EIROPAS
KOMISIJA

Briselē, 7.2.2013
COM(2013) 48 final

2013/0027 (COD)

Priekšlikums

EIROPAS PARLAMENTA UN PADOMES DIREKTĪVA

par pasākumiem, kas nodrošinātu vienādi augsta līmeņa tīklu un informācijas drošību visā Savienībā

{SWD(2013) 31 final}
{SWD(2013) 32 final}

PASKAIDROJUMA RAKSTS

Šī direktīvas priekšlikuma mērķis ir nodrošināt vienādi augsta līmeņa tīklu un informācijas drošību (TID). Tas nozīmē, ka jāpalielina mūsu sabiedrībai un ekonomikai vitāli nepieciešamā interneta un privāto tīklu, un informācijas sistēmu drošība. Tas tiks panākts, pieprasot dalībvalstīm palielināt savu sagatavotības līmeni un uzlabot savstarpējo sadarbību, kā arī pieprasot kritiskās infrastruktūras (piemēram, enerģētika, transports) apsaimniekotājiem un nozīmīgākajiem informācijas sabiedrības pakalpojumu (e-tirdzniecības platformas, sociālie tīkli utt.) sniedzējiem, kā arī valsts pārvaldes iestādēm veikt piemērotus pasākumus, lai pārvaldītu drošības riskus, un par nopietniem incidentiem paziņot valsts kompetentajām iestādēm.

Šis priekšlikums iesniegts saistībā ar paziņojumu par Eiropas kiberdrošības stratēģiju, ko kopīgi sagatavojusi Komisija un Savienības Augstā pārstāve ārlietās un drošības politikas jautājumos. Stratēģijas mērķis ir nodrošināt drošu un uzticamu digitālo vidi, vienlaikus sekmējot un aizsargājot pamattiesības un citas ES pamatvērtības. Šis priekšlikums ir galvenais stratēģijā paredzētais pasākums. Citas stratēģijā paredzētās darbības šajā jomā ir orientētas uz informētības palielināšanu, kiberdrošības produktu un pakalpojumu iekšējā tirgus izveidi, kā arī ieguldījumu sekmēšanu pētniecībā un izstrādē. Šīs darbības papildinās citas, kuru mērķis ir pastiprināt kibernoziedzības apkarošanu un ES starptautiskas kiberdrošības politikas izveidi.

1.1. Priekšlikuma pamatojums un mērķi

TID kļūst aizvien nozīmīgāks jautājums mūsu ekonomikas un sabiedrības kontekstā. TID ir arī būtisks priekšnoteikums, lai izveidotu uzticamu vidi globālās pakalpojumu tirdzniecības jomā.Tomēr informācijas sistēmas var apdraudēt drošības incidenti, piemēram, tādi, ko izraisījušas cilvēka kļūdas, dabas parādības, tehniskas nepilnības vai ļaunprātīgi uzbrukumi. Šādi incidenti sastopami arvien biežāk un plašākā mērogā, turklāt tie kļūst sarežģītāki. Pēc Komisijas organizētās sabiedriskās apspriešanas tiešsaistē „Tīklu un informācijas drošības uzlabošana ES”[1] atklājās, ka iepriekšējā gadā 57 % respondentu ir saskārušies ar TID incidentiem, kas būtiski ietekmējis viņu darbību. TID trūkums var apdraudēt izšķirošas nozīmes pakalpojumus, kuri ir atkarīgi no tīklu un informācijas sistēmu integritātes. Tas var arī apturēt uzņēmumu darbību, ES ekonomikai radīt ievērojamus finansiālus zaudējumus un negatīvi ietekmēt sabiedrības labklājību.

