na obvezne informacije, ki jih je treba predložiti posamezniku, na katerega se nanašajo podatki, npr. kako se izvaja člen 13 Splošne uredbe o varstvu podatkov ([13]).>

([13]) Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL L 119, 4.5.2016, str. 1).

Dodatek E

Minimalne zahteve za varovanje tajnih podatkov EU v elektronski obliki na stopnji tajnosti RESTREINT UE/EU RESTRICTED, ki se obravnavajo z upravičenčevimi komunikacijskimi in informacijskimi sistemi

Splošno

1. Upravičenec mora biti odgovoren za zagotovitev, da je varovanje podatkov stopnje tajnosti RESTREINT UE/EU RESTRICTED v skladu z minimalnimi varnostnimi zahtevami, določenimi v tej varnostni klavzuli, in vsemi drugimi dodatnimi zahtevami, ki mu jih svetuje organ, ki dodeli donacijo, ali, če je primerno, nacionalni varnostni organ (NVO) ali imenovani varnostni organ (IVO).

2. Upravičenec je odgovoren za izvajanje varnostnih zahtev, opredeljenih v tem dokumentu.

3. V tem dokumentu komunikacijski in informacijski sistem zajema vso opremo, ki se uporablja za obravnavanje, hranjenje in razpošiljanje tajnih podatkov EU, vključno z delovnimi postajami, tiskalniki, fotokopirnimi stroji, telefaksi, strežniki, sistemi upravljanja omrežja, krmilniki omrežij in krmilniki komunikacijskih kanalov, prenosnimi računalniki, notesniki, tabličnimi računalniki, pametnimi telefoni in odstranljivimi pomnilniki, kot so USB ključi, CD-ji, SD kartice itd.

4. Posebna oprema, kot so šifrirni izdelki, mora biti zaščitena v skladu z namenskimi varnostno-operativnimi postopki (SecOP).

5. Upravičenec mora vzpostaviti strukturo, odgovorno za varnostno upravljanje komunikacijskih in informacijskih sistemov, s katerimi se obravnavajo tajni podatki stopnje tajnosti RESTREINT UE/EU RESTRICTED, in imenovati uradnika za varnost, odgovornega za zadevni objekt.

6. Uporaba rešitev informacijske tehnologije (strojne opreme, programske opreme ali storitev) v zasebni lasti osebja upravičenca za hranjenje ali obdelavo podatkov stopnje tajnosti RESTREINT UE/EU RESTRICTED ni dovoljena.

7. Akreditacijo komunikacijskih in informacijskih sistemov upravičenca, s katerimi se obravnavajo podatki stopnje tajnosti RESTREINT UE/EU RESTRICTED, mora odobriti organ za varnostno akreditacijo zadevne države članice ali pa je treba pooblastilo za akreditacijo prenesti na upravičenčevega uradnika za varnost v skladu z nacionalnimi zakoni in predpisi.

8. Samo tisti podatki stopnje tajnosti RESTREINT UE/EU RESTRICTED, ki so šifrirani z uporabo odobrenih šifrirnih izdelkov, se lahko obravnavajo, hranijo ali razpošiljajo (prek žičnih ali brezžičnih sredstev) kot kateri koli drugi netajni podatki v okviru sporazuma o donaciji. Te šifrirne izdelke mora odobriti EU ali država članica.

9. Zunanji subjekti, ki se najamejo za vzdrževanje ali popravila, morajo biti pogodbeno zavezani k izpolnjevanju veljavnih določb za obravnavo tajnih podatkov stopnje tajnosti RESTREINT UE/EU RESTRICTED, kot je določeno v tem dokumentu.

10. Na zahtevo organa, ki dodeli donacijo, ali zadevnega nacionalnega varnostnega organa, imenovanega varnostnega organa ali organa za varnostno akreditacijo mora upravičenec predložiti dokazilo o skladnosti s klavzulo sporazuma o donaciji o pogodbeni varnosti. Če se za zagotovitev skladnosti s temi zahtevami zahtevata tudi revizija in inšpekcijski pregled postopkov in prostorov upravičenca, upravičenci dovolijo predstavnikom organa, ki dodeli donacijo, nacionalnemu varnostnemu organu, imenovanemu varnostnemu organu in/ali organu za varnostno akreditacijo ali ustreznemu varnostnemu organu EU, da izvede tako revizijo in inšpekcijski pregled.

Fizična varnost

11. Območja, na katerih se komunikacijski in informacijski sistem uporabljajo za prikaz, hrambo, obdelavo ali razpošiljanje podatkov stopnje tajnosti RESTREINT UE/EU RESTRICTED, ali območja, v katerih so strežniki, sistemi upravljanja omrežja, krmilniki omrežij in krmilniki komunikacijskih kanalov za te komunikacijske in informacijske sisteme, bi bilo treba vzpostaviti kot ločena in nadzorovana območja z ustreznim sistemom za nadzor dostopa. Dostop do teh ločenih in nadzorovanih območij bi moral biti omejen na posameznike s posebnim dovoljenjem. Brez poseganja v odstavek 8 je treba opremo, kot je opisana v odstavku 3, skladiščiti na takšnih ločenih in nadzorovanih območjih.

12. Vzpostaviti je treba varnostne mehanizme in/ali postopke, da se uredi vstavljanje ali priključitev odstranljivih računalniških nosilcev podatkov (kot so USB ključi, naprave za shranjevanje velikih količin podatkov ali bralno pisalni pomnilniki CD-RW) na komponente komunikacijskih in informacijskih sistemov.

Dostop do informacijskih in komunikacijskih sistemov

13. Dostop do upravičenčevih informacijskih in komunikacijskih sistemov, s katerimi se obravnavajo tajni podatki EU, je dovoljen na podlagi stroge potrebe po seznanitvi in pooblastitve osebja.

14. Vsi komunikacijski in informacijski sistemi morajo imeti posodobljene sezname pooblaščenih uporabnikov. Na začetku vsake obdelave je treba potrditi identiteto vseh uporabnikov.

15. Gesla, ki so del večine varnostnih ukrepov za identifikacijo in potrjevanje identitete, morajo biti dolga vsaj devet znakov in biti sestavljena iz črk, številk in „posebnih“ znakov (če sistem to dovoljuje). Gesla je treba spremeniti vsaj vsakih 180 dni. Če so bila nepooblaščeno razkrita ali razkrita nepooblaščenim osebam oziroma obstaja sum tovrstnega razkritja, jih je treba čim prej spremeniti.

16. Vsi komunikacijski in informacijski sistemi morajo imeti notranji nadzor dostopa, ki nepooblaščenim uporabnikom preprečuje dostop do podatkov stopnje tajnosti RESTREINT UE/EU RESTRICTED ali njihovo spreminjanje ter spreminjanje sistema in varnostnih zahtev. Odjava uporabnikov iz komunikacijskega in informacijskega sistema mora biti samodejna, če so njihovi terminali določen čas nedejavni, ali pa mora komunikacijski in informacijski sistem po 15 minutah nedejavnosti aktivirati z geslom zaščiten ohranjevalnik zaslona.

17. Vsakemu uporabniku komunikacijskega in informacijskega sistema se dodeli edinstven uporabniški račun in uporabniška identifikacijska koda (ID). Uporabniški računi se morajo samodejno zakleniti po najmanj petih zaporednih nepravilnih poskusih prijave.

18. Vsi uporabniki komunikacijskih in informacijskih sistemov morajo biti seznanjeni s svojimi odgovornostmi in postopki, ki jih je treba upoštevati pri varovanju podatkov stopnje tajnosti RESTREINT UE/EU RESTRICTED v komunikacijskih in informacijskih sistemih. Odgovornosti in postopki, ki jih je treba upoštevati, morajo biti dokumentirani in uporabniki morajo svojo seznanitev z njimi pisno potrditi.

19. Varnostno-operativni postopki morajo biti na voljo uporabnikom in sistemskim skrbnikom ter morajo vključevati opise varnostnih vlog in povezanega seznama nalog, navodil in načrtov.

Računovodstvo, revizija in odzivanje na incidente

20. Vsak dostop do komunikacijskega in informacijskega sistema je treba zabeležiti.

21. Evidentirati je treba naslednje dogodke:

    (a) vse poskuse prijave, ne glede na to, ali je bila prijava uspešna ali neuspešna;

    (b) odjavo (vključno z iztekom prijave, kadar se uporablja);

    (c) ustvarjanje, izbris ali spremembo dostopnih pravic;

    (d) ustvarjanje, izbris ali spremembo gesel.

22. Za vse navedene dogodke je treba sporočiti vsaj naslednje informacije:

    (a) vrsto dogodka;

    (b) uporabniško identifikacijsko kodo;

    (c) datum in čas;

    (d) identifikacijsko kodo naprave.

23. Računovodske evidence bi morale uradniku za varnost zagotavljati pomoč pri preverjanju morebitnih varnostnih incidentov. Uporabijo se lahko tudi v podporo morebitnim pravnim preiskavam v primeru varnostnega incidenta. Vse varnostne evidence je treba redno preverjati, da se ugotovijo morebitni varnostni incidenti. Računovodske evidence morajo biti zaščitene pred nepooblaščenim izbrisom ali spremembo.

24. Upravičenec mora imeti vzpostavljeno strategijo za odzivanje na varnostne incidente. Uporabnike in sistemske skrbnike je treba poučiti, kako se odzivati na incidente, kako jih prijaviti in kaj storiti v izrednih razmerah.

25. O nepooblaščenem razkritju ali sumu nepooblaščenega razkritja podatkov stopnje tajnosti RESTREINT UE/EU RESTRICTED je treba poročati organu, ki dodeli donacijo. Poročilo mora vsebovati opis zadevnih podatkov in opis okoliščin nepooblaščenega razkritja ali suma nepooblaščenega razkritja. Vse uporabnike komunikacijskih in informacijskih sistemov je treba ozavestiti o tem, kako poročati uradniku za varnost o dejanskem ali domnevnem varnostnem incidentu.

Povezovanje v mreže in medsebojne povezave

26. Če je upravičenčev komunikacijski in informacijski sistem, s katerim se obravnavajo podatki stopnje tajnosti RESTREINT UE/EU RESTRICTED, povezan s komunikacijskim in informacijskim sistemom, ki ni akreditiran, to znatno poveča grožnjo za varnost komunikacijskega in informacijskega sistema in varnost podatkov stopnje tajnosti RESTREINT UE/EU RESTRICTED, ki se obravnavajo s tem komunikacijskim in informacijskim sistemom. To vključuje internet in druge javne ali zasebne komunikacijske in informacijske sisteme, kot so na primer drugi komunikacijski in informacijski sistemi, ki so v lasti upravičenca ali podizvajalca. V tem primeru mora upravičenec izvesti oceno tveganja, da opredeli dodatne varnostne zahteve, ki jih je treba uveljavljati v okviru postopka varnostne akreditacije. Upravičenec organu, ki dodeli donacijo, in, če tako zahtevajo nacionalni zakoni in drugi predpisi, pristojnemu organu za varnostno akreditacijo, predloži izjavo o skladnosti, ki potrjuje, da so bili upravičenčevi komunikacijski in informacijski sistemi in povezane medsebojne povezave akreditirani za obravnavanje tajnih podatkov EU stopnje tajnosti RESTREINT UE/EU RESTRICTED.

27. Dostop na daljavo iz drugih sistemov do storitev lokalnega omrežja (npr. dostop na daljavo do elektronske pošte in sistemske podpore na daljavo) je prepovedan, razen če se izvajajo posebni varnostni ukrepi, s katerimi soglaša organ, ki dodeli donacijo, in če to zahtevajo nacionalni zakoni in drugi predpisi, ki jih odobri pristojni organ za varnostno akreditacijo.

Upravljanje konfiguracij

28. Na voljo in redno vzdrževana mora biti podrobna konfiguracija strojne in programske opreme, kot je navedeno v dokumentaciji o akreditaciji/odobritvi (vključno s sistemskimi in omrežnimi diagrami).

29. Upravičenčev uradnik za varnost mora izvajati preglede konfiguracij strojne in programske opreme, da zagotovi, da ni bila vgrajena nobena nedovoljena strojna ali programska oprema.

30. Spremembe konfiguracije upravičenčevega komunikacijskega in informacijskega sistema je treba oceniti z vidika varnosti, odobriti pa jih mora uradnik za varnost in, če to zahtevajo nacionalni zakoni in drugi predpisi, tudi organ za varnostno akreditacijo.

31. Sistem je treba vsaj enkrat na četrtletje pregledati, da se odkrijejo morebitne varnostne pomanjkljivosti. Namestiti in posodabljati je treba programsko opremo za odkrivanje zlonamerne programske opreme. Če je mogoče, bi morala imeti ta programska oprema nacionalno ali priznano mednarodno odobritev oziroma bi morala izpolnjevati splošno sprejete standarde.

32. Upravičenec mora pripraviti načrt neprekinjenega poslovanja. Vzpostaviti je treba postopke za varnostno kopiranje, da se obravnavajo:

    (a) pogostost varnostnega kopiranja;

    (b) zahteve za hrambo na kraju samem (ognjevarni vsebniki) ali zunaj objekta;

    (c) nadzor nad pooblaščenim dostopom do varnostnih kopij.

Čiščenje in uničenje

33. Za komunikacijske in informacijske sisteme ali nosilce podatkov, ki so kadar koli vsebovali podatke stopnje tajnosti RESTREINT UE/EU RESTRICTED, je treba pred uničenjem izvesti v nadaljevanju opisano čiščenje celotnega sistema ali nosilca:

(a) bliskovni pomnilnik (npr. USB ključi, SD kartice, polprevodniški diski, hibridni trdi diski) je treba prepisati vsaj trikrat in nato preveriti, da se zagotovi, da izvirne vsebine ni mogoče obnoviti, ali pa vsebino izbrisati z odobreno programsko opremo za izbris;

(b) magnetne medije (npr. trde diske) je treba prepisati ali razmagnetiti;

(c) optične medije (npr. CD-ji in DVD-ji) je treba razrezati ali razkrojiti;

(d) glede vseh drugih nosilcev podatkov se je treba o varnostnih zahtevah, ki morajo biti izpolnjene, posvetovati z organom, ki dodeli donacijo, ali po potrebi z nacionalnim varnostnim organom, imenovanim varnostnim organom ali organom za varnostno akreditacijo.

34. Z vseh medijev za shranjevanje podatkov je treba očistiti podatke stopnje tajnosti RESTREINT UE/EU RESTRICTED, preden se predajo kateremu koli subjektu, ki ni pooblaščen za dostop do podatkov stopnje tajnosti RESTREINT UE/EU RESTRICTED (npr. za vzdrževalna dela).

PRILOGA IV

Varnostna dovoljenja organizacij in dovoljenja za dostop do tajnih podatkov za upravičence ali podizvajalce, ki vključujejo tajne podatke stopnje RESTREINT UE/EU RESTRICTED, in nacionalni varnostni organi / imenovani varnostni organi, ki zahtevajo uradno obvestilo o tajnih sporazumih o donaciji s stopnjo tajnosti RESTREINT UE/EU RESTRICTED ([1])

Država članica	Varnostno dovoljenje organizacije		Uradno obvestilo o sporazumu o donaciji ali oddaji v podizvajanje, ki vključuje informacije R-UE/EU-R nacionalnemu varnostnemu organu in/ali imenovanemu varnostnemu organu		Dovoljenje za dostop do tajnih podatkov	
	DA	NE	DA	NE	DA	NE
Belgija		**X**		**X**		**X**
Bolgarija		**X**		**X**		**X**
Češka		**X**		**X**		**X**
Danska	**X**		**X**		**X**	
Nemčija		**X**		**X**		**X**
Estonija	**X**		**X**			**X**
Irska		**X**		**X**		**X**
Grčija	**X**			**X**	**X**	
Španija		**X**	**X**			**X**
Francija		**X**		**X**		**X**
Hrvaška		**X**	**X**			**X**
Italija		**X**	**X**			**X**
Ciper		**X**	**X**			**X**
Latvija		**X**		**X**		**X**
Litva	**X**		**X**			**X**
Luksemburg	**X**		**X**		**X**	
Madžarska		**X**		**X**		**X**
Malta		**X**		**X**		**X**
Nizozemska	**X** (samo za sporazume o donaciji in oddaji v podizvajanje v zvezi z obrambo)		**X** (samo za sporazume o donaciji in oddaji v podizvajanje v zvezi z obrambo)			**X**
Avstrija		**X**		**X**		**X**
Poljska		**X**		**X**		**X**

([1]) Te nacionalne zahteve za varnostna dovoljenja organizacij / dovoljenja za dostop do tajnih podatkov in uradno obveščanje o tajnih sporazumih o donaciji stopnje tajnosti RESTREINT UE/EU RESTRICTED, ne smejo nalagati nobenih dodatnih obveznosti drugim državam članicam ali upravičencem in podizvajalcem v njihovi pristojnosti.
Opomba: uradno obveščanje o sporazumih o donaciji, ki vključujejo podatke stopnje tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL in SECRET UE/EU SECRET, je obvezno.

Portugalska		**X**		**X**		**X**
Romunija		**X**		**X**		**X**
Slovenija	**X**		**X**			**X**
Slovaška	**X**		**X**			**X**
Finska		**X**		**X**		**X**
Švedska		**X**		**X**		**X**

PRILOGA V

SEZNAM ODDELKOV ORGANOV ZA NACIONALNO VARNOST / IMENOVANIH VARNOSTNIH ORGANOV, PRISTOJNIH ZA POSTOPKE V ZVEZI Z INDUSTRIJSKO VARNOSTJO

BELGIJA

National Security Authority
FPS Foreign Affairs
Rue des Petits Carmes 15
1000 Brussels

Tel. +32 25014542 (telefon sekretariata)

Faks +32 25014596

E-naslov: nvo-ans@diplobel.fed.be

BOLGARIJA

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

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

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

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

(Zgoraj navedeni pristojni organi izvajajo postopke varnostnega preverjanja za izdajo varnostnih dovoljenj organizacij pravnim subjektom, ki konkurirajo za sklenitev pogodbe s tajnimi podatki, in dovoljenj za dostop do tajnih podatkov posameznikom, ki izvajajo pogodbo s tajnimi podatki za potrebe teh organov.)

5. State Agency National Security (security service)

   45 Cherni Vrah Blvd.

   1407 Sofia

   Tel. +359 28147109

   Faks +359 29632188, +359 28147441

   E-naslov: dans@dans.bg

(Zgoraj navedena varnostna služba izvaja postopke varnostnega preverjanja za izdajanje varnostnih dovoljenj organizacij in dovoljenj za dostop do tajnih podatkov vsem drugim pravnim subjektom in posameznikom v državi, ki konkurirajo za sklenitev pogodbe s tajnimi podatki ali tajnega sporazuma o donaciji ali izvajajo pogodbo s tajnimi podatki ali tajni sporazum o donaciji.)

ČEŠKA

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

Tel. +420 257283129

E-naslov: sbr@nbu.cz

DANSKA

1. Politiets Efterretningstjeneste
   (Danish Security Intelligence Service)

   Klausdalsbrovej 1

   2860 Søborg

   Tel. +45 33148888

   Faks +45 33430190

2. Forsvarets Efterretningstjeneste
   (Danish Defence Intelligence Service)
   Kastellet 30
   2100 Copenhagen Ø

   Tel. +45 33325566

   Faks +45 33931320

NEMČIJA

1. V zvezi z zadevami, ki se nanašajo na politiko industrijske varnosti, varnostna dovoljenja organizacij, načrte prevoza (razen za šifrirni material / zaupne poslovne informacije):
   Federal Ministry for Economic Affairs and Energy

   Industrial Security Division – RS3

   Villemombler Str. 76

   53123 Bonn

   Tel. +49 228996154028

   Faks:+49 228996152676

   E-naslov: dsagermany-rs3@bmwi.bund.de (službeni elektronski naslov)

2. Za standardna zaprosila za najavo obiska v nemških podjetjih / iz nemških podjetij:

Federal Ministry for Economic Affairs and Energy

Industrial Security Division – RS2
Villemombler Str. 76
53123 Bonn

Tel. +49 228996152401

Faks +49 228996152603

E-naslov: rs2-international@bmwi.bund.de (službeni elektronski naslov)

3. Načrti prevoza šifrirnega materiala:

Federal Office for Information Security (BSI)
National Distribution Agency / NDA-EU DEU
Mainzer Str. 84
53179 Bonn

Tel. +49 2289995826052

Faks +49 228991095826052

E-naslov: 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-naslov: 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-naslov: nsa@dfa.ie

GRČIJA

Hellenic National Defence General Staff
E' Division (Security INTEL, CI BRANCH)
E3 Directorate
Industrial Security Office
227–231 Mesogeion Avenue
15561 Holargos, Athens

Tel. +30 2106572022, +30 2106572178

Faks +30 2106527612

E-naslov: daa.industrial@hndgs.mil.gr

ŠPANIJA

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

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

Faks +34 913725808

E-naslov: nsa-sp@areatec.com

Za podatke o zaupnih programih: programas.ons@areatec.com

Za zadeve v zvezi z dovoljenji za dostop do tajnih podatkov: hps.ons@areatec.com

Za načrte prevoza in mednarodne obiske: sp-ivtco@areatec.com

FRANCIJA

National Security Authority (NSA) (za politiko in izvajanje na področjih razen obrambne industrije)
Secrétariat général de la défense et de la sécurité nationale
Sous-direction Protection du secret (SGDSN/PSD)
51 boulevard de la Tour-Maubourg
75700 Paris 07 SP

Tel. +33 171758193

Faks +33 171758200

E-naslov: ANSFrance@sgdsn.gouv.fr

Designated Security Authority (za izvajanje v obrambni 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 Paris CEDEX 15

Tel. +33 988670421

E-naslov: za obrazce in zaprosila za najavo obiska ob pošiljanju: dga-ssdi.ai.fct@intradef.gouv.fr

za zaprosila za najavo obiska ob sprejemanju: dga-ssdi.visit.fct@intradef.gouv.fr

HRVAŠKA

Office of the National Security Council
Croatian NSA
Jurjevska 34
HR-10000 Zagreb

Tel. +385 14681222

Faks +385 14686049

E-naslov: NSACroatia@uvns.hr

ITALIJA

Presidenza del Consiglio dei Ministri
D.I.S. – U.C.Se.
Via di Santa Susanna 15
00187 Roma

Tel. +39 0661174266

Faks +39 064885273

CIPER

ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Λεωφόρος Στροβόλου, 172-174
Στρόβολος, 2048, Λευκωσία

Tel. +357 22807569, +357 22807764

Faks +357 22302351

E-naslov: 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-naslov: 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-naslov: 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-naslov: nsa@vsd.lt

LUKSEMBURG

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

Tel. +352 24782210

E-naslov: ans@me.etat.lu

MADŽARSKA

National Security Authority of Hungary
H-1399 Budapest P.O. Box 710/50
H-1024 Budapest, Szilágyi Erzsébet fasor 11/B

Tel. +36 13911862

Faks +36 13911889

E-naslov: 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-naslov: certification@mccaa.org.mt

NIZOZEMSKA

1. Ministry of the Interior and Kingdom Relations

   PO Box 20010
   2500 EA The Hague

   Tel. +31 703204400

   Faks +31 703200733

   E-naslov: nsa-nl-industry@minbzk.nl

2. Ministry of Defence

   Industrial Security Department

   PO Box 20701
   2500 ES The Hague

   Tel. +31 704419407

   Faks +31 703459189

   E-naslov: indussec@mindef.nl

AVSTRIJA

1. Federal Chancellery of Austria

   Department I/10, Office for Information Security

   Ballhausplatz 2
   10104 Vienna

   Tel. +43 153115202594

   E-naslov: isk@bka.gv.at

2. Imenovani varnostni organ na vojaškem področju:

   BMLVS/Abwehramt

   Postfach 2000
   1030 Vienna

   E-naslov: abwa@bmlvs.gv.at

POLJSKA

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

Tel. +48 225857944

Faks +48 225857443

E-naslov: nsa@abw.gov.pl

PORTUGALSKA

Gabinete Nacional de Segurança
Serviço de Segurança Industrial
Rua da Junqueira nº 69
1300-342 Lisbon

Tel. +351 213031710

Faks +351 213031711

E-naslov: sind@gns.gov.pt, franco@gns.gov.pt

ROMUNIJA

Oficiul Registrului Național al Informațiilor Secrete de Stat - ORNISS
Romanian NSA - ORNISS - National Registry Office for Classified Information
4th Mures Street
012275 Bucharest

Tel. +40 212075115

Faks +40 212245830

E-naslov: relatii.publice@orniss.ro, nsa.romania@nsa.ro

SLOVENIJA

Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
SI-1000 Ljubljana

Tel. +386 14781390

Faks +386 14781399

E-naslov: gp.uvtp@gov.si

SLOVAŠKA

Národný bezpečnostný úrad
(National Security Authority)
Security Clearance Department
Budatínska 30
851 06 Bratislava

Tel. +421 268691111

Faks +421 268691700

E-naslov: podatelna@nbu.gov.sk

FINSKA

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

E-naslov: 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-naslov: ud-nsa@gov.se

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