KOMISIJAS LĒMUMS (ES, Euratom) 2021/259

(2021. gada 10. februāris),

ar ko nosaka īstenošanas noteikumus industriālās drošības jomā attiecībā uz klasificētām dotācijām

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību un jo īpaši tā 249. pantu,

ņemot vērā Eiropas Atomenerģijas kopienas dibināšanas līgumu un jo īpaši tā 106. pantu,

ņemot vērā Eiropas Parlamenta un Padomes Regulu (ES, Euratom) 2018/1046 (2018. gada 18. jūlijs) par finanšu noteikumiem, ko piemēro Savienības vispārējam budžetam, ar kuru groza Regulas (ES) Nr. 1296/2013, (ES) Nr. 1301/2013, (ES) Nr. 1303/2013, (ES) Nr. 1304/2013, (ES) Nr. 1309/2013, (ES) Nr. 1316/2013, (ES) Nr. 223/2014, (ES) Nr. 283/2014 un Lēmumu Nr. 541/2014/ES un atceļ Regulu (ES, Euratom) Nr. 966/2012 ([1]),

ņemot vērā Komisijas Lēmumu (ES, Euratom) 2015/443 (2015. gada 13. marts) par drošību Komisijā ([2]),

ņemot vērā Komisijas Lēmumu (ES, Euratom) 2015/444 (2015. gada 13. marts) par drošības noteikumiem ES klasificētas informācijas aizsardzībai ([3]),

ņemot vērā Komisijas Lēmumu (ES, Euratom) 2017/46 (2017. gada 10. janvāris) par komunikācijas un informācijas sistēmu drošību Eiropas Komisijā ([4]),

pēc apspriešanās ar Komisijas drošības ekspertu grupu saskaņā ar Lēmuma (ES, Euratom) 2015/444 41. panta 5. punktu,

tā kā:

(1) Lēmuma (ES, Euratom) 2015/444 41., 42., 47. un 48. pantā ir noteikts, ka, lai papildinātu un atbalstītu minētā lēmuma 6. nodaļu, īstenošanas noteikumos industriālās drošības jomā ir jānosaka sīkāki noteikumi attiecībā uz tādiem jautājumiem kā klasificēti dotācijas nolīgumi, iestādes drošības pielaides, personāla drošības pielaides, apmeklējumi un Eiropas Savienības klasificētās informācijas (ESKI) pārsūtīšana un pārvietošana.

(2) Lēmumā (ES, Euratom) 2015/444 ir teikts, ka klasificētie dotācijas nolīgumi ir jāīsteno ciešā sadarbībā ar valsts drošības iestādi, izraudzīto drošības iestādi vai jebkuru citu attiecīgās dalībvalsts kompetento iestādi. Dalībvalstis ir vienojušās nodrošināt, ka visas struktūras to jurisdikcijā, kuras varētu saņemt vai radīt klasificētu informāciju, kas sagatavota Komisijā, ir saņēmušas atbilstošu drošības pielaidi un spēj nodrošināt pienācīgu aizsardzību, kas līdzvērtīga tai, kura paredzēta Eiropas Savienības Padomes drošības noteikumos atbilstošā līmenī klasificētas ES informācijas aizsardzībai, kā noteikts Padomē sanākušo Eiropas Savienības dalībvalstu nolīgumā par tādas klasificētās informācijas aizsardzību, ar kuru apmainās Eiropas Savienības interesēs (2011/C 202/05) ([5]).

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

(3) Padome, Komisija un Savienības Augstā pārstāve ārlietās un drošības politikas jautājumos ir vienojušies nodrošināt maksimālu konsekvenci drošības noteikumu piemērošanā ESKI aizsardzībai, vienlaikus ņemot vērā īpašās institucionālās un organizatoriskās vajadzības saskaņā ar deklarācijām, kas pievienotas Padomes tās sanāksmes protokolam, kurā tika pieņemts Padomes Lēmums 2013/488/ES ([6]) par drošības noteikumiem ES klasificētas informācijas aizsardzībai.

(4) Tāpēc arī Komisijas īstenošanas noteikumiem industriālās drošības jomā attiecībā uz klasificētām dotācijām būtu jānodrošina maksimāla konsekvence un tajos būtu jāņem vērā Pamatnostādnes par industriālo drošību, ko Padomes Drošības komiteja apstiprināja 2016. gada 13. decembrī.

(5) Komisija 2016. gada 4. maijā pieņēma lēmumu ([7]), ar ko pilnvaroja par drošības jautājumiem atbildīgo Komisijas locekli pieņemt Komisijas vārdā un tās atbildībā īstenošanas noteikumus, kuri paredzēti Lēmuma (ES, Euratom) 2015/444 60. pantā,

IR PIEŅĒMUSI ŠO LĒMUMU.

1. NODAĻA

VISPĀRĪGIE NOTEIKUMI

1. pants

Priekšmets un piemērošanas joma

1. Šajā lēmumā ir izklāstīti īstenošanas noteikumi industriālās drošības jomā attiecībā uz klasificētiem dotācijas nolīgumiem Lēmuma (ES, Euratom) 2015/444 un jo īpaši tā 6. nodaļas nozīmē.

2. Šajā lēmumā ir noteiktas īpašas prasības, kas nodrošina ES klasificētas informācijas (ESKI) aizsardzību, publicējot uzaicinājumus un piešķirot dotācijas, kā arī īstenojot klasificētos dotācijas nolīgumus, ko noslēgusi Eiropas Komisija.

3. Šo lēmumu piemēro dotācijām saistībā ar informāciju, kas klasificēta šādos līmeņos:

a) *RESTREINT UE/EU RESTRICTED*;

b) *CONFIDENTIEL UE/EU CONFIDENTIAL*;

c) *SECRET UE/EU SECRET*.

4. Šo lēmumu piemēro, neskarot īpašos noteikumus, kas paredzēti citos tiesību aktos, piemēram, attiecībā uz Eiropas aizsardzības rūpniecības attīstības programmu.

2. pants

Atbildība Komisijā

1. Eiropas Parlamenta un Padomes Regulā (ES, Euratom) 2018/1046 minētās piešķīrējas iestādes kredītrīkotāja pienākumi ietver arī to, ka kredītrīkotājs nodrošina, ka klasificētā dotācija atbilst Lēmumam (ES, Euratom) 2015/444 un tā īstenošanas noteikumiem.

([6]) Padomes Lēmums 2013/488/ES (2013. gada 23. septembris) par drošības noteikumiem ES klasificētas informācijas aizsardzībai (OV L 274, 15.10.2013., 1. lpp.).

([7]) Komisijas 2016. gada 4. maija Lēmums par pilnvarojumu drošības jomā (C(2016) 2797 final).

2. Šajā saistībā attiecīgais kredītrīkotājs visos posmos konsultējas ar Komisijas drošības iestādi par jautājumiem, kas saistīti ar klasificēta dotācijas nolīguma, programmas vai projekta drošības elementiem, un informē vietējo drošības speciālistu par noslēgtajiem klasificētajiem dotācijas nolīgumiem. Lēmumu par konkrēto subjektu klasifikācijas līmeni pieņem piešķīrēja iestāde, pienācīgi ņemot vērā drošības klasifikācijas rokasgrāmatā izklāstīto.

3. Ja piemēro 5. panta 3. punktā minētās programmas vai projekta drošības instrukcijas, piešķīrēja iestāde un Komisijas drošības iestāde pilda pienākumus, kas tām uzticēti minētajās instrukcijās.

4. Pildot šo īstenošanas noteikumu prasības, Komisijas drošības iestāde cieši sadarbojas ar attiecīgo dalībvalstu valsts drošības iestādēm (VDI) un izraudzītajām drošības iestādēm (IDI), jo īpaši attiecībā uz iestādes drošības pielaidēm (IDP) un personāla drošības pielaidēm (PDP), apmeklējumu procedūrām un transportēšanas plāniem.

5. Ja dotācijas pārvalda ES izpildaģentūras vai citas finansēšanas struktūras un 1. panta 4. punktā minētajos citos tiesību aktos paredzētos īpašos noteikumus nepiemēro:

a) deleģējošais Komisijas dienests īsteno autora tiesības attiecībā uz ESKI, kura radīta saistībā ar dotācijām, ja to paredz deleģēšanas kārtība;

b) deleģējošais Komisijas dienests atbild par drošības klasifikācijas noteikšanu;

c) drošības pielaides informācijas pieprasījumus un paziņojumus VDI un/vai IDI nosūta ar Komisijas drošības iestādes starpniecību.

2. NODAĻA

UZAICINĀJUMU IESNIEGT PRIEKŠLIKUMUS ATTIECĪBĀ UZ KLASIFICĒTĀM DOTĀCIJĀM APSTRĀDE

3. pants

Pamatprincipi

1. Dotāciju klasificētās daļas īsteno tikai labuma guvēji, kas reģistrēti dalībvalstī, vai labuma guvēji, kuri reģistrēti trešā valstī vai kurus izveidojusi starptautiska organizācija, ja šī trešā valsts vai starptautiskā organizācija ir noslēgusi informācijas drošības nolīgumu ar Savienību vai administratīvu vienošanos ar Komisiju ([8]).

2. Pirms piešķīrēja iestāde publicē uzaicinājumu saistībā ar klasificētu dotāciju, tā nosaka drošības klasifikācijas līmeni informācijai, kuru varētu sniegt pieteikuma iesniedzējiem. Piešķīrēja iestāde nosaka arī maksimālo drošības klasifikācijas līmeni visai informācijai, kas tiek izmantota vai radīta dotācijas nolīguma, programmas vai projekta izpildes ietvaros, vai vismaz to, kāds ir tās informācijas apjoms un veids, kuru ir paredzēts sagatavot vai ar kuru ir paredzēts rīkoties, un vai ir nepieciešama klasificēta komunikācijas un informācijas sistēma (KIS).

3. Piešķīrēja iestāde nodrošina, ka uzaicinājumos saistībā ar klasificētiem dotācijas nolīgumiem ir sniegta informācija par īpašiem drošības pienākumiem saistībā ar klasificētu informāciju. Uzaicinājuma dokumentācijā iekļauj precizējumus par grafiku, kādā labuma guvēji var saņemt IDP, ja tas ir nepieciešams. Lēmuma I un II pielikumā ir iekļautas veidnes informācijai par uzaicinājuma nosacījumiem.

([8]) To ES noslēgto nolīgumu un Eiropas Komisijas noslēgto administratīvo vienošanos saraksts, saskaņā ar kuriem var veikt ES klasificētās informācijas apmaiņu ar trešām valstīm un starptautiskām organizācijām, ir pieejams Komisijas tīmekļa vietnē.

4. Piešķirēja iestāde nodrošina, ka informācija, kas klasificēta *RESTREINT UE/EU RESTRICTED*, *CONFIDENTIEL UE/EU CONFIDENTIAL* un *SECRET UE/EU SECRET* līmenī, tiek izpausta pieteikuma iesniedzējiem tikai pēc tam, kad tie ir parakstījuši nolīgumu par informācijas neizpaušanu, kas uzliek pieteikuma iesniedzējiem par pienākumu rīkoties ar ESKI un aizsargāt to saskaņā ar Lēmumu (ES, Euratom) 2015/444, tā īstenošanas noteikumiem un piemērojamiem valsts noteikumiem.

5. Ja pieteikuma iesniedzējiem tiek sniegta *RESTREINT UE/EU RESTRICTED* informācija, šā lēmuma 5. panta 7. punktā minētās minimālās prasības iekļauj uzaicinājumā vai informācijas neizpaušanas kārtībā, ko noslēdz priekšlikumu iesniegšanas posmā.

6. Visiem pieteikumu iesniedzējiem un labuma guvējiem, kuriem ir jārīkojas ar informāciju, kas klasificēta *CONFIDENTIEL UE/EU CONFIDENTIAL* vai *SECRET UE/EU SECRET* līmenī, vai šāda informācija jāglabā savās telpās vai nu priekšlikumu iesniegšanas posmā, vai arī paša klasificētā dotācijas nolīguma izpildes laikā, ir vajadzīgā līmeņa IDP, izņemot 9. punktā minētos gadījumus. Tālāk ir izklāstīti trīs scenāriji, kādi var rasties priekšlikumu iesniegšanas posmā klasificētai dotācijai saistībā ar ESKI, kura klasificēta *CONFIDENTIEL UE/EU CONFIDENTIAL* vai *SECRET UE/EU SECRET* līmenī:

a) priekšlikumu iesniegšanas posmā ESKI, kas klasificēta *CONFIDENTIEL UE/EU CONFIDENTIAL* vai *SECRET UE/EU SECRET* līmenī, nav pieejama.

   Ja uzaicinājums attiecas uz dotāciju, kas būs saistīta ar ESKI, kura klasificēta *CONFIDENTIEL UE/EU CONFIDENTIAL* vai *SECRET UE/EU SECRET* līmenī, bet pieteikuma iesniedzējam nav jārīkojas ar šādu informāciju priekšlikumu iesniegšanas posmā, pieteikuma iesniedzēju, kuram nav vajadzīgā līmeņa IDP, neizslēdz no priekšlikumu iesniegšanas procesa, pamatojoties uz to, ka tam nav IDP;

b) priekšlikumu iesniegšanas posmā ESKI, kas klasificēta *CONFIDENTIEL UE/EU CONFIDENTIAL* vai *SECRET UE/EU SECRET* līmenī, ir pieejama piešķirējas iestādes telpās.

   Piekļuvi sniedz pieteikuma iesniedzēja darbiniekiem, kuriem ir vajadzīgā līmeņa PDP un kuriem ir vajadzība pēc šīs informācijas;

c) priekšlikumu iesniegšanas posmā ar ESKI, kas klasificēta *CONFIDENTIEL UE/EU CONFIDENTIAL* vai *SECRET UE/EU SECRET* līmenī, rīkojas vai to glabā pieteikuma iesniedzēja telpās.

   Ja uzaicinājumā ir noteikts, ka pieteikuma iesniedzējiem ir jārīkojas ar ESKI vai tā ir jāglabā to telpās, attiecīgajam pieteikuma iesniedzējam ir jābūt saņēmušam vajadzīgā līmeņa IDP. Šādos apstākļos piešķirēja iestāde ar Komisijas drošības iestādes starpniecību pārliecinās pie attiecīgās VDI vai IDI, ka pieteikuma iesniedzējam ir piešķirta atbilstoša IDP, pirms pieteikuma iesniedzējam tiek nodoti jebkādi ESKI materiāli. Piekļuvi sniedz pieteikuma iesniedzēja darbiniekiem, kuriem ir vajadzīgā līmeņa PDP un kuriem ir vajadzība pēc šīs informācijas;

7. Parasti IDP vai PDP nav vajadzīga, lai priekšlikumu iesniegšanas posmā vai dotācijas nolīguma izpildes posmā piekļūtu informācijai, kas klasificēta *RESTREINT UE/EU RESTRICTED* līmenī. Ja dalībvalstis saskaņā ar saviem valsts normatīvajiem aktiem pieprasa IDP vai PDP attiecībā uz dotācijas nolīgumiem vai apakšlīgumiem, kas klasificēti *RESTREINT UE/EU RESTRICTED* līmenī, kā noteikts IV pielikumā, šīs valsts prasības neuzliek papildu pienākumus citām dalībvalstīm un pieteikuma iesniedzēji, labuma guvēji vai apakšuzņēmēji no dalībvalstīm, kurās piekļuvei informācijai, kas klasificēta *RESTREINT UE/EU RESTRICTED* līmenī, nepiemēro IDP vai PDP prasību, netiek izslēgti no dalības attiecīgajos dotācijas nolīgumos vai apakšlīgumos vai pašā konkursā. Šādi dotācijas nolīgumi tiek pildīti dalībvalstīs saskaņā ar valsts normatīvajiem aktiem.

8. Ja uzaicinājuma apstrādes vai klasificēta dotācijas nolīguma īstenošanas nolūkā ir vajadzīga IDP, piešķirēja iestāde ar Komisijas drošības iestādes starpniecību iesniedz labuma guvēja VDI vai IDI pieprasījumu, izmantojot iestādes drošības pielaides informācijas lapu (IDPIL). Lēmuma III pielikuma D papildinājumā ir sniegts IDPIL piemērs ([9]). Ja iespējams, atbildi uz IDPIL sniedz desmit darba dienās no šāda pieprasījuma saņemšanas dienas.

9. Ja dalībvalsts valdības iestādes vai iestādes, kas atrodas valdības kontrolē, piedalās klasificētās dotācijās, kurām nepieciešama IDP, un ja saskaņā ar valsts tiesību aktiem šīm iestādēm netiek izsniegta IDP, piešķirēja iestāde ar Komisijas drošības iestādes starpniecību pārbauda attiecīgajā VDI vai IDI, vai minētās valsts iestādes spēj rīkoties ar ESKI vajadzīgajā līmenī.

([9]) Citu izmantoto veidlapu struktūra var atšķirties no šajos īstenošanas noteikumos sniegtā parauga.

10. Ja klasificēta dotācijas nolīguma izpildei ir vajadzīga PDP un ja saskaņā ar valsts noteikumiem pirms PDP piešķiršanas ir vajadzīga IDP, piešķirēja iestāde ar Komisijas drošības iestādes starpniecību, izmantojot IDPIL, pārbauda pie labuma guvēja VDI vai IDI, vai labuma guvējam ir IDP vai notiek IDP piešķiršanas process. Šajā gadījumā Komisija neizdod PDP pieprasījumus, izmantojot personāla drošības pielaides informācijas lapu ("PDPIL").

4. pants

Apakšlīgumu slēgšana klasificētu dotāciju gadījumā

1. Nosacījumus, saskaņā ar kuriem labuma guvēji var slēgt apakšlīgumus par darbības uzdevumiem, kas saistīti ar ESKI, nosaka uzaicinājumā un dotācijas nolīgumā. Šie nosacījumi ietver prasību, ka visas IDPIL iesniedz ar Komisijas drošības iestādes starpniecību. Apakšlīgumu slēgšanai ir vajadzīga piešķirējas iestādes iepriekšēja rakstiska piekrišana. Attiecīgā gadījumā apakšlīgumu slēgšana atbilst programmas izveides pamataktam.

2. Par dotāciju klasificētajām daļām apakšlīgumu var noslēgt tikai ar subjektiem, kas reģistrēti dalībvalstī, vai subjektiem, kas reģistrēti trešā valstī vai kurus izveidojusi starptautiska organizācija, ja šī trešā valsts vai starptautiskā organizācija ir noslēgusi informācijas drošības nolīgumu ar Savienību vai administratīvu vienošanos ar Komisiju ([10]).

3. NODAĻA

KLASIFICĒTU DOTĀCIJU APSTRĀDE

5. pants

Pamatprincipi

1. Piešķirot klasificētu dotāciju, piešķirēja iestāde kopā ar Komisijas drošības iestādi nodrošina, ka labuma guvēju pienākumi attiecībā uz tādas ESKI aizsardzību, ko izmanto vai kas radīta, pildot dotācijas nolīgumu, ir dotācijas nolīguma neatņemama daļa. Uz dotāciju attiecināmas drošības prasības noformē drošības aspektu vēstules (DAV) veidā. DAV veidnes paraugs ir sniegts III pielikumā.

2. Pirms klasificēta dotācijas nolīguma parakstīšanas piešķirēja iestāde apstiprina drošības klasifikācijas rokasgrāmatu (DKR) par dotācijas īstenošanas gaitā vai – attiecīgā gadījumā – programmas vai projekta līmenī veicamajiem uzdevumiem un radīto informāciju. DKR ir DAV daļa.

3. Uz programmu vai projektu attiecināmas īpašas drošības prasības noformē programmas (vai projekta) drošības instrukcijas (PDI) veidā. PDI var sagatavot, izmantojot III pielikumā sniegtās DAV veidnes noteikumus. PDI izstrādā Komisijas departaments, kas vada programmu vai projektu, ciešā sadarbībā ar Komisijas drošības iestādi, un tā tiek iesniegta Komisijas drošības ekspertu grupai piezīmju sniegšanai. Ja dotācijas nolīgums ir tādas programmas vai projekta daļa, kuram ir savs PDI, dotācijas nolīguma DAV noformē vienkāršotā veidā un tajā ietver atsauci uz drošības noteikumiem, kas izklāstīti minētās programmas vai projekta PDI.

4. Izņemot 3. panta 9. punktā minētos gadījumus, klasificētu dotācijas nolīgumu neparaksta, kamēr pieteikuma iesniedzēja VDI vai IDI nav apstiprinājusi pieteikuma iesniedzēja IDP vai, ja klasificēts dotācijas nolīgums ir piešķirts konsorcijam, kamēr konsorcija ietvaros vismaz viena pieteikuma iesniedzēja (vai, ja nepieciešams, vairāku pieteikuma iesniedzēju) VDI vai IDI nav apstiprinājusi minētā pieteikuma iesniedzēja IDP.

5. Principā, ja vien citos attiecīgajos noteikumos nav paredzēts citādi, piešķirēju iestādi uzskata par tās ESKI autoru, kas radīta, pildot dotācijas nolīgumu.

([10]) To ES noslēgto nolīgumu un Eiropas Komisijas noslēgto administratīvo vienošanos saraksts, saskaņā ar kuriem var veikt ES klasificētās informācijas apmaiņu ar trešām valstīm un starptautiskām organizācijām, ir pieejams Komisijas tīmekļa vietnē.

6. Piešķirēja iestāde ar Komisijas drošības iestādes starpniecību paziņo visu labuma guvēju un apakšuzņēmēju VDI un/vai IDI par klasificēta dotācijas nolīguma vai apakšlīguma noslēgšanu un par šādu dotācijas nolīgumu vai apakšlīgumu termiņa pagarināšanu vai pirmstermiņa izbeigšanu. Valstu prasību saraksts ir sniegts IV pielikumā.

7. dotācijas nolīgumos, kas saistīti ar informāciju, kura klasificēta *RESTREINT UE/EU RESTRICTED* līmenī, ietver drošības klauzulu, ar ko III pielikuma E papildinājumā izklāstītos noteikumus padara saistošus labuma guvējiem. Šajos dotācijas nolīgumos iekļauj DAV, kurā izklāstītas vismaz prasības attiecībā uz rīkošanos ar informāciju, kas klasificēta *RESTREINT UE/EU RESTRICTED* līmenī, ietverot informācijas apliecināšanas aspektus un īpašas prasības, kas jāizpilda labuma guvējiem attiecībā uz tās KIS akreditāciju, kurā rīkojas ar informāciju, kas klasificēta *RESTREINT UE/EU RESTRICTED* līmenī.

8. Ja tas paredzēts dalībvalstu valsts normatīvajos aktos, VDI vai IDI nodrošina, ka labuma guvēji vai apakšuzņēmēji to jurisdikcijā ievēro piemērojamos drošības noteikumus par tādas informācijas aizsardzību, kas klasificēta *RESTREINT UE/EU RESTRICTED* līmenī, un veic pārbaudes apmeklējumus labuma guvēju vai apakšuzņēmēju objektos, kas atrodas to teritorijā. Ja VDI vai IDI nav šāda pienākuma, piešķirēja iestāde nodrošina, ka labuma guvējs īsteno nepieciešamās drošības prasības, kas izklāstītas III pielikuma E papildinājumā.

6. pants

Labuma guvēju un apakšuzņēmēju darbinieku piekļuve ESKI

1. Piešķirēja iestāde nodrošina, ka klasificētajos dotācijas nolīgumos ir iekļauti noteikumi, kuros norādīts, ka labuma guvēja vai apakšuzņēmēja darbiniekiem, kuriem, lai izpildītu dotācijas nolīgumu vai apakšlīgumu, ir vajadzīga piekļuve ESKI, var piešķirt šādu piekļuvi vienīgi tad, ja:

a) ir konstatēts, ka viņiem ir vajadzība pēc šīs informācijas;

b) tādas informācijas gadījumā, kas klasificēta *CONFIDENTIEL UE/EU CONFIDENTIAL* vai *SECRET UE/EU SECRET* līmenī, attiecīgā VDI vai IDI vai cita kompetenta drošības iestāde viņiem ir piešķirusi attiecīga līmeņa drošības pielaidi;

c) viņi ir iepazīstināti ar ESKI aizsardzībai piemērojamiem drošības noteikumiem un ir apliecinājuši savus pienākumus saistībā ar šādas informācijas aizsargāšanu.

2. Attiecīgā gadījumā piekļuve ESKI notiek, ievērojot pamataktu, ar ko izveido programmu, un tiek ņemti vērā visi papildu marķējumi, kas noteikti DKR.

3. Ja labuma guvējs vai apakšuzņēmējs vēlas pieņemt darbā valsts, kas nav ES dalībvalsts, valstspiederīgo tādā amatā, kurā ir vajadzīga piekļuve ESKI, kas klasificēta *CONFIDENTIEL UE/EU CONFIDENTIAL* vai *SECRET UE/EU SECRET* līmenī, labuma guvēja vai apakšuzņēmēja pienākums ir sākt procedūru drošības pielaides piešķiršanai šai personai saskaņā ar valsts normatīvajiem aktiem, kas piemērojami vietā, kurā ir paredzēts piešķirt piekļuvi ESKI.

7. pants

Ekspertu, kas piedalās pārbaudēs, pārskatīšanā vai revīzijās, piekļuve ESKI

1. Ja piešķirējas iestādes veiktajās pārbaudēs, pārskatīšanā vai revīzijās, ko veic piešķirēja iestāde, vai labuma guvēju snieguma izskatīšanā ir iesaistītas ārējas personas (“eksperti”), kurām vajadzīga piekļuve informācijai, kas klasificēta *CONFIDENTIEL UE/EU CONFIDENTIAL* vai *SECRET UE/EU SECRET* līmenī, tām līgumu piešķir tikai tad, ja tām attiecīgā VDI vai IDI, vai jebkura cita kompetenta drošības iestāde ir piešķīrusi drošības pielaidi attiecīgajā līmenī. Piešķirēja iestāde ar Komisijas drošības iestādes starpniecību pārbauda un vajadzības gadījumā lūdz VDI vai IDI sākt ekspertu pārbaudes procesu vismaz sešus mēnešus pirms attiecīgo līgumu sākuma.

2. Pirms līguma parakstīšanas ekspertus iepazīstina ar ESKI aizsardzībai piemērojamiem drošības noteikumiem un tie apliecina savus pienākumus saistībā ar šādas informācijas aizsargāšanu.

4. NODAĻA

AR KLASIFICĒTIEM DOTĀCIJAS NOLĪGUMIEM SAISTĪTI APMEKLĒJUMI

8. pants

Pamatprincipi

1. Ja piešķīrēja iestāde, eksperti, labuma guvēji vai apakšuzņēmēji lūdz piekļuvi informācijai, kas klasificēta *CONFIDENTIEL UE/EU CONFIDENTIAL* vai *SECRET UE/EU SECRET* līmenī, cits cita telpās klasificēta dotācijas nolīguma īstenošanai, apmeklējumus organizē sadarbībā ar VDI vai IDI vai jebkuru citu attiecīgo kompetento drošības iestādi.

2. Uz 1. punktā minētajiem apmeklējumiem attiecas šādas prasības:

a) apmeklējumu oficiālais mērķis ir saistīts ar klasificētu dotāciju;

b) visiem apmeklētājiem ir attiecīga līmeņa PDP un vajadzība pēc informācijas, lai varētu piekļūt ESKI, ko izmanto vai rada klasificētās dotācijas izpildes gaitā.

9. pants

Apmeklējumu pieprasījumi

1. Tādus labuma guvēju vai apakšuzņēmēju apmeklējumus citu labuma guvēju vai apakšuzņēmēju iestādēs vai piešķīrējas iestādes telpās, kas saistīti ar piekļuvi informācijai, kura klasificēta *CONFIDENTIEL UE/EU CONFIDENTIAL* vai *SECRET UE/EU SECRET* līmenī, organizē atbilstīgi šādai procedūrai:

a) tās iestādes drošības speciālists, kas sūta apmeklētāju, aizpilda visas attiecīgās apmeklējuma pieprasījuma (AP) veidlapas daļas un iesniedz šo pieprasījumu minētās iestādes VDI vai IDI. AP veidlapas veidne ir iekļauta III pielikuma C papildinājumā;

b) nosūtītājas iestādes VDI vai IDI ir jāapstiprina apmeklētāja PDP pirms AP iesniegšanas uzņēmējas iestādes VDI vai IDI (vai Komisijas drošības iestādei, ja paredzēts apmeklēt piešķīrējas iestādes telpas);

c) pēc tam nosūtītājas iestādes drošības speciālists saņem no savas VDI vai IDI uzņēmējas iestādes VDI vai IDI (vai Komisijas drošības iestādes) atbildi par AP apstiprināšanu vai noraidīšanu;

d) uzskata, ka AP ir apstiprināts, ja piecas darba dienas pirms apmeklējuma dienas nav celti iebildumi.

2. Piešķīrējas iestādes amatpersonu, ekspertu vai revidentu apmeklējumus labuma guvēju vai apakšuzņēmēju iestādēs saistībā ar piekļuvi informācijai, kura klasificēta *CONFIDENTIEL UE/EU CONFIDENTIAL* vai *SECRET UE/EU SECRET* līmenī, organizē atbilstīgi šādai procedūrai:

a) apmeklētājs aizpilda visas attiecīgās AP veidlapas daļas un iesniedz šo veidlapu Komisijas drošības iestādei;

b) Komisijas drošības iestāde apstiprina apmeklētāja PDP pirms AP iesniegšanas uzņēmējas iestādes VDI vai IDI;

c) Komisijas drošības iestāde no uzņēmējas iestādes VDI vai IDI saņem atbildi, kurā AP tiek apstiprināts vai noraidīts;

d) uzskata, ka AP ir apstiprināts, ja piecas darba dienas pirms apmeklējuma dienas nav celti iebildumi.

3. AP var attiekties uz vienu apmeklējumu vai atkārtotiem apmeklējumiem. Atkārtotu apmeklējumu gadījumā AP derīguma termiņš var būt maksimāli viens gads no pieprasītā sākuma datuma.

4. AP derīguma termiņš nepārsniedz apmeklētāja PDP derīguma termiņu.

5. Parasti AP iesniedz uzņēmējas iestādes kompetentajai drošības iestādei vismaz 15 darba dienas pirms apmeklējuma dienas.

10. pants

Apmeklējumu procedūras

1. Pirms apmeklētājam tiek atļauta piekļuve ESKI, uzņēmējas iestādes drošības speciālists izpilda visas ar apmeklējumu saistītās drošības procedūras un attiecīgās VDI vai IDI paredzētos noteikumus.

2. Apmeklētāji pierāda savu identitāti, uzrādot derīgu ID karti vai pasi laikā, kad ierodas uzņēmējā iestādē. Identifikācijas informācijai ir jāatbilst informācijai, kas sniegta AP.

3. Uzņēmēja iestāde nodrošina, ka tiek reģistrēta informācija par visiem apmeklētājiem, tostarp to vārdi, organizācija, kuru tie pārstāv, PDP derīguma termiņš, apmeklējuma datums un to personu vārdi, pie kurām dodas apmeklētāji. Šādus ierakstus glabā vismaz piecus gadus vai ilgāk, ja tā ir paredzēts tās valsts normatīvajos aktos, kurā atrodas uzņēmēja iestāde.

11. pants

Tieši organizēti apmeklējumi

1. Saistībā ar konkrētiem projektiem attiecīgās VDI vai IDI un Komisijas drošības iestāde var vienoties par procedūru, atbilstīgi kurai apmeklējumus konkrētas klasificētās dotācijas kontekstā var organizēt tieši, sadarbojoties apmeklētāja drošības speciālistam un tās iestādes drošības speciālistam, kuru paredzēts apmeklēt. Šajā nolūkā izmantojamās veidlapas veidne ir iekļauta III pielikuma C papildinājumā. Šādu izņēmuma procedūru izklāsta PDI vai citā īpašā kārtībā. Šādos gadījumos nepiemēro 9. pantā un 10. panta 1. punktā izklāstītās procedūras.

2. Apmeklējumus, kas saistīti ar piekļuvi informācijai, kura klasificēta *RESTREINT UE/EU RESTRICTED* līmenī, organizē tieši, sadarbojoties nosūtītājai iestādei un saņēmējai iestādei un neievērojot 9. pantā un 10. panta 1. punktā izklāstītās procedūras.

5. NODAĻA

ESKI NOSŪTĪŠANA UN PĀRVIETOŠANA, PILDOT KLASIFICĒTOS DOTĀCIJAS NOLĪGUMUS

12. pants

Pamatprincipi

Piešķīrēja iestāde nodrošina, ka visi lēmumi par ESKI nosūtīšanu un pārvietošanu atbilst Lēmumam (ES, Euratom) 2015/444 un tā īstenošanas noteikumiem, kā arī klasificētā dotācijas nolīguma noteikumiem, tostarp par autora piekrišanu.

13. pants

Rīcība elektroniskā formātā

1. Ar ESKI rīkojas un to nosūta elektroniskā formātā saskaņā ar 5. un 6. nodaļu Lēmumā (ES, Euratom) 2015/444 un tā īstenošanas noteikumiem.

Labuma guvējam piederošās komunikācijas un informācijas sistēmas, kurās rīkojas ar ESKI dotācijas nolīguma izpildes vajadzībām ("labuma guvēja KIS"), akreditē atbildīgā drošības akreditācijas iestāde (DAI). ESKI elektronisku nosūtīšanu aizsargā ar kriptogrāfijas produktiem, kas apstiprināti saskaņā ar Lēmuma (ES, Euratom) 2015/444 36. panta 4. punktu. *TEMPEST* drošības pasākumus veic saskaņā ar minētā lēmuma 36. panta 6. punktu.

2. Labuma guvēja KIS, kurā rīkojas ar ESKI, kas klasificēta *RESTREINT UE / EU RESTRICTED* līmenī, un visu šīs KIS starpsavienojumu drošības akreditāciju var deleģēt labuma guvēja drošības speciālistam, ja tas ir atļauts valsts normatīvajos aktos. Ja šis uzdevums ir deleģēts, labuma guvējs atbild par DAV izklāstīto minimālo drošības prasību izpildi, rīkojoties savā KIS ar informāciju, kas klasificēta *RESTREINT UE/EU RESTRICTED* līmenī. Tomēr attiecīgās VDI vai IDI un DAI saglabā atbildību par tās informācijas aizsardzību, kas klasificēta *RESTREINT UE/EU RESTRICTED* līmenī un ar ko rīkojas labuma guvējs, kā arī tiesības pārbaudīt labuma guvēja veiktos drošības pasākumus. Turklāt saņēmējs iesniedz piešķīrējai iestādei un, ja tas paredzēts valsts normatīvajos aktos, kompetentajai valsts DAI paziņojumu par atbilstību, apliecinot, ka saņēmēja KIS un attiecīgie starpsavienojumi ir akreditēti tā, lai tajos varētu rīkoties ar ESKI, kas klasificēta *RESTREINT UE/EU RESTRICTED* līmenī ([11]).

14. pants

Transportēšana ar komerciāliem kurjeriem

Transportējot ESKI ar komerciāliem kurjeriem, ievēro attiecīgos noteikumus, kas izklāstīti Komisijas Lēmumā (ES, Euratom) 2019/1962 ([12]) par īstenošanas noteikumiem attiecībā uz rīkošanos ar *RESTREINT UE/EU RESTRICTED* līmenī klasificētu informāciju un Komisijas Lēmumā (ES, Euratom) 2019/1961 ([13]) par īstenošanas noteikumiem attiecībā uz rīkošanos ar *CONFIDENTIEL UE/EU CONFIDENTIAL* un *SECRET UE/EU SECRET* līmenī klasificētu informāciju.

15. pants

Pārvietošana rokas bagāžā

1. Attiecībā uz klasificētas informācijas pārvietošanu rokas bagāžā piemēro stingras drošības prasības.

2. Labuma guvēja darbinieki Savienībā var pārvietot rokas bagāžā informāciju, kas klasificēta *RESTREINT UE/EU RESTRICTED* līmenī, ja ir izpildītas šādas prasības:

a) izmantotā aploksne vai iepakojums ir necaurredzams, un uz tā nav norāžu par tā satura klasifikāciju;

b) klasificētā informācija vienmēr atrodas pie nesēja;

c) aploksne vai iepakojums netiek atvērts pa ceļam.

3. Par kārtību, kā labuma guvēja darbinieki dalībvalstī veic tādas informācijas pārvietošanu rokas bagāžā, kas klasificēta *CONFIDENTIEL UE/EU CONFIDENTIAL* un *SECRET UE/EU SECRET* līmenī, iepriekš vienojas nosūtītāja iestāde un saņēmēja iestāde. Nosūtītāja iestāde vai objekts sniedz saņēmējai iestādei vai objektam sīkas ziņas par sūtījumu, tostarp norādot atsauces numuru, klasifikācijas līmeni, paredzamo piegādes laiku un kurjera vārdu. Šāda pārvietošana rokas bagāžā ir atļauta, ja ir izpildītas šādas prasības:

a) klasificētā informācija tiek pārvietota dubultā aploksnē vai iepakojumā;

b) ārējā aploksne vai iepakojums ir nodrošināts, un uz tā nav norādījumu par tā satura klasifikācijas līmeni, savukārt uz iekšējās aploksnes ir norādīts klasifikācijas līmenis;

c) ESKI vienmēr atrodas pie nesēja;

d) aploksne vai iepakojums netiek atvērts pa ceļam;

e) aploksne vai iepakojums tiek pārvietots aizslēdzamā portfelī vai līdzīgā apstiprinātā konteinerā, kura izmērs un svars ir tāds, ka to visu laiku var paturēt pie nesēja un nenodot bagāžas glabātuvē;

f) kurjeram ir piešķirts kurjera sertifikāts, ko izdevusi viņa vai viņas kompetentā drošības iestāde, kas pilnvaro kurjeru pārvietot noteiktus klasificētus sūtījumus.

([11]) Minimālās prasības attiecībā uz komunikācijas un informācijas sistēmām, kurās rīkojas ar ESKI, kas klasificēta *RESTREINT UE/EU RESTRICTED* līmenī, ir noteiktas III pielikuma E papildinājumā.

([12]) Komisijas Lēmums (ES, Euratom) 2019/1962 (2019. gada 17. oktobris) par īstenošanas noteikumiem attiecībā uz rīkošanos ar *RESTREINT UE/EU RESTRICTED* līmenī klasificētu informāciju (OV L 311, 2.12.2019., 21. lpp.).

([13]) Komisijas Lēmums (ES, Euratom) 2019/1961 (2019. gada 17. oktobris) par īstenošanas noteikumiem attiecībā uz rīkošanos ar *CONFIDENTIEL UE/EU CONFIDENTIAL* un *SECRET UE/EU SECRET* līmenī klasificētu informāciju (OV L 311, 2.12.2019., 1. lpp.).

4. Ja labuma guvēja darbinieks pārvieto rokas bagāžā informāciju, kas klasificēta *CONFIDENTIEL UE/EU CONFIDENTIAL* un *SECRET UE / EU SECRET* līmenī, no vienas dalībvalsts uz citu, piemēro šādus papildu noteikumus:

a) kurjers atbild par pārvietojamā klasificētā materiāla drošu uzraudzību, līdz tas tiek nodots saņēmējam;

b) drošības pārkāpuma gadījumā sūtītāja VDI vai IDI var pieprasīt, lai iestādes valstī, kurā tika izdarīts pārkāpums, veiktu izmeklēšanu, paziņotu savus konstatējumus un veiktu atbilstošas tiesiskas vai citas darbības;

c) kurjers ir informēts par visiem drošības pienākumiem, kuri ir jāpilda pārvietošanas laikā, un ir parakstījis attiecīgu apstiprinājumu;

d) kurjeram paredzētie norādījumi ir pievienoti kurjera sertifikātam;

e) kurjeram ir iesniegts sūtījuma apraksts un maršruts;

f) dokumentus atgriež izdevējai VDI vai IDI, kad pārvietošana ir pabeigta, vai saņēmējs nodrošina, ka tie ir pieejami uzraudzības nolūkos;

g) ja muitas vai imigrācijas iestādes vai robežsardzes dienests lūdz pārbaudīt sūtījumu, tiem ir atļauts atvērt un aplūkot sūtījuma daļas tiktāl, lai varētu noteikt, ka tajā ir vienīgi deklarētais materiāls;

h) muitas iestādes būtu jālūdz ievērot kurjeram līdzi esošo pavaddokumentu un pilnvarojuma dokumentu oficiālo statusu.

Ja muitas iestādes atver sūtījumu, tas ir jādara tā, lai to neredzētu nepilnvarotas personas, un, ja iespējams, kurjera klātbūtnē. Kurjers pieprasa atkārtoti iepakot sūtījumu un lūdz iestādēm, kas veic pārbaudi, atkārtoti aizzīmogot sūtījumu un rakstiski apstiprināt, ka tās to tika atvērušas.

5. Ja labuma guvēja darbinieks informāciju, kas klasificēta *RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL* un *SECRET UE/EU SECRET* līmenī, pārvieto rokas bagāžā uz trešo valsti vai starptautisku organizāciju, piemēro noteikumus, kas izklāstīti informācijas drošības nolīgumā, vai administratīvo vienošanos, ko noslēgusi attiecīgi Savienība vai Komisija un minētā trešā valsts vai starptautiskā organizācija.

6. NODAĻA

DARBĪBAS NEPĀRTRAUKTĪBAS PLĀNOŠANA

16. pants

Plāni ārkārtas situācijām un atgūšanas pasākumi

Piešķīrēja iestāde nodrošina, ka klasificētā dotācijas nolīgumā ir noteikts, ka labuma guvējam ir jāizstrādā darbības nepārtrauktības plāni (DNP), lai ārkārtas situācijās aizsargātu ESKI, ar ko rīkojas saistībā ar klasificētu dotācijas nolīgumu, un ir jāievieš preventīvi un atgūšanas pasākumi darbības nepārtrauktības plānošanas kontekstā, lai mazinātu tādu incidentu ietekmi, kas saistīti ar rīkošanos ar ESKI un tās glabāšanu. Labuma guvēji apstiprina piešķīrējai iestādei, ka to DNP ir izstrādāti.

17. pants

Stāšanās spēkā

Šis lēmums stājas spēkā divdesmitajā dienā pēc tā publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī*.

Briselē, 2021. gada 10. februārī

Komisijas
un tās priekšsēdētājas vārdā –
Komisijas loceklis
Johannes HAHN

I PIELIKUMS

UZAICINĀJUMA STANDARTINFORMĀCIJA

(pielāgot atkarībā no izmantotā uzaicinājuma)

Drošība

Projektiem, kas saistīti ar ES klasificēto informāciju, jāiztur drošības pārbaude, lai tiem apstiprinātu finansējumu, un uz tiem var attiecināt īpašus drošības noteikumus (tie ir sīki izklāstīti drošības aspektu vēstulē (DAV), kura pievienota dotācijas nolīgumam).

Šie noteikumi (ko reglamentē Komisijas Lēmums (ES, Euratom) 2015/444 ([1]) un/vai valsts noteikumi) paredz, piemēram, ka:

— **NEVAR** finansēt projektus, kas saistīti ar informāciju, kura klasificēta kā *TRES SECRET UE/EU TOP SECRET* (vai līdzvērtīga),

— klasificētai informācijai jābūt marķētai saskaņā ar DAV iekļautajām piemērojamajām drošības instrukcijām,

— informāciju, kas klasificēta līmenī *CONFIDENTIEL UE/EU CONFIDENTIAL* vai augstāk (un *RESTREINT UE/EU RESTRICTED*, ja to prasa valsts noteikumi):

  — drīkst izveidot vai tai piekļūt tikai telpās, kurām kompetentā valsts drošības iestāde (VDI) piešķīrusi drošības pielaidi saskaņā ar valsts noteikumiem,

  — ar to drīkst rīkoties tikai drošā zonā, ko akreditējusi kompetentā VDI,

  — tai piekļūst un to apstrādāt drīkst tikai personas ar derīgu personāla drošības pielaidi (PDP), kurām ir vajadzība pēc informācijas,

— dotācijas beigās klasificētā informācija ir vai nu jāatdod atpakaļ, vai jāturpina aizsargāt saskaņā ar piemērojamajiem noteikumiem,

— par darbības uzdevumiem, kas saistīti ar ES klasificēto informāciju (ESKI), apakšuzņēmuma līgumus drīkst slēgt tikai ar piešķīrējas iestādes iepriekšēju rakstisku apstiprinājumu un tikai ar subjektiem, kas veic uzņēmējdarbību ES dalībvalstī vai trešā valstī, kurai ar ES ir noslēgts informācijas drošības nolīgums (vai administratīva vienošanās ar Komisiju),

— trešām personām ESKI drīkst izpaust vienīgi tad, ja piešķīrēja iestāde iepriekš ir devusi rakstisku atļauju.

Jāņem vērā, ka atkarībā no darbības veida pirms parakstīšanas var būt jānodrošina iestādes drošības pielaide. Piešķīrēja iestāde katrā konkrētajā gadījumā novērtēs pielaides nepieciešamību un dotācijas nolīguma sagatavošanas gaitā noteiks tās piešķiršanas datumu. Ņemiet vērā, ka mēs **nekādā gadījumā** nevaram parakstīt dotācijas nolīgumu, iekams vismaz vienam no konsorcijā iesaistītajiem saņēmējiem nav iestādes drošības pielaides.

Dotācijas nolīgumam var pievienot papildu drošības ieteikumus, kas izpaužas kā drošības uzdevumi (*piemēram, izveidot drošības konsultantu grupu, ierobežot detalizācijas pakāpi, izmantot viltus scenāriju, izslēgt klasificētas informācijas izmantošanu utt.*).

Saņēmējiem jānodrošina, ka viņu projekti netiek pakļauti valsts / trešās valsts drošības prasībām, kas varētu ietekmēt dotācijas īstenošanu vai likt apšaubīt tās piešķiršanu (*piemēram, tehnoloģiju ierobežojumi, valsts drošības klasifikācija utt.*). Piešķīrējai iestāde nekavējoties jātiek informētai par visām iespējamajām drošības problēmām.

[*Papildu VARIANTS partnerības pamatnolīgumiem*. Ja runa ir par partnerības pamatnolīgumiem, drošības pārbaude var būt jāiztur gan pamatpartnerības pieteikumiem, gan dotācijas pieteikumiem.]

([1]) Sk. Komisijas Lēmumu (ES, Euratom) 2015/444 (2015. gada 13. marts) par drošības noteikumiem ES klasificētas informācijas aizsardzībai (OV L 72, 17.3.2015., 53. lpp.).

II PIELIKUMS

DOTĀCIJAS NOLĪGUMA STANDARTNOTEIKUMI

(pielāgot atkarībā no izmantotā dotācijas nolīguma)

13.2 Drošība – klasificēta informācija

Ar klasificētu (ES vai valsts) informāciju Pusēm ir jārīkojas saskaņā ar piemērojamajiem ES vai valsts tiesību aktiem par klasificētu informāciju (jo īpaši Komisijas Lēmumu (ES, Euratom) 2015/444 ([1]) un tā īstenošanas noteikumiem).

Īpašie drošības noteikumi (ja tādi pastāv) ir izklāstīti 5. pielikumā.

5. PIELIKUMS

Drošība – ES klasificētā informācija

[*VARIANTS pasākumiem ar ES klasificētu informāciju (standartgadījums)*. Ja darbības gaitā tiek izmantota vai radīta ES klasificētā informācija, tā ir jāapstrādā saskaņā ar drošības klasifikācijas rokasgrāmatu (DKR) un drošības aspektu vēstuli (DAV), kas sniegta 1. pielikumā, un saskaņā ar Lēmumu (ES, Euratom) 2015/444 un tā īstenošanas noteikumiem, līdz minētā informācija tiek deklasificēta.

Rezultāti, kas satur klasificētu informāciju, ir jāiesniedz saskaņā ar īpašām procedūrām, ko apstiprinājusi piešķīrēja iestāde.

Par darbības uzdevumiem, kas saistīti ar ES klasificēto informāciju, apakšuzņēmuma līgumus drīkst slēgt tikai ar piešķīrējas iestādes iepriekšēju nepārprotamu rakstisku piekrišanu un tikai ar subjektiem, kas veic uzņēmējdarbību ES dalībvalstī vai trešā valstī, kurai ar ES ir noslēgts informācijas drošības nolīgums (vai administratīva vienošanās ar Komisiju).

ES klasificēto informāciju nedrīkst izpaust trešām personām (t. sk. darbības īstenošanā iesaistītajiem dalībniekiem) bez piešķīrējas iestādes iepriekšējas nepārprotamas rakstiskas piekrišanas.]

([1]) Komisijas Lēmums (ES, Euratom) 2015/444 (2015. gada 13. marts) par drošības noteikumiem ES klasificētas informācijas aizsardzībai (OV L 72, 17.3.2015., 53. lpp.).

III PIELIKUMS

[IV pielikums (.....)]

DROŠĪBAS ASPEKTU VĒSTULE (DAV) [1]

[Paraugs]

[1] Šo DAV paraugu izmanto gadījumos, kad Komisija tiek uzskatīta par tādas klasificētas informācijas autoru, kura ir izveidota un ar kuru rīkojas dotācijas nolīguma izpildes nolūkā. Ja Komisija nav tās klasificētās informācijas autors, kura ir izveidota un ar kuru rīkojas dotācijas nolīguma izpildes nolūkā, un ja dalībvalstis, kuras piedalās dotācijas apgūšanā, ir izveidojušas īpašu drošības satvaru, var izmantot citus DAV modeļus.

A papildinājums

DROŠĪBAS PRASĪBAS

Piešķīrējai iestādei drošības aspektu vēstulē (DAV) ir jāiekļauj tālāk minētās drošības prasības. Daži noteikumi var neattiekties uz dotācijas nolīgumu. Tie ir norādīti kvadrātiekavās.

Noteikumu saraksts nav izsmeļošs. Atkarībā no klasificētās dotācijas veida var pievienot papildu punktus.

VISPĀRĪGI NOSACĪJUMI [*NB! Attiecas uz visiem klasificētajiem dotāciju nolīgumiem*]

1. Šī drošības aspektu vēstule (DAV) ir klasificētā dotācijas nolīguma [vai apakšlīguma] neatņemama daļa, un tajā ir norādītas drošības prasības, kas attiecas uz dotācijas nolīgumu. Šo prasību nepildīšana var būt pietiekams pamats dotācijas nolīguma izbeigšanai.

2. Uz dotācijas saņēmējiem attiecas visas saistības, kas izklāstītas Komisijas Lēmumā (ES, Euratom) 2015/444 ([2]) (turpmāk "KL 2015/444") un tā īstenošanas noteikumos ([3]). Ja dotācijas saņēmējs dalībvalstī saskaras ar problēmu, kas saistīta ar piemērojamā tiesiskā regulējuma piemērošanu, tam jāvēršas Komisijas drošības iestādē un valsts drošības iestādē (VDI) vai izraudzītajā drošības iestādē (IDI).

3. Klasificēta informācija, kas ir radīta, pildot dotācijas nolīgumu, ir jāmarķē kā ES klasificēta informācija (ESKI) tādā drošības klasifikācijas līmenī, kāds paredzēts šīs vēstules B papildinājumā sniegtajā drošības klasifikācijas rokasgrāmatā (DKR). Atkāpe no DKR noteiktā drošības klasifikācijas līmeņa ir pieļaujama vienīgi ar piešķīrējas iestādes rakstisku atļauju.

4. Tiesības, kas attiecināmas uz tādas ESKI autoru, kura radīta un ar kuru rīkojas, lai izpildītu klasificēto dotācijas nolīgumu, īsteno Komisija kā piešķīrēja iestāde.

5. Informāciju vai materiālu, kuru sniegusi piešķīrēja iestāde vai kurš radīts minētās iestādes vārdā, saņēmējs vai apakšuzņēmējs nedrīkst izmantot citam, dotācijas nolīgumā neparedzētam mērķim, ja piešķīrēja iestāde nav paudusi rakstisku piekrišanu.

6. Ja dotācijas nolīguma izpildei ir vajadzīga iestādes drošības pielaide (IDP), saņēmējam ir jālūdz piešķīrējai iestādei izskatīt IDP pieprasījumu.

7. Saņēmējam ir jāizmeklē visi ar ESKI saistītie drošības pārkāpumi un jāziņo par tiem piešķīrējai iestādei, cik vien drīz iespējams. Saņēmējam vai apakšuzņēmējam ir nekavējoties jāziņo savai VDI vai IDI un – gadījumos, kad to atļauj valsts normatīvie akti, – Komisijas drošības iestādei par visiem gadījumiem, kad ir zināms vai kad ir pamats aizdomām, ka ESKI, kas sniegta vai radīta saskaņā ar dotācijas nolīgumu, ir pazaudēta vai izpausta nesankcionētām personām.

([2]) Komisijas Lēmums (ES, Euratom) 2015/444 (2015. gada 13. marts) par drošības noteikumiem ES klasificētas informācijas aizsardzībai (OV L 72, 17.3.2015., 53. lpp.).

([3]) Piešķīrējai iestādei būtu jānorāda atsauces, tiklīdz ir pieņemti īstenošanas noteikumi.

8. Pēc dotācijas nolīguma izbeigšanās saņēmējam vai apakšuzņēmējam pēc iespējas drīzāk ir jāatdod piešķīrējai iestādei tam pieejamā ESKI. Kad tas ir praktiski iespējams, saņēmējs vai apakšuzņēmējs drīkst iznīcināt ESKI, nevis to atdot. Tas jādara saskaņā ar tās valsts normatīvajiem aktiem, kurā atrodas saņēmējs, turklāt iepriekš jāsaņem Komisijas drošības iestādes piekrišana un jāseko tās norādījumiem. ESKI ir jāiznīcina tā, lai to nevarētu atjaunot ne pilnībā, ne daļēji.

9. Ja saņēmējam vai apakšuzņēmējam ir atļauts paturēt ESKI pēc dotācijas nolīguma izbeigšanas vai noslēgšanas, ir jāturpina aizsargāt ESKI saskaņā ar KL 2015/444 un tā īstenošanas noteikumiem ([4]).

10. Rīkojoties ar ESKI, to apstrādājot un pārsūtot elektroniskā formātā, ir jāievēro KL 2015/444 5. un 6. nodaļā izklāstītie noteikumi. Tie cita starpā ietver prasību, ka ir jāakreditē ([5]) komunikācijas un informācijas sistēmas, kas pieder saņēmējam un ko izmanto, lai rīkotos ar ESKI dotācijas nolīguma vajadzībām (turpmāk "saņēmēja KIS"); ka, nosūtot ESKI elektroniskā veidā, tā ir jāaizsargā ar kriptogrāfijas produktiem, kas apstiprināti saskaņā ar KL 2015/444 36. panta 4. punktu, un ka *TEMPEST* drošības pasākumi ir jāīsteno saskaņā ar KL 2015/444 36. panta 6. punktu.

11. Saņēmējam vai apakšuzņēmējam ir darbības nepārtrauktības plāni (DNP), lai ārkārtas situācijās aizsargātu ESKI, ar ko rīkojas, pildot klasificētu dotācijas nolīgumu, un ir ieviesti preventīvi un atgūšanas pasākumi, lai samazinātu tādu incidentu ietekmi, kas saistīti ar rīkošanos ar ESKI un tās glabāšanu. Saņēmējam vai apakšuzņēmējam ir jāinformē piešķīrēja iestāde par savu DNP.

DOTĀCIJU NOLĪGUMI, KUROS VAJADZĪGA PIEKĻUVE INFORMĀCIJAI, KAS KLASIFICĒTA *RESTREINT UE/EU RESTRICTED* LĪMENĪ

12. Lai izpildītu dotācijas nolīgumu ([6]), nav vajadzīga personāla drošības pielaide (PDP). Tomēr informācijai vai materiālam, kas klasificēts *RESTREINT UE/EU RESTRICTED* līmenī, ir jābūt pieejamam vienīgi saņēmēja darbiniekiem, kuri pieprasa šādu informāciju dotācijas nolīguma izpildes vajadzībām (*vajadzības pēc informācijas princips*) un kurus saņēmēja drošības speciālists ir informējis par pienākumiem un sekām šādas informācijas drošības apdraudēšanas vai pārkāpuma gadījumā, turklāt viņiem ir rakstiski jāapliecina, ka viņi apzinās sekas, kas rodas gadījumā, ja ESKI netiek aizsargāta.

13. Ja vien piešķīrēja iestāde nav devusi rakstisku piekrišanu, saņēmējs vai apakšuzņēmējs piekļuvi informācijai vai materiālam, kas klasificēts *RESTREINT UE/EU RESTRICTED* līmenī, nedrīkst piešķirt nevienam subjektam vai personai, izņemot savus darbiniekus, kuriem ir vajadzība pēc informācijas.

14. Saņēmējam vai apakšuzņēmējam ir jāsaglabā tās klasificētās informācijas drošības klasifikācijas marķējumi, kas radīta vai sniegta dotācijas nolīguma izpildes gaitā, un tas nedrīkst deklasificēt informāciju bez piešķīrējas iestādes rakstiskas piekrišanas.

15. Laikā, kad informācija vai materiāls, kas klasificēts *RESTREINT UE/EU RESTRICTED* līmenī, netiek lietots, tas ir jāglabā slēgtās biroja mēbelēs. Piegādājot dokumentus, tiem ir jāatrodas necaurredzamā aploksnē. Dokumentiem vienmēr ir jāatrodas pie to nesēja, un aploksni nedrīkst atvērt pa ceļam.

([4]) Piešķīrējai iestādei būtu jānorāda atsauces, tiklīdz ir pieņemti īstenošanas noteikumi.

([5]) Pusei, kas veic akreditāciju, būs jāiesniedz piešķīrējai iestādei paziņojums par atbilstību, to darot ar Komisijas drošības iestādes starpniecību un saskaņojot ar attiecīgo valsts drošības akreditācijas iestādi (DAI).

([6]) Ja saņēmēji ir no dalībvalstīm, kuras pieprasa PDP un/vai IDP attiecībā uz dotācijām, kas klasificētas kā *RESTREINT UE/EU RESTRICTED*, piešķīrēja iestāde drošības aspektu vēstulē (DAV) uzskaita PDP un IDP prasības attiecīgajiem saņēmējiem.

16. Saņēmējs vai apakšuzņēmējs dokumentus, kas klasificēti *RESTREINT UE/EU RESTRICTED* līmenī, drīkst piegādāt piešķīrējai iestādei, izmantojot kurjeru uzņēmumu pakalpojumus, pasta pakalpojumus, elektroniskus līdzekļus vai rokas bagāžā. Šajā saistībā saņēmējam vai apakšuzņēmējam ir jārīkojas saskaņā ar Komisijas izdoto programmas (vai projekta) drošības instrukciju (PDI) un/vai Komisijas īstenošanas noteikumiem industriālās drošības jomā attiecībā uz klasificētām dotācijām ([7]).

17. Kad dokumenti, kas klasificēti *RESTREINT UE/EU RESTRICTED* līmenī, vairs nav vajadzīgi, tie ir jāiznīcina tā, lai tos nevarētu atjaunot ne pilnībā, ne daļēji.

18. Saņēmēja KIS, kurā rīkojas ar ESKI, kas klasificēta *RESTREINT UE/EU RESTRICTED* līmenī, un visu šīs KIS starpsavienojumu drošības akreditāciju var deleģēt saņēmēja drošības speciālistam, ja tas ir atļauts valsts normatīvajos aktos. Ja akreditācija tiek šādi deleģēta, VDI, IDI vai drošības akreditācijas iestādes (DAI) saglabā atbildību par tās informācijas aizsardzību, kas klasificēta *RESTREINT UE/EU RESTRICTED* līmenī un ar ko rīkojas saņēmējs, kā arī tiesības pārbaudīt saņēmēja veiktos drošības pasākumus. Turklāt saņēmējs iesniedz piešķīrējai iestādei un, ja tas paredzēts valsts normatīvajos aktos, kompetentajai valsts DAI paziņojumu par atbilstību, apliecinot, ka saņēmēja KIS un attiecīgie starpsavienojumi ir akreditēti rīcībai ar ESKI, kas klasificēta *RESTREINT UE/EU RESTRICTED* līmenī.

RĪKOŠANĀS AR *RESTREINT UE* / *EU RESTRICTED* LĪMENĪ KLASIFICĒTU INFORMĀCIJU KOMUNIKĀCIJAS UN INFORMĀCIJAS SISTĒMĀS (KIS)

19. Minimālās prasības KIS, kurā rīkojas ar *RESTREINT UE/EU RESTRICTED* līmenī klasificētu informāciju, ir izklāstītas šīs drošības aspektu vēstules E papildinājumā.

APSTĀKĻI, KUROS SAŅĒMĒJS VAR SLĒGT APAKŠLĪGUMUS

20. Saņēmējam jāiegūst piešķīrējas iestādes atļauja pirms apakšuzņēmuma līguma noslēgšanas par jebkuru klasificēta dotācijas nolīguma daļu.

21. Apakšlīgumus nevar slēgt ar subjektu, kas reģistrēts ārpussavienības valstī, vai starptautiskas organizācijas struktūru, ja šī ārpussavienības valsts vai starptautiskā organizācija nav noslēgusi informācijas drošības nolīgumu ar ES vai administratīvu vienošanos ar Komisiju.

22. Ja saņēmējs ir noslēdzis apakšlīgumu, dotācijas nolīguma drošības noteikumi attiecīgi ir piemērojami apakšuzņēmējam(-iem) un tā (to) darbiniekiem. Šādā gadījumā saņēmēja pienākums ir nodrošināt, ka visi apakšuzņēmēji piemēro šos principus paši savos apakšlīgumos. Lai nodrošinātu pienācīgu drošības uzraudzību, Komisijas drošības iestāde informē saņēmēja un apakšuzņēmēja VDI un/vai IDI par visiem saistītajiem noslēgtajiem apakšlīgumiem, kas klasificēti *CONFIDENTIEL UE/EU CONFIDENTIAL* un *SECRET UE/EU SECRET* līmenī. Attiecīgā gadījumā apakšlīgumam piemērojamo drošības noteikumu kopija ir jāiesniedz saņēmēja un apakšuzņēmēja VDI un/vai IDI. Tās VDI un IDI, kurām ir jāsaņem paziņojums par drošības noteikumiem dotāciju nolīgumos, kas klasificēti *RESTREINT UE / EU RESTRICTED* līmenī, ir uzskaitītas Komisijas īstenošanas noteikumu industriālās drošības jomā pielikumā par klasificētiem dotāciju nolīgumiem ([8]).

23. Saņēmējs nedrīkst izpaust ESKI apakšuzņēmējam bez piešķīrējas iestādes iepriekšējas rakstiskas piekrišanas. Ja ESKI apakšuzņēmējiem ir jāsūta bieži vai regulāri, piešķīrēja iestāde var sniegt savu apstiprinājumu uz noteiktu laikposmu (piemēram, 12 mēnešiem) vai uz apakšlīguma termiņu.

([7]) Piešķīrējai iestādei būtu jānorāda atsauces, tiklīdz ir pieņemti īstenošanas noteikumi.
([8]) Piešķīrējai iestādei būtu jānorāda atsauces, tiklīdz ir pieņemti īstenošanas noteikumi.

APMEKLĒJUMI

Ja apmeklējumiem, kuri saistīti ar informāciju, kas klasificēta CONFIDENTIEL UE/EU CONFIDENTIAL vai SECRET UE/EU SECRET līmenī, ir paredzēts piemērot standarta apmeklējuma pieprasījuma (AP) procedūru, piešķīrējai iestādei ir jāiekļauj 24., 25. un 26. punkts un jāsvītro 27. punkts. Ja apmeklējumus, kuri saistīti ar informāciju, kas klasificēta CONFIDENTIEL UE/EU CONFIDENTIAL vai SECRET UE/EU SECRET līmenī, organizē tieši starp nosūtītāju un saņēmēju struktūru, piešķīrējai iestādei ir jāsvītro 25. un 26. punkts un jāiekļauj vienīgi 27. punkts.

24. Apmeklējumus, kas saistīti ar piekļuvi vai iespējamu piekļuvi informācijai, kura klasificēta *RESTREINT UE/EU RESTRICTED* līmenī, organizē tieši, sadarbojoties nosūtītājai iestādei un saņēmējai iestādei un neievērojot tālāk 25. līdz 27. punktā izklāstīto procedūru.

[25. Apmeklējumiem, kas saistīti ar piekļuvi vai iespējamu piekļuvi informācijai, kura klasificēta *CONFIDENTIEL UE/EU CONFIDENTIAL* vai *SECRET UE/EU SECRET* līmenī, piemēro šādu procedūru:

a) apmeklētāja nosūtītājas iestādes drošības speciālists aizpilda visas attiecīgās apmeklējuma pieprasījuma (AP) veidlapas (C papildinājums) daļas un iesniedz šo pieprasījumu iestādes VDI vai IDI;

b) nosūtītājas iestādes VDI vai IDI ir jāapstiprina apmeklētāja PDP pirms AP iesniegšanas uzņēmējas iestādes VDI vai IDI (vai Komisijas drošības iestādei, ja paredzēts apmeklēt piešķīrējas iestādes telpas);

c) pēc tam nosūtītājas iestādes drošības speciālists saņem no savas VDI vai IDI atbildi, ko uzņēmējas iestādes VDI vai IDI (vai Komisijas drošības iestāde) sniegusi par AP apstiprināšanu vai noraidīšanu;

d) AP uzskata par apstiprinātu, ja piecas darba dienas pirms apmeklējuma dienas nav celti iebildumi.]

[26. Pirms uzņēmēja iestāde atļauj apmeklētājam(-iem) piekļūt informācijai, kas klasificēta *CONFIDENTIEL UE/EU CONFIDENTIAL* vai *SECRET UE/EU SECRET* līmenī, tai ir jāsaņem atļauja no savas VDI vai IDI.]

[27. Apmeklējumus, kas saistīti ar piekļuvi vai iespējamu piekļuvi informācijai, kura klasificēta *CONFIDENTIEL UE/EU CONFIDENTIAL* vai *SECRET UE/EU SECRET* līmenī, organizē tieši starp nosūtītāju iestādi un saņēmēju iestādi (šajā nolūkā izmantojamās veidlapas piemērs ir sniegts C papildinājumā).]

28. Apmeklētājiem ir jāpierāda sava identitāte, uzrādot derīgu ID karti vai pasi brīdī, kad viņi ierodas uzņēmējā iestādē.

29. Iestādei, kas uzņem apmeklētājus, ir jānodrošina, ka visi apmeklētāji tiek reģistrēti. Cita starpā ir jānorāda apmeklētāju vārds, viņu pārstāvēto organizāciju nosaukums, (attiecīgā gadījumā) PDP derīguma termiņš, apmeklējuma datums un apmeklētās(-o) personas(-u) vārds(-i). Neskarot Eiropas datu aizsardzības noteikumus, šie ieraksti ir jāsaglabā attiecīgi vismaz piecus gadus vai atbilstīgi valsts noteikumiem.

NOVĒRTĒJUMA APMEKLĒJUMI

30. Komisijas drošības iestāde sadarbībā ar attiecīgajām VDI vai IDI var apmeklēt saņēmēju vai apakšuzņēmēju iestādes, lai pārbaudītu, vai tiek ievērotas drošības prasības attiecībā uz rīkošanos ar ESKI.

DROŠĪBAS KLASIFIKĀCIJAS ROKASGRĀMATA

31. Drošības klasifikācijas rokasgrāmatā (DKR) ir ietverts visu dotācijas nolīguma klasificēto elementu vai dotācijas nolīguma izpildes laikā klasificējamo elementu saraksts, klasificēšanas noteikumi un drošības klasifikācijas līmeņu piemērošanas noteikumi. DKR ir šā dotācijas nolīguma neatņemama daļa un ir pieejama šā pielikuma B papildinājumā.

B papildinājums

DROŠĪBAS KLASIFIKĀCIJAS ROKASGRĀMATA

[konkrētais teksts ir jāpielāgo atkarībā no dotācijas nolīguma priekšmeta]

C papildinājums

APMEKLĒJUMA PIEPRASĪJUMS (PARAUGS)

SĪKI IZKLĀSTĪTI NORĀDĪJUMI PAR APMEKLĒJUMA PIEPRASĪJUMA VEIDLAPAS AIZPILDĪŠANU

(Pieteikums jāiesniedz vienīgi angļu valodā.)

HEADING	Atzīmējiet lodziņos apmeklējuma veidu, informācijas veidu un norādiet, cik daudz vietu tiks apmeklētas, kā arī apmeklētāju skaitu.
4. **ADMINISTRATIVE DATA**	Aizpilda pieprasītāja VDI/IDI.
5. **REQUESTING ORGANISATION OR INDUSTRIAL FACILITY**	Norādiet pilnu nosaukumu un pasta adresi. Attiecīgā gadījumā iekļaujiet pilsētu, valsti un pasta indeksu.
6. **ORGANISATION OR INDUSTRIAL FACILITY TO BE VISITED**	Norādiet pilnu nosaukumu un pasta adresi. Iekļaujiet pilsētu, valsti, pasta indeksu, teleksa vai faksa numuru (attiecīgā gadījumā), tālruņa numuru un e-pasta adresi. Norādiet sava galvenā kontaktpunkta vai personas, ar kuru esat vienojušies par apmeklējumu, nosaukumu/vārdu un tālruņa/faksa numurus, kā arī e-pasta adresi. Piezīmes: 1) ir svarīgi norādīt pareizu pasta indeksu (*zip* kodu), jo uzņēmumam var būt vairāki objekti; 2) piesakoties manuāli, 1. pielikumu var izmantot, ja saistībā ar to pašu tematu paredzēts apmeklēt divus vai vairākus objektus. Ja izmanto pielikumu, 3. punktā būtu jānorāda: “SEE ANNEX 1, NUMBER OF FAC.:..” (norādīt objektu skaitu).
7. **DATES OF VISIT**	Norādiet apmeklējuma faktisko datumu vai laikposmu (no viena datuma līdz otram) formātā “diena - mēnesis - gads.”. Attiecīgā gadījumā iekavās norādiet alternatīvu datumu vai laikposmu.
8. **TYPE OF INITIATIVE**	Norādiet, vai apmeklējumu ir ierosinājusi pieprasītāja organizācija vai iestāde, vai arī tas ir ierosināts, pamatojoties uz apmeklējamās iestādes uzaicinājumu.
9. **THE VISIT RELATES TO**	Norādiet pilnu projekta nosaukumu, līgumu vai uzaicinājumu iesniegt piedāvājumus, izmantojot vienīgi vispārpieņemtus saīsinājumus.
10. **SUBJECT TO BE DISCUSSED/ JUSTIFICATION**	Īsi izklāstiet apmeklējuma iemeslu(-us). Neizmantojiet saīsinājumus, kas nav izskaidroti. Piezīmes: atkārtotu apmeklējumu gadījumā šajā datu elementā kā pirmie vārdi būtu jānorāda *Recurring visits* (piemēram, *Recurring visits to discuss*_____).
11. **ANTICIPATED LEVEL OF CLASSIFIED INFORMATION TO BE INVOLVED**	Norādiet *SECRET UE / EU SECRET (S-UE/EU-S)* vai attiecīgā gadījumā *CONFIDENTIEL UE/EU CONFIDENTIAL (C-UE/EU-C)*.

12. **PARTICULARS OF VISITOR**	Piezīme: ja apmeklējumā piedalās vairāk nekā divi apmeklētāji, būtu jāizmanto 2. pielikums.
13. **THE SECURITY OFFICER OF THE REQUESTING ENTITY**	Šajā pozīcijā ir jānorāda pieprasītājas iestādes drošības speciālista vārds, tālruņa numurs, faksa numurs un e-pasta adrese.
14. **CERTIFICATION OF SECURITY CLEARANCE**	Šo lauku aizpilda sertifikācijas iestāde. Sertifikācijas iestādes ievērībai: a) norādiet nosaukumu, adresi, tālruņa numuru, faksa numuru un e-pasta adresi (var būt nodrukāts veidlapā); b) šī pozīcija būtu jāparaksta un jāapzīmogo (attiecīgā gadījumā).
15. **REQUESTING SECURITY AUTHORITY**	Šo lauku aizpilda VDI/IDI. Piezīme VDI/IDI: a) norādiet nosaukumu, adresi, tālruņa numuru, faksa numuru un e-pasta adresi (var būt iepriekš iespiests); b) šī pozīcija būtu jāparaksta un jāapzīmogo (attiecīgā gadījumā).

Jāaizpilda ir visi lauki, un veidlapa jāiesniedz, izmantojot starpvaldību kanālus ([9]).

REQUEST FOR VISIT

(MODEL)

TO: _____

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

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

([9]) Ja ir panākta vienošanās, ka apmeklējumus, kas saistīti ar piekļuvi vai iespējamu piekļuvi ESKI, kura klasificēta *CONFIDENTIEL UE/EU CONFIDENTIAL* un *SECRET UE/EU SECRET* līmenī, var organizēt tieši, aizpildīto veidlapu var iesniegt tieši tās iestādes drošības speciālistam, kuru ir paredzēts apmeklēt.

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)*:**

<Vietturis atsaucei uz piemērojamajiem persondatu aizsardzības tiesību aktiem un saite uz datu subjektam obligāti sniedzamo informāciju, piemēram, par to, kā tiek īstenots Vispārīgās datu aizsardzības regulas ([10]) 13. pants.>

([10]) Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (OV L 119, 4.5.2016., 1. lpp.).

AP VEIDLAPAS 1. PIELIKUMS

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)***

<Vietturis atsaucei uz piemērojamajiem persondatu aizsardzības tiesību aktiem un saite uz datu subjektam obligāti sniedzamo informāciju, piemēram, par to, kā tiek īstenots Vispārīgās datu aizsardzības regulas ([11]) 13. pants.>

([11]) Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (OV L 119, 4.5.2016., 1. lpp.).

AP VEIDLAPAS 2. PIELIKUMS

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)***

<Vietturis atsaucei uz piemērojamajiem persondatu aizsardzības tiesību aktiem un saite uz datu subjektam obligāti sniedzamo informāciju, piemēram, par to, kā tiek īstenots Vispārīgās datu aizsardzības regulas ([12]) 13. pants.>

([12]) Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (OV L 119, 4.5.2016., 1. lpp.).

D papildinājums

IESTĀDES DROŠĪBAS PIELAIDES INFORMĀCIJAS LAPA (IDPIL) (PARAUGS)

1. **IEVADS**

1.1. Pielikumā pievienots iestādes drošības pielaides informācijas lapas (IDPIL) paraugs, ko izmantot ātrai informācijas apmaiņai starp valsts drošības iestādi (VDI) vai izraudzīto drošības iestādi (IDI), citām kompetentajām valsts drošības iestādēm un Komisijas drošības iestādi (kas darbojas piešķīrēju iestāžu vārdā) saistībā ar klasificētu dotāciju vai apakšlīgumu īstenošanā vai pieteikumos iesaistītas iestādes drošības pielaidi (IDP).

1.2. IDPIL ir derīga tikai tad, ja to ir apzīmogojusi attiecīgā VDI, IDI vai cita kompetentā iestāde.

1.3. IDPIL ir sadalīta pieprasījuma un atbildes daļās, un to var izmantot iepriekš minētajiem mērķiem vai jebkuram citam mērķim, attiecībā uz kuru ir nepieciešams konkrētās iestādes drošības pielaides statuss. Pieprasītājai VDI vai IDI pieprasījuma iemesls ir jānorāda pieprasījuma sadaļas 7. laukā.

1.4. Parasti IDPIL iekļautās ziņas nav klasificētas; attiecīgi, ja IDPIL ir jāpārsūta starp attiecīgo VDI/IDI/Komisiju, to būtu ieteicams darīt, izmantojot elektroniskus līdzekļus.

1.5. VDI/IDI būtu jādara viss iespējamais, lai atbildētu uz IDPIL pieprasījumu desmit darba dienās.

1.6. Ja saistībā ar šo apliecinājumu ir jānosūta klasificēta informācija vai jāpiešķir dotācija vai apakšlīguma slēgšanas tiesības, par to ir jāinformē izdevēja VDI vai IDI.

Procedūras un norādījumi par iestādes drošības pielaides informācijas lapas (IDPIL) izmantošanu

Šie sīki izklāstītie norādījumi ir paredzēti VDI vai IDI, vai piešķīrējai iestādei un Komisijas drošības iestādei, kas aizpilda IDPIL. Vēlams aizpildīt pieprasījumu ar drukātiem burtiem.

GALVENE	Pieprasītājs norāda pilnu VDI/IDI un valsts nosaukumu.
1. **PIEPRASĪJUMA VEIDS**	Pieprasījumu iesniedzošā piešķīrēja iestāde izvēlas lodziņu, kas atbilst IDPIL pieprasījuma veidam. Norādīt pieprasītās drošības pielaides līmeni. Jāizmanto šādi saīsinājumi: SECRET UE/EU SECRET = S-UE/EU-S CONFIDENTIEL UE/EU CONFIDENTIAL = C-UE/EU-C KIS = komunikācijas un informācijas sistēmas, kurās rīkojas ar klasificētu informāciju
2. **SĪKA INFORMĀCIJA PAR TEMATU**	1.–6. lauks ir pašsaprotams. 4. laukā ir jānorāda standarta divu burtu valsts kods; 5. lauks ir neobligāts.
3. **PIEPRASĪJUMA PAMATOJUMS**	Norādiet konkrētu pieprasījuma iemeslu, projekta rādītājus, uzaicinājuma iesniegt priekšlikumus vai dotācijas numuru. Norādiet nepieciešamo uzglabāšanas spēju, KIS klasifikācijas līmeni u. c. Jānorāda visi termiņi / termiņa beigu datumi / piešķiršanas datumi, kuriem varētu būt nozīme, piešķirot IDP.

4. **PIEPRASĪTĀJA VDI/IDI**	Jānorāda faktiskā pieprasītāja (VDI/IDI vārdā) vārds un pieprasījuma datums ciparu formātā (dd/mm/gggg.).
5. **ATBILDES SADAĻA**	1.–5. lauks: izvēlieties atbilstošos laukus. 2. lauks: ja notiek IDP piešķiršana, ieteicams pieprasītāju orientējoši informēt par nepieciešamo apstrādes laiku (ja tas ir zināms). 6. lauks: a) lai gan apstiprināšana dažādās valstīs vai pat iestādēs ir atšķirīga, ieteicams norādīt IDP termiņa beigu datumu; b) ja IDP apliecinājuma termiņa beigu datums ir nenoteikts, šo lauku var pārsvītrot; c) saskaņā ar attiecīgajiem valsts normatīvajiem aktiem par pieteikuma iesniegšanu IDP atjaunošanai atbild pieprasītājs vai saņēmējs (vai apakšuzņēmējs).
6. **PIEZĪMES**	Var izmantot, lai sniegtu papildu informāciju par IDP, iestādi vai iepriekš minētajām pozīcijām.
7. **IZDEVĒJA VDI/IDI**	Jānorāda izdevējas iestādes (VDI/IDI vārdā) nosaukums un atbildes datums ciparu formātā (dd.mm.gggg.).

IESTĀDES DROŠĪBAS PIELAIDES INFORMĀCIJAS LAPA (IDPIL) (PARAUGS)

Jāaizpilda visi lauki, un veidlapa jāiesniedz, izmantojot starpvaldību vai valdības–starptautiskās organizācijas kanālus.

IESTĀDES DROŠĪBAS PIELAIDES APLIECINĀJUMA PIEPRASĪJUMS

ADRESĀTS: _____

(VDI/IDI valsts nosaukums)

Aizpildiet attiecīgos atbilžu lodziņus:

[ ] Sniegt IDP apliecinājumu: [ ] *S-UE/EU-S* līmenī [ ] *C-UE/EU-C* līmenī

par tālāk minēto iestādi,

[ ] ietverot klasificēta materiāla/informācijas nodrošinājumu

[ ] ietverot komunikācijas un informācijas sistēmas (KIS), kurās rīkojas ar klasificēto informāciju

[ ] tieši vai pēc labuma guvēja vai apakšuzņēmēja attiecīga pieprasījuma sākt IDP iegūšanas procesu līdz līmenim ..... ar ..... līmeņa nodrošinājumu un ..... līmeņa KIS, ja iestādei pašlaik nav šāda līmeņa iespēju.

Apstipriniet, ka tālāk uzskaitītās ziņas par iestādi ir precīzas, un vajadzības gadījumā labojiet/papildiniet tās.

1. Pilns iestādes nosaukums:	Labojumi/papildinājumi:
.....	.....
2. Pilna iestādes adrese:	
.....	.....
3. Pasta adrese (ja atšķiras no 2. punktā norādītās adreses):	
.....	.....
4. *Zip* / pasta indekss / pilsēta / valsts:	
.....	.....

5. Drošības speciālista vārds:

.....
.....

6. Drošības speciālista tālruņa numurs / faksa numurs / e-pasta adrese:

....

7. Šis pieprasījums ir iesniegts šāda(-u) iemesla(-u) dēļ: (sniedziet sīkas ziņas par posmu pirms līguma noslēgšanas (priekšlikumu atlases posmu), dotāciju vai apakšlīgumu, programmu/projektu u. c.)

.....

Pieprasītāja VDI / IDI / piešķīrēja iestāde: Datums: (dd.mm.gggg) .....
Nosaukums: .....

ATBILDE (desmit darba dienās)

Ar šo tiek apliecināts, ka:

1. [ ] iepriekš minētajai iestādei ir piešķirta IDP līdz līmenim [ ] *S-UE/EU-S*

   [ ] *C-UE/EU-C*.

2. Iepriekš minētā iestāde spēj aizsargāt klasificētu informāciju/materiālu:

   [ ] jā, līmenis: ..... [ ] nē.

3. Iepriekš minētajai iestādei ir akreditēta/apstiprināta KIS.

   [ ] jā, līmenis: ..... [ ] nē.

4. [ ] attiecībā uz iepriekš minēto pieprasījumu ir ierosināts IDP process. Jūs informēs, kad IDP tiks piešķirta vai atteikta.

5. [ ] iepriekš minētajai iestādei nav IDP.

6. Šā IDP apliecinājuma termiņš beidzas: ..... (*dd.mm.gggg.*) vai citā VDI/IDI noteiktā laikā. Ja apliecinājums zaudē derīgumu pirms termiņa beigām vai tiek veiktas izmaiņas iepriekš minētajā informācijā, Jūs informēs.

7. Piezīmes:
   .....

Izdevēja VDI/IDI (nosaukums): ..... *Datums: (dd.mm.gggg.)* .....

<Vietturis atsaucei uz piemērojamajiem persondatu aizsardzības tiesību aktiem un saite uz datu subjektam obligāti sniedzamo informāciju, piemēram, par to, kā tiek īstenots Vispārīgās datu aizsardzības regulas ([13]) 13. pants.>

([13]) Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (OV L 119, 4.5.2016., 1. lpp.).

E papildinājums

Minimālās prasības attiecībā uz elektroniska formāta ESKI aizsardzību, ja ESKI ir klasificēta *RESTREINT UE/EU RESTRICTED* līmenī un ar to rīkojas saņēmēja *KIS* sistēmā

Vispārīga informācija

1. Saņēmējam jābūt atbildīgam par to, lai tiktu nodrošināts, ka tādas informācijas aizsardzība, kas klasificēta *RESTREINT UE/EU RESTRICTED* līmenī, atbilst minimālajām drošības prasībām, kas izklāstītas šajā drošības klauzulā, un visām citām papildu prasībām, kuras ievērot ieteikusi piešķirēja iestāde vai attiecīgā gadījumā valsts drošības iestāde (VDI) vai izraudzītā drošības iestāde (IDI).

2. Saņēmēja pienākums ir izpildīt šajā dokumentā noteiktās drošības prasības.

3. Šā dokumenta izpratnē komunikācijas un informācijas sistēma (KIS) aptver visu aprīkojumu, ko izmanto, lai rīkotos ar ESKI, to uzglabātu un nosūtītu, tostarp darbstacijas, printerus, kopēšanas iekārtas, faksa aparātus, serverus, tīkla pārvaldības sistēmas, tīkla vadības ierīces un sakaru vadības ierīces, klēpjdatorus, piezīmjdatorus, planšetdatorus, viedtālruņus un tādus noņemamus informācijas nesējus kā *USB* atmiņas kartes, kompaktdiski, *SD* kartes u. c.

4. Īpašais aprīkojums, piemēram, kriptogrāfijas produkti, ir jāaizsargā saskaņā ar īpašām drošības darba procedūrām (*SecOPs*).

5. Saņēmējam ir jāizveido struktūra, kas atbild par tādas KIS drošības pārvaldību, kurā rīkojas ar informāciju, kas klasificēta *RESTREINT UE/EU RESTRICTED* līmenī, un ir jāieceļ drošības speciālists, kurš atbild par attiecīgo iestādi.

6. Nav atļauts izmantot saņēmēja darbiniekiem privāti piederošus IT risinājumus (aparatūru, programmatūru vai pakalpojumus), lai glabātu informāciju, kas klasificēta *RESTREINT UE/EU RESTRICTED* līmenī, vai rīkotos ar to.

7. Saņēmēja KIS sistēmas, kurā rīkojas ar *RESTREINT UE/EU RESTRICTED* līmenī klasificētu informāciju, akreditācija ir jāapstiprina attiecīgās dalībvalsts drošības akreditācijas iestādei (DAI) vai jādeleģē saņēmēja drošības speciālistam, ja tas ir atļauts valsts normatīvajos aktos.

8. Ja informācija ir klasificēta *RESTREINT UE/EU RESTRICTED* līmenī un ir šifrēta, izmantojot apstiprinātus kriptogrāfijas produktus, ar to var rīkoties, to var uzglabāt vai nosūtīt (izmantojot vadu vai bezvadu līdzekļus) kā jebkuru citu neklasificētu informāciju saskaņā ar dotācijas nolīgumu. Šādiem kriptogrāfijas produktiem ir jābūt apstiprinātiem ES vai dalībvalstī.

9. Ārējām iestādēm, kas iesaistītas tehniskajā apkopē/remontdarbos, ir jābūt līgumiskam pienākumam pildīt piemērojamos noteikumus par rīkošanos ar informāciju, kas klasificēta *RESTREINT UE/EU RESTRICTED* līmenī, kā noteikts šajā dokumentā.

10. Pēc piešķirējas iestādes vai attiecīgās VDI, IDI vai DAI pieprasījuma saņēmējam ir jāiesniedz pierādījums par atbilstību dotācijas nolīguma drošības klauzulai. Ja ir nepieciešama arī saņēmēja procesu un iestāžu revīzija un pārbaude, lai nodrošinātu atbilstību šīm prasībām, saņēmēji atļauj piešķirējas iestādes, VDI, IDI un/vai DAI, vai attiecīgās ES drošības iestādes pārstāvjiem veikt šādu revīziju un pārbaudi.

Fiziskā drošība

11. Zonas, kurās izmanto KIS, lai parādītu, uzglabātu, apstrādātu vai nosūtītu informāciju, kas klasificēta *RESTREINT UE/EU RESTRICTED* līmenī, vai zonas, kurās atrodas šādas KIS serveri, tīkla pārvaldības sistēmas, tīkla vadības ierīces un komunikācijas vadības ierīces, būtu jānosaka par atsevišķām un kontrolētām zonām ar atbilstošu piekļuves kontroles sistēmu. Piekļūt šādām atsevišķām un kontrolētām zonām drīkstētu vienīgi personas ar īpašu atļauju. Neskarot 8. punktu, 3. punktā minētais aprīkojums ir jāglabā šādās atsevišķās un kontrolētās zonās.

12. Ir jāievieš drošības mehānismi un/vai procedūras, lai regulētu noņemamu elektronisko informācijas nesēju (piemēram, *USB* atslēgu, lielapjoma atmiņas ierīču vai pārrakstāmu kompaktdisku) ievietošanu KIS vai pieslēgšanu KIS komponentiem.

Piekļuve KIS

13. Piekļūt saņēmēja KIS, kurā rīkojas ar ESKI, drīkst vienīgi tad, ja ir vajadzība pēc informācijas un personāls ir saņēmis atļauju.

14. Visām KIS ir jābūt atjauninātiem pilnvaroto lietotāju sarakstiem. Katras apstrādes sesijas sākumā visi lietotāji ir jāautentificē.

15. Parolēs, kas ir vairuma identifikācijas un autentifikācijas drošības pasākumu daļa, ir jābūt vismaz deviņām rakstzīmēm, tostarp cipariem un īpašajiem simboliem (ja sistēma to ļauj), kā arī burtiem. Paroles ir jāmaina ne retāk kā ik pēc 180 dienām. Tās ir jānomaina pēc iespējas drīzāk, ja tās ir apdraudētas vai ir izpaustas nepilnvarotai personai, vai ja ir aizdomas par šādu apdraudējumu vai izpaušanu.

16. Visās KIS ir jābūt ieviestiem iekšējiem piekļuves kontroles pasākumiem, lai nepieļautu, ka nesankcionēti lietotāji piekļūst informācijai, kas klasificēta *RESTREINT UE/EU RESTRICTED* līmenī, vai to izmaina, vai arī izmaina sistēmu un drošības kontroles pasākumus. Lietotāji ir automātiski jāatslēdz no KIS, ja to termināļi ir bijuši neaktīvi kādu iepriekš noteiktu laikposmu, vai KIS pēc 15 minūšu ilgas bezdarbības ir jāaktivizē ekrāna saudzētājs, kuru var atslēgt tikai ar paroli.

17. Katram KIS lietotājam ir piešķirts unikāls lietotāja konts un ID. Lietotāju konti ir automātiski jāslēdz, ja ir bijuši vismaz pieci secīgi neveiksmīgi mēģinājumi ievadīt paroli.

18. Visi KIS lietotāji ir jāinformē par to pienākumiem un procedūrām, kas jāveic, lai KIS aizsargātu informāciju, kas klasificēta *RESTREINT UE/EU RESTRICTED* līmenī. Pienākumi un procedūras, kas jāveic, ir jādokumentē, un lietotājiem to izpilde ir jāapstiprina rakstiski.

19. Lietotājiem un administratoriem ir jābūt pieejamām *SecOPs* procedūrām, un tajās ir jābūt iekļautiem drošības pienākumu aprakstiem un saistītajam uzdevumu, norādījumu un plānu sarakstam.

Uzskaite, revīzija un reaģēšana uz incidentiem

20. Piekļuvei KIS jātiek reģistrētai.

21. Ir jāreģistrē šādi notikumi:

    a) visi veiksmīgie un neveiksmīgie pieslēgšanās mēģinājumi;

    b) atslēgšanās (tostarp attiecīgā gadījumā pārtraukuma dēļ);

    c) piekļuves tiesību un privilēģiju izveide, dzēšana vai maiņa;

    d) paroļu izveide, dzēšana vai maiņa.

22. Visos iepriekš uzskaitītajos gadījumos ir jāpaziņo vismaz šāda informācija:

    a) notikuma veids;

    b) lietotāja ID numurs;

    c) datums un laiks;

    d) ierīces ID numurs.

23. Protokoliem būtu jāpalīdz drošības speciālistam pārbaudīt iespējamos drošības incidentus. Tos var izmantot arī juridiskas izmeklēšanas atbalstam drošības incidenta gadījumā. Visi drošības ieraksti būtu regulāri jāpārbauda, lai konstatētu iespējamos drošības incidentus. Protokoli ir jāaizsargā no nesankcionētas dzēšanas vai izmaiņu veikšanas tajos.

24. Saņēmējam ir jānodrošina, ka ir ieviesta reaģēšanas stratēģija, kā rīkoties drošības incidentu gadījumā. Lietotāji un administratori ir jāinstruē par to, kā reaģēt uz incidentiem, kā par tiem ziņot un ko darīt ārkārtas situācijā.

25. Par informācijas, kas klasificēta *RESTREINT UE/EU RESTRICTED* līmenī, apdraudējumu vai iespējamu apdraudējumu ir jāziņo piešķīrējai iestādei. Ziņojumam ir jāietver iesaistītās informācijas apraksts un apdraudējuma vai aizdomu par apdraudējumu apstākļu apraksts. Visiem KIS lietotājiem ir jāzina, kā ziņot drošības speciālistam par jebkādu faktisku drošības incidentu vai aizdomām par drošības incidentu.

Saziņa tīklā un starpsavienojumi

26. Ja saņēmēja KIS, kurā rīkojas ar informāciju, kas klasificēta *RESTREINT UE/EU RESTRICTED* līmenī, ir savienota ar KIS, kas nav akreditēta, tas būtiski palielina draudus gan KIS drošībai, gan tās informācijas drošībai, kas klasificēta *RESTREINT UE/EU RESTRICTED* līmenī un ar ko rīkojas šajā KIS. Tas ietver internetu un citas publiskas vai privātas KIS, piemēram, citu attiecīgajam saņēmējam vai apakšuzņēmējam piederošu KIS. Šajā gadījumā saņēmējam ir jāveic riska novērtējums, lai identificētu papildu drošības prasības, kuras ir jāizpilda drošības akreditācijas procesā. Saņēmējs iesniedz piešķīrējai iestādei un, ja tas paredzēts valsts normatīvajos aktos, kompetentajai valsts DAI paziņojumu par atbilstību, apliecinot, ka saņēmēja KIS un attiecīgie starpsavienojumi ir akreditēti tā, lai tajos varētu rīkoties ar ESKI, kas klasificēta *RESTREINT UE/EU RESTRICTED* līmenī.

27. Ir aizliegta attālināta piekļuve no citām sistēmām lokālo tīklu (*LAN*) pakalpojumiem (piemēram, attālināta piekļuve e-pastam un attālināts sistēmas atbalsts), izņemot gadījumus, ja ir veikti īpaši drošības pasākumi, par kuriem ir panākta vienošanās ar piešķīrēju iestādi, kā arī ir saņemts kompetentās DAI apstiprinājums, ja tas ir prasīts valsts normatīvajos aktos.

Konfigurācijas vadība

28. Jābūt pieejamai un regulāri jātiek atjauninātai detalizētai aparatūras un programmatūras konfigurācijai, kas atspoguļota akreditācijas/apstiprinājuma dokumentācijā (tostarp sistēmas un tīkla diagrammās).

29. Saņēmēja drošības speciālistam ir jāveic aparatūras un programmatūras konfigurācijas pārbaudes, lai nodrošinātu, ka nav ieviesta neatļauta aparatūra vai programmatūra.

30. Ir jānovērtē saņēmēja KIS konfigurācijā veikto izmaiņu ietekme uz drošību, un šīs izmaiņas ir jāapstiprina drošības speciālistam un, ja tas ir paredzēts valsts normatīvajos aktos, arī DAI.

31. Vismaz reizi ceturksnī sistēma ir rūpīgi jāskenē, lai noteiktu drošības nepilnības. Ir jāuzstāda un regulāri jāatjaunina programmatūra ļaunprogrammatūras atklāšanai. Ja iespējams, šādai programmatūrai ir jābūt apstiprinātai valsts vai starptautiskā līmenī, vai arī tai būtu jāatbilst vispārpieņemtam nozares standartam.

32. Saņēmējam ir jāizstrādā darbības nepārtrauktības plāns. Ir jāievieš dublēšanas procedūras, lai izpildītu:

    a) prasības attiecībā uz dublēšanas biežumu;

    b) prasības attiecībā uz uzglabāšanu uz vietas (ugunsdrošos konteineros) vai citur;

    c) prasības attiecībā uz kontrolētu sankcionētu piekļuvi rezerves kopijām.

Dzēšana un iznīcināšana

33. Ja KIS vai datu nesējos jebkad ir bijusi informācija, kas klasificēta *RESTREINT UE/EU RESTRICTED* līmenī, visā sistēmā vai datu nesējā pirms tā iznīcināšanas ir jāveic šādas dzēšanas darbības:

    a) zibatmiņa (piemēram, *USB* atmiņas kartes, *SD* kartes, cietvielu diski, hibrīdi cietie diski) ir jāpārraksta vismaz trīs reizes un pēc tam ir jāpārbauda, lai pārliecinātos, ka sākotnējo saturu nav iespējams atgūt, vai ir jāizdzēš, izmantojot apstiprinātu dzēšanas programmatūru;

    b) magnētiskās ierīces (piemēram, cietie diski) ir jāpārraksta vai jādemagnetizē;

    c) optiskās ierīces (piemēram, kompaktdiski un *DVD*) ir jāsasmalcina vai jāsadala;

    d) citu datu nesēju gadījumā būtu jāapspriežas ar piešķirēju iestādi vai attiecīgā gadījumā VDI, IDI vai DAI par to, kādas drošības prasības ir jāizpilda.

34. Informācija, kas klasificēta *RESTREINT UE/EU RESTRICTED* līmenī, ir jāizdzēš no visiem datu nesējiem pirms to nodošanas kādai struktūrai, kura nav pilnvarota piekļūt informācijai, kas klasificēta *RESTREINT UE/EU RESTRICTED* līmenī (piemēram, lai veiktu tehnisko apkopi).

IV PIELIKUMS

Labuma guvēju vai apakšuzņēmēju iestādes un personāla drošības pielaide, kas saistīta ar informāciju, kura klasificēta *RESTREINT UE/EU RESTRICTED* līmenī, un VDI/IDI, kurām ir jāpaziņo par dotāciju nolīgumiem, kas klasificēti *RESTREINT UE/EU RESTRICTED* līmenī [1]

Dalībvalsts	IDP		VDI un/vai IDI informēšana par dotācijas nolīgumu vai apakšlīgumu, kas saistīts ar informāciju, kura klasificēta *R-UE/EU-R* līmenī		PDP	
	JĀ	NĒ	JĀ	NĒ	JĀ	NĒ
Beļģija		**X**		**X**		**X**
Bulgārija		**X**		**X**		**X**
Čehija		**X**		**X**		**X**
Dānija	**X**		**X**		**X**	
Vācija		**X**		**X**		**X**
Igaunija	**X**		**X**			**X**
Īrija		**X**		**X**		**X**
Grieķija	**X**			**X**	**X**	
Spānija		**X**	**X**			**X**
Francija		**X**		**X**		**X**
Horvātija		**X**	**X**			**X**
Itālija		**X**	**X**			**X**
Kipra		**X**	**X**			**X**
Latvija		**X**		**X**		**X**
Lietuva	**X**		**X**			**X**
Luksemburga	**X**		**X**		**X**	
Ungārija		**X**		**X**		**X**
Malta		**X**		**X**		**X**
Nīderlande	**X** (tikai ar aizsardzību saistītiem dotāciju nolīgumiem un apakšlīgumiem)		**X** (tikai ar aizsardzību saistītiem dotāciju nolīgumiem un apakšlīgumiem)			**X**
Austrija		**X**		**X**		**X**
Polija		**X**		**X**		**X**

[1] Ar šīm valsts prasībām attiecībā uz IDP/PDP un paziņošanu par dotāciju nolīgumiem, kas saistīti ar informāciju, kura klasificēta *RESTREINT UE / EU RESTRICTED* līmenī, nedrīkst uzlikt nekādus papildu pienākumus citām dalībvalstīm vai labuma guvējiem un apakšuzņēmējiem to jurisdikcijā.
NB! Paziņošana par dotāciju nolīgumiem, kas saistīti ar informāciju, kura klasificēta *CONFIDENTIEL UE/EU CONFIDENTIAL* un *SECRET UE/EU SECRET* līmenī, ir obligāta.

Portugāle		**X**		**X**		**X**
Rumānija		**X**		**X**		**X**
Slovēnija	**X**		**X**			**X**
Slovākija	**X**		**X**			**X**
Somija		**X**		**X**		**X**
Zviedrija		**X**		**X**		**X**

V PIELIKUMS

PAR APSTRĀDES PROCEDŪRĀM, KAS SAISTĪTAS AR INDUSTRIĀLO DROŠĪBU, ATBILDĪGO VALSTS DROŠĪBAS IESTĀŽU / IZRAUDZĪTO DROŠĪBAS IESTĀŽU STRUKTŪRVIENĪBU SARAKSTS

BEĻĢIJA

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

Tālr.: +32 25014542 (sekretariāts)

Fakss: +32 25014596

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

BULGĀRIJA

1. State Commission on Information Security - National Security Authority
   4 Kozloduy Street
   1202 Sofia
   Tālr.: +359 29835775
   Fakss: +359 29873750
   E-pasts: dksi@government.bg

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

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

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

(Iepriekš uzskaitītās kompetentās iestādes veic drošības pārbaudes procedūras attiecībā uz IDP izdošanu juridiskām personām, kuras piesakās noslēgt klasificētu līgumu, un PDP izdošanu privātpersonām, kas pilda klasificētu līgumu šo iestāžu vajadzībām.)

5. State Agency National Security (security service)

   45 Cherni Vrah Blvd.
   1407 Sofia

   Tālr.: +359 28147109

   Fakss: +359 29632188, +359 28147441

   E-pasts: dans@dans.bg

(Iepriekš minētais drošības dienests veic drošības pārbaudes procedūras attiecībā uz IDP un PDP izdošanu visām pārējām juridiskajām personām un privātpersonām valstī, kas piesakās noslēgt klasificētu līgumu vai klasificētu dotācijas nolīgumu vai pilda klasificētu līgumu vai klasificētu dotācijas nolīgumu.)

ČEHIJA

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

Tālr.: +420 257283129

E-pasts: sbr@nbu.cz

DĀNIJA

1. Politiets Efterretningstjeneste
   (Danish Security Intelligence Service)

   Klausdalsbrovej 1

   2860 Søborg

   Tālr.: +45 33148888

   Fakss: +45 33430190

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

   Tālr.: +45 33325566

   Fakss: +45 33931320

VĀCIJA

1. Attiecībā uz jautājumiem saistībā ar industriālās drošības politiku, IDP, transportēšanas plāniem (izņemot kripto/KKR):
   Federal Ministry for Economic Affairs and Energy

   Industrial Security Division - RS3

   Villemombler Str. 76

   53123 Bonn

   Tālr.: +49 228996154028

   Fakss: +49 228996152676

   E-pasts: dsagermany-rs3@bmwi.bund.de (biroja e-pasta adrese)

2. Attiecībā uz standarta apmeklējumu pieprasījumiem, ko nosūta/saņem Vācijas uzņēmumi:

Federal Ministry for Economic Affairs and Energy

Industrial Security Division – RS2
Villemombler Str. 76
53123 Bonn

Tālr.: +49 228996152401

Fakss: +49 228996152603

E-pasts: rs2-international@bmwi.bund.de (biroja e-pasta adrese)

3. Attiecībā uz kriptomateriālu transportēšanas plāniem:

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

Tālr.: +49 2289995826052

Fakss: +49 228991095826052

E-pasts: NDAEU@bsi.bund.de

IGAUNIJA

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

Tālr.: +372 6939211

Fakss: +372 6935001

E-pasts: nsa@fis.gov.ee

ĪRIJA

National Security Authority Ireland
Department of Foreign Affairs and Trade
76-78 Harcourt Street
Dublin 2
D02 DX45

Tālr.: +353 14082724

E-pasts: nsa@dfa.ie

GRIEĶIJA

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

Tālr.: +30 2106572022, +30 2106572178

Fakss: +30 2106527612

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

SPĀNIJA

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

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

Fakss: +34 913725808

E-pasts: nsa-sp@areatec.com

Attiecībā uz jautājumiem par personāla drošības pielaidi: programas.ons@areatec.com

Jautājumi par personāla drošības pielaidi: hps.ons@areatec.com

Attiecībā uz transportēšanas plāniem un starptautiskiem apmeklējumiem: sp-ivtco@areatec.com

FRANCIJA

Valsts drošības iestāde (VDI) (attiecībā uz policiju un īstenošanu jomās, kas nav aizsardzības nozare)
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

Tālr.: +33 171758193

Fakss: +33 171758200

E-pasts: ANSFrance@sgdsn.gouv.fr

Izraudzītā drošības iestāde (attiecībā uz īstenošanu aizsardzības nozarē)
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

Tālr.: +33 988670421

E-pasts: veidlapām un nosūtāmajiem AP: dga-ssdi.ai.fct@intradef.gouv.fr

ienākošajiem AP: dga-ssdi.visit.fct@intradef.gouv.fr

HORVĀTIJA

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

Tālr.: +385 14681222

Fakss: +385 14686049

E-pasts: NSACroatia@uvns.hr

ITĀLIJA

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

Tālr.: +39 0661174266

Fakss: +39 064885273

KIPRA

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

Tālr.: +357 22807569, +357 22807764

Fakss: +357 22302351

E-pasts: cynsa@mod.gov.cy

Ministry of Defence
National Security Authority (NSA)
172-174, Strovolos Avenue
2048 Strovolos, Nicosia

Tālr.: +357 22807569, +357 22807764

Fakss: +357 22302351

E-pasts: cynsa@mod.gov.cy

LATVIJA

National Security Authority
Constitution Protection Bureau of the Republic of Latvia
P.O. Box 286
Riga LV-1001

Tālr.: +371 67025418, +371 67025463

Fakss: +371 67025454

E-pasts: ndi@sab.gov.lv, ndi@zd.gov.lv

LIETUVA

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

Tālr.: +370 70666128

E-pasts: nsa@vsd.lt

LUKSEMBURGA

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

Tālr.: +352 24782210

E-pasts: ans@me.etat.lu

UNGĀRIJA

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

Tālr.: +36 13911862

Fakss: +36 13911889

E-pasts: 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

Tālr.: +356 23952000

Fakss: +356 21242406

E-pasts: certification@mccaa.org.mt

NĪDERLANDE

1. Ministry of the Interior and Kingdom Relations

   PO Box 20010
   2500 EA The Hague

   Tālr.: +31 703204400

   Fakss: +31 703200733

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

2. Ministry of Defence

   Industrial Security Department

   PO Box 20701
   2500 ES The Hague

   Tālr.: +31 704419407

   Fakss: +31 703459189

   E-pasts: indussec@mindef.nl

AUSTRIJA

1. Federal Chancellery of Austria

   Department I/10, Federal Office for Information Security

   Ballhausplatz 2
   10104 Vienna

   Tālr.: +43 153115202594

   E-pasts: isk@bka.gv.at

2. IDI militārajā jomā:

   BMLV/Abwehramt

   Postfach 2000
   1030 Vienna

   E-pasts: abwa@bmlvs.gv.at

POLIJA

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

Tālr.: +48 225857944

Fakss: +48 225857443

E-pasts: nsa@abw.gov.pl

PORTUGĀLE

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

Tālr.: +351 213031710

Fakss: +351 213031711

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

RUMĀNIJA

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

Tālr.: +40 212075115

Fakss: +40 212245830

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

SLOVĒNIJA

Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
1000 Ljubljana

Tālr.: +386 14781390

Fakss: +386 14781399

E-pasts: gp.uvtp@gov.si

SLOVĀKIJA

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

Tālr.: +421 268691111

Fakss: +421 268691700

E-pasts: podatelna@nbu.gov.sk

SOMIJA

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

E-pasts: NSA@formin.fi

ZVIEDRIJA

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

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