Turklāt kā pārrobežu saziņas instruments izmantotās digitālās informācijas sistēmas, jo īpaši internets, ir savstarpēji savienotas visās dalībvalstīs un īpaši nozīmīgas preču un pakalpojumu aprites un personu pārvietošanās sekmēšanā pāri robežām. Šo sistēmu būtiski traucējumi vienā dalībvalstī var ietekmē arī citas dalībvalstis un ES kopumā. Tāpēc tīklu un informācijas sistēmu noturībai un stabilitātei ir būtiska nozīme, lai pabeigtu Eiropas digitālā vienotā tirgus izveidi un nodrošinātu iekšējā tirgus netraucētu darbību. Incidentu iespējamība un biežums un nespēja nodrošināt efektīvu aizsardzību arī iedragā sabiedrības uzticēšanos tīklu un informācijas pakalpojumiem un paļāvību uz tiem; piemēram, 2012. gada Eirobarometra aptaujā par kiberdrošību konstatēts, ka 38 % ES interneta lietotāju ir uztraukušies par tiešsaistes maksājumu drošību un ar drošību saistīto bažu dēļ ir mainījuši savu rīcību: 18 % respondentu varētu mazāk pirkt preces tiešsaistē, un 15 % varētu mazāk izmantot banku pakalpojumus tiešsaistē[2].

Pašreizējos apstākļos Eiropas Savienībā, kuri atspoguļo līdz šim izmantoto pilnībā brīvprātīgo pieeju, nav nodrošināta pietiekama aizsardzība pret TID incidentiem un riskiem visā ES.

---

1 Sabiedriskā apspriešana tiešsaistē „Tīklu un informācijas drošības uzlabošana ES” notika no 2012. gada 23. jūlija līdz 15. oktobrim.

2 *Eurobarometer* aptauja Nr. 390/2012.

Pašreizējās TID spējas un mehānismi gluži vienkārši nav pietiekami, lai neatpaliktu no straujās apdraudējumu attīstības un visās dalībvalstīs nodrošinātu vienlīdz augstu aizsardzības līmeni.

Neraugoties uz sāktajām iniciatīvām, dalībvalstu spēju un sagatavotības līmenis ir ļoti atšķirīgs, visā ES radot sadrumstalotību. Ņemot vērā, ka tīkli un sistēmas ir savstarpēji savienoti, ES vispārējo TID līmeni ir samazinājušas tās dalībvalstis, kurās aizsardzības līmenis nav pietiekami augsts. Šādā situācijā kavēta ir arī uzticības veidošanās speciālistu starpā, kas ir priekšnoteikums sadarbībai un informācijas apmaiņai. Rezultātā sadarbība izveidojusies tikai to nedaudzo dalībvalstu starpā, kurās ir augsta līmeņa spējas.

Tāpēc ES līmenī pagaidām nav izveidots efektīvs mehānisms, kas nodrošinātu efektīvu sadarbību un uzticamas informācijas apmaiņu par TID incidentiem un riskiem dalībvalstīs. Tas var novest pie nekoordinētas regulatīvas iejaukšanās, nesaskaņotām stratēģijām un atšķirīgiem standartiem, kas savukārt radītu nepietiekamu aizsardzību pret TID apdraudējumiem visā ES. Turklāt tas var radīt iekšējā tirgus šķēršļus, radot ar atbilstības nodrošināšanu saistītas izmaksas tiem uzņēmumiem, kuri darbību veic vairāk nekā vienā dalībvalstī.

Visbeidzot, tirgus dalībniekiem, kuri apsaimnieko kritisko infrastruktūru vai sniedz mūsu sabiedrības funkcionēšanai būtiskus pakalpojumus, nav noteikti atbilstīgi pienākumi veikt riska pārvaldības pasākumus un informācijas apmaiņu ar attiecīgajām iestādēm. Tādējādi, no vienas puses, efektīvu stimulu trūkuma dēļ uzņēmumi neveic nopietnu riska pārvaldību, tostarp risku novērtējumu un atbilstīgus pasākumus TID nodrošināšanai. No otras puses, informācija par lielu daļu incidentu nenonāk līdz kompetentajām iestādēm un tiek atstāta bez ievērības. Taču informācija par incidentiem ir svarīga, jo tā liek publiskām iestādēm reaģēt, veikt atbilstošus risku mazināšanas pasākumus un attiecībā uz TID noteikt piemērotas stratēģiskās prioritātes.

Pašreizējais tiesiskais regulējums paredz tikai to, ka telekomunikāciju uzņēmumiem jāpieņem riska pārvaldības pasākumi un jāziņo par nopietniem TID incidentiem. Tomēr no informācijas un komunikācijas tehnoloģiju (IKT) nozares ir atkarīga darbība daudzās citās nozarēs, tāpēc arī to pārstāvjiem būtu jārūpējas par TID. Vairāki konkrētas infrastruktūras nodrošinātāji un pakalpojumu sniedzēji ir īpaši neaizsargāti, jo viņi ir ļoti atkarīgi no pienācīgi strādājošām tīklu un informācijas sistēmām. Šīm nozarēm ir būtiska loma, sniedzot nozīmīgus atbalsta pakalpojumus mūsu ekonomikas un sabiedrības vajadzībām, un šo nozaru sistēmu drošība ir īpaši svarīga iekšējā tirgus darbības nodrošināšanai. Šīs nozares ietver banku nozari, biržas pakalpojumus, enerģijas ražošanu, pārvadi un sadali, transportu (gaisa, dzelzceļa un jūras transports), veselības aprūpi, interneta pakalpojumus un valsts pārvaldes iestādes.

Tādēļ attiecībā uz TID jautājumu risināšanas pieeju ES ir jāpanāk nozīmīgas izmaiņas. Lai radītu vienlīdzīgus konkurences apstākļus un novērstu pašreizējās likumdošanas nepilnības, ir jāievieš regulatīvie pienākumi. Tādēļ, lai atrisinātu šīs problēmas un Eiropas Savienībā palielinātu TID līmeni, direktīvas priekšlikumā ir noteikti šādi mērķi.

Pirmkārt, priekšlikumā noteikts, ka, izveidojot TID kompetentās iestādes, datorapdraudējumu reaģēšanas vienības (*CERT*) un pieņemot valsts TID stratēģijas un valstu TID sadarbības plānus, visām dalībvalstīm jānodrošina minimālais valsts spēju līmenis.

Otrkārt, valsts kompetentajām iestādēm būtu jāsadarbojas vienotā tīklā, kas nodrošinātu drošu un efektīvu koordināciju, tostarp koordinētu informācijas apmaiņu, kā arī atklāšanu un reaģēšanu ES līmenī. Šajā tīklā dalībvalstīm vajadzētu apmainīties ar informāciju un sadarboties, lai apkarotu TID apdraudējumus un incidentus, pamatojoties uz Eiropas TID sadarbības plānu.

Treškārt, pamatojoties uz Elektronisko komunikāciju pamatdirektīvā paredzēto modeli, šā priekšlikuma mērķis ir nodrošināt, ka tiek attīstīta riska pārvaldības kultūra un veikta informācijas apmaiņa starp privāto un publisko sektoru. Uzņēmumiem, kuri darbojas konkrētās kritiskās infrastruktūras nozarēs, kas minētas iepriekš, un valsts pārvaldes iestādēm būs jānovērtē riski, ar ko tie saskaras, un jāpieņem piemēroti un samērīgi pasākumi TID nodrošināšanai. Šīm struktūrvienībām būs jāziņo kompetentajām iestādēm par visiem incidentiem, kas nopietni apdraud to tīklus un informācijas sistēmas un būtiski ietekmē svarīgāko pakalpojumu sniegšanas un preču piegādes nepārtrauktību.

1.2. Vispārīgais konteksts

TID pieaugošo nozīmi Komisija uzsvēra jau 2001. gada paziņojumā „Tīklu un informācijas drošība: priekšlikums Eiropas politikas pieejai”[3]. Vēlāk, 2006. gadā, tika pieņemta Drošas informācijas sabiedrības stratēģija[4], kuras mērķis ir TID kultūras attīstība Eiropā. Tās galvenie elementi tika ietverti Padomes rezolūcijā[5].

Turklāt Komisija 2009. gada 30. martā pieņēma paziņojumu par informācijas kritiskās infrastruktūras aizsardzību (*CIIP*)[6], kurā galvenā uzmanība pievērsta tādai Eiropas aizsardzībai pret kibertraucējumiem, ko sniegtu uzlabota drošība. Paziņojumā ir izklāstīts rīcības plāns, lai atbalstītu dalībvalstu centienus nodrošināt novēršanu un reaģēšanu. Rīcības plāns tika apstiprināts prezidentvalsts secinājumos, ko pieņēma *CIIP* veltītajā ministru konferencē, kas norisinājās 2009. gadā Tallinā. Padome 2009. gada 18. decembrī pieņēma rezolūciju par Eiropas sadarbības pieeju tīklu un informācijas drošībai[7].

2010. gada maijā pieņemtajā Eiropas digitalizācijas programmā[8] (EDP) un ar to saistītajos Padomes secinājumos[9] tika uzsvērta kopīgā izpratne, ka uzticēšanās un drošība ir pamata priekšnoteikumi IKT plašai izvēršanai un līdz ar to stratēģijas „Eiropa 2020”[10] „gudrās izaugsmes” dimensijas mērķu sasniegšanai. Eiropas digitalizācijas programmā, nodaļā „Uzticēšanās un drošība”, ir uzsvērts, ka visām ieinteresētajām personām ir jāapvieno spēki kopīgos centienos, lai nodrošinātu IKT infrastruktūras drošību un noturību, galveno uzmanību pievēršot novēršanai, sagatavotībai un informētībai, kā arī izstrādātu efektīvus un koordinētus drošības mehānismus. Jo īpaši saistībā ar Eiropas digitalizācijas programmas 6. pamatpasākumu pausts aicinājums veikt pasākumus, kuru mērķis ir pastiprināta augsta līmeņa TID politika.

Paziņojumā „Sasniegumi un turpmākie pasākumi – virzība uz globālu kiberdrošību”[11], kas tika pieņemts 2011. gada martā, Komisija apkopoja rezultātus, kuri sasniegti pēc *CIIP* rīcības plāna pieņemšanas 2009. gadā, un secināja: plāna īstenošana ir apliecinājusi, ka drošības un noturības problēmu risināšanā ar valsts pieeju vien nepietiek un ka Eiropai būtu jāturpina veidot saskanīgu un uz sadarbību balstītu pieeju visā ES. Vairākas darbības ir paredzētas 2011. gada *CIIP* paziņojumā, kurā Komisija aicināja dalībvalstis izveidot TID spējas un pārrobežu sadarbību. Lielākā daļa šo darbību bija jāpabeidz līdz 2012. gadam, taču pagaidām tās nav īstenotas.

---

3 COM(2001) 298.
4 COM(2006) 251, http://eur-lex.europa.eu/LexUriServ/site/lv/com/2006/com2006_0251lv01.pdf.
5 2007/068/01.
6 COM(2009) 149.
7 2009/C 321/01.
8 COM(2010) 245.
9 Padomes 2010. gada 31. maija secinājumi par Eiropas digitalizācijas programmu (10130/10).
10 COM(2010) 2020 un Eiropadomes 2010. gada 25. un 26. marta secinājumi (EUCO 7/10).
11 COM(2011) 163.

Eiropas Savienības Padome 2011. gada 27. maija secinājumos par *CIIP* uzsvēra steidzamo vajadzību nodrošināt IKT sistēmu un tīklu noturību un drošību pret visiem iespējamajiem traucējumiem – gan nejaušiem, gan tīšiem, panākt visā ES augsta līmeņa sagatavotību, drošību un noturības spējas, uzlabot tehnisko kompetenci, lai Eiropa varētu atrisināt tīklu un informācijas infrastruktūras aizsardzības problēmu, kā arī sekmēt dalībvalstu sadarbību, izstrādājot ar incidentiem saistītus dalībvalstu sadarbības mehānismus.

1.3. Pašreizējie Eiropas Savienības un starptautiskie noteikumi šajā jomā

Saskaņā ar Regulu (EK) Nr. 460/2004 Eiropas Kopiena 2004. gadā izveidoja Eiropas Tīklu un informācijas drošības aģentūru (*ENISA*)[12], lai sekmētu TID augsta līmeņa aizsardzību un attīstītu TID kultūru ES. Priekšlikums pagarināt *ENISA* pilnvaru termiņu tika pieņemts 2010. gada 30. septembrī[13], un patlaban to apspriež Padome un Eiropas Parlaments. Pārskatītais tiesiskais regulējums par elektroniskajām komunikācijām[14], kas ir spēkā kopš 2009. gada novembra, elektronisko komunikāciju pakalpojumu sniedzējiem uzliek saistības drošības jomā[15]. Valsts līmenī šīs saistības bija jātransponē līdz 2011. gada maijam.

Visiem dalībniekiem, kas ir personas datu pārziņi (piemēram, bankas vai slimnīcas), datu aizsardzības tiesiskais regulējums[16] uzliek pienākumu ieviest drošības pasākumus, lai aizsargātu personas datus. Turklāt saskaņā ar Komisijas 2012. gada priekšlikumu par Vispārīgo datu aizsardzības regulu[17] par personas datu aizsardzības pārkāpumiem datu pārziņiem būtu jāziņo valsts uzraudzības iestādēm. Tas nozīmē, ka, piemēram, par TID drošības pārkāpumu, kas ietekmē pakalpojuma sniegšanu, bet neapdraud personas datus (piemēram, par IKT darbības pārrāvumu energoapgādes uzņēmumā, kas izraisa elektroenerģijas padeves pārrāvumu), nebūtu jāziņo.

Saskaņā ar Direktīvu 2008/114/EK par to, lai apzinātu un noteiktu Eiropas kritiskās infrastruktūras un novērtētu vajadzību uzlabot to aizsardzību, Eiropas programmā kritiskās infrastruktūras aizsardzībai (*EPCIP*)[18] ir izklāstīta visaptveroša pieeja kritisko infrastruktūru aizsardzībai ES. *EPCIP* mērķi ir pilnībā saderīgi ar šo priekšlikumu, un šī direktīva būtu jāpiemēro, neskarot Direktīvu 2008/114/EK. *EPCIP* neuzliek apsaimniekotājiem pienākumu ziņot par būtiskiem drošības pārkāpumiem un ar to nav izveidoti mehānismi dalībvalstu sadarbībai un reaģēšanai incidentu gadījumā.

Likumdevējas iestādes patlaban apspriež Komisijas priekšlikumu direktīvai par uzbrukumiem informācijas sistēmām[19], kuras mērķis ir ieviest saskaņotu pieeju, kā nosakāma krimināltiesību piemērošana par konkrētiem nodarījumu veidiem. Tas attiecas tikai uz krimināltiesību noteikšanu konkrētiem nodarījumu veidiem, bet tajā nav aplūkoti jautājumi par TID risku un incidentu novēršanu, reaģēšanu uz TID incidentiem un to ietekmes mazināšanu. Šī direktīva jāpiemēro, neskarot direktīvu par uzbrukumiem informācijas sistēmām.

Komisija 2012. gada 28. martā pieņēma paziņojumu par Eiropas Kibernoziedzības centra (*EC3*) izveidi[20]. Šis centrs, kas tika izveidots 2013. gada 11. janvārī, ir daļa no Eiropas Policijas biroja (Eiropola) un darbojas kā koordinācijas iestāde kibernoziedzības apkarošanā

---

12 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:LV:HTML.

13 COM(2010) 521.

14 Sk. http://ec.europa.eu/information_society/policy/ecomm/doc/library/regframeforec_dec2009.pdf.

15 Pamatdirektīvas 13.a un 13.b pants.

16 2002. gada 12. jūlija Direktīva 2002/58/EK.

17 COM(2012) 11.

18 COM(2006) 786, http://eur-lex.europa.eu/LexUriServ/site/lv/com/2006/com2006_0786lv01.pdf.

19 COM(2010) 517, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:LV:PDF.

20 COM(2012) 140, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0140:FIN:LV:PDF.

ES. *EC3* izveides mērķis ir apkopot Eiropola īpašās zināšanas kibernoziedzības jomā, lai atbalstītu dalībvalstu spēju veidošanu, sniegtu atbalstu dalībvalstīm kibernoziegumu izmeklēšanā un ciešā sadarbībā ar *Eurojust* par Eiropas kibernoziegumu izmeklētāju ruporu tiesībaizsardzības un tiesu iestādēs.

Eiropas iestādes, aģentūras un organizācijas ir izveidojušas savu Datorapdraudējumu reaģēšanas vienību *CERT-EU*.

Starptautiskā mērogā ES darbs kiberdrošības jomā tiek veikts gan divpusējā, gan daudzpusējā līmenī. 2010. gada ES un ASV augstākā līmeņa sanāksmē[21] tika izveidota ES un ASV darba grupa kiberdrošības un kibernoziedzības jautājumos. ES arī aktīvi darbojas citos daudzpusējos forumos šajā jomā, piemēram, Ekonomiskās sadarbības un attīstības organizācijā (ESAO), Apvienoto Nāciju Organizācijas Ģenerālajā asamblejā (*UNGA*), Starptautiskajā Telesakaru savienībā (*ITU*), Eiropas Drošības un sadarbības organizācijā (EDSO), Pasaules samitā par informācijas sabiedrību (*WSIS*) un Interneta pārvaldības forumā (*IPF*).

2. APSPRIEŠANĀS AR IEINTERESĒTAJĀM PERSONĀM UN IETEKMES NOVĒRTĒJUMI

2.1. Apspriešanās ar ieinteresētajām personām un ekspertu atzinumu izmantošana

Sabiedriskā apspriešanās tiešsaistē „TID uzlabošana ES" norisinājās no 2012. gada 23. jūlija līdz 15. oktobrim. Tiešsaistes aptaujā Komisija kopā saņēma 160 atbildes.
Galvenais secinājums – ieinteresētās personas kopumā atbalsta ideju par to, ka TID jāuzlabo visā ES. Konkrētāk: 82,8 % respondentu pauž viedokli, ka ES valstu valdībām būtu jāpalielina savs ieguldījums, lai nodrošinātu augsta līmeņa TID; 82,8 % uzskata, ka informācijas un sistēmu lietotāji nav bijuši informēti par pastāvošajiem TID apdraudējumiem un incidentiem; 66,3 % respondentu principā atbalsta tādas regulatīvas prasības ieviešamu, kas paredz TID riska pārvaldību; 84,8 % aptaujāto atzīst, ka šādas prasības būtu jānosaka ES līmenī. Liels skaits respondentu domā, ka būtu svarīgi pieņemt TID prasības jo īpaši šādās nozarēs: banku un finanšu nozarē (91,1 %), enerģētikā (89,4 %), transportā (81,7 %), veselības aprūpē (89,4 %), interneta pakalpojumos (89,1 %) un valsts pārvaldē (87,5 %). Respondenti arī uzskata, ka gadījumā, ja tiktu ieviesta prasība par TID drošības pārkāpumiem ziņot valsts kompetentajai iestādei, tad tā būtu jānosaka ES līmenī (65,1 %), un ir pārliecināti, ka šī prasība būtu jāattiecina arī uz valsts pārvaldes iestādēm (93,5 %). Visbeidzot, respondenti apstiprina, ka prasība TID riska pārvaldību īstenot saskaņā ar nozares jaunākajiem sasniegumiem tiem neradītu būtiskas papildu izmaksas (63,4 %) un arī prasība ziņot par drošības pārkāpumiem neradītu būtiskas papildu izmaksas (72,3 %).
Apspriešanās ar dalībvalstīm notika dažādos attiecīgos Padomes sastāvos, Dalībvalstu Eiropas foruma (*EFMS*) kontekstā, konferencē par kiberdrošību, ko 2012. gada 6. jūlijā organizēja Komisija un Eiropas Ārējās darbības dienests, kā arī īpašās divpusējās sanāksmēs, kas tika organizētas pēc atsevišķu dalībvalstu pieprasījuma.

Saistībā ar Eiropas publiskā un privātā sektora partnerību infrastruktūru noturības jautājumos[22] un divpusējās sanāksmēs notika arī apspriedes ar privātā sektora pārstāvjiem. Lai tiktos publiskā sektora pārstāvjiem, Komisija organizēja apspriedes ar *ENISA* un *CERT* ES iestādēm.

2.2. Ietekmes novērtējums

Komisija ir veikusi ietekmes novērtējumu par trim iespējamiem politikas risinājumiem.

---

21 http://europa.eu/rapid/press-release_MEMO-10-597_en.htm.

22 http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r.

Pirmais risinājums – ierastā darbība (pamatscenārijs), proti, tiek saglabāta pašreizējā pieeja.

Otrais risinājums – regulatīvā pieeja, ko veido tiesību akta priekšlikums, ar ko izveido vienotu ES tiesisko regulējumu TID jomā attiecībā uz dalībvalstu spējām, ES līmeņa sadarbības mehānismiem un prasībām, kas jāievēro galvenajiem privātā sektora dalībniekiem un valsts pārvaldes iestādēm.

Trešais risinājums – jauktā pieeja, kas saistībā ar dalībvalstu TID spējām un ES līmeņa sadarbības mehānismiem izstrādātās brīvprātīgās iniciatīvas apvieno ar regulatīvajām prasībām, kuras jāievēro galvenajiem privātā sektora dalībniekiem un valsts pārvaldes iestādēm.

Komisija secināja, ka vislabvēlīgākā ietekme būtu otrajam risinājumam, jo tas ievērojami uzlabotu ES patērētāju, uzņēmumu un valstu valdību aizsardzību pret TID incidentiem. Šie dalībvalstīm uzliktie pienākumi jo īpaši nodrošinātu pienācīgu sagatavotību valsts līmenī un palīdzētu veidot savstarpējas uzticēšanās gaisotni, kas ir priekšnoteikums efektīvai sadarbībai ES līmenī. ES līmeņa sadarbības mehānismu izveide, izmantojot tīklu, nodrošinātu saskaņotu un koordinētu TID incidentu un risku novēršanu un reaģēšanu uz tiem. Ieviešot prasības valsts pārvaldes iestādēm un galvenajiem privātā sektora dalībniekiem veikt TID riska pārvaldību, tiktu radīts spēcīgs stimuls, lai efektīvi pārvaldītu drošības riskus. Pienākums ziņot par TID incidentiem, kuriem ir būtiska ietekme, uzlabotu spēju reaģēt uz incidentiem un sekmētu pārredzamību. Turklāt, ieviešot kārtību Savienības mērogā, ES varētu paplašināt savu ietekmi starptautiskā mērogā un kļūt par vēl uzticamāku partneri divpusējā un daudzpusējā sadarbībā. Tādējādi arī ES spētu daudz labāk veicināt pamattiesības un ES pamatvērtības ārzemēs.

Kvantitatīvajā novērtējumā tika konstatēts, ka otrais risinājums dalībvalstīm neradītu nesamērīgu slogu. Arī privātajam sektoram nerastos lielas izmaksas, jo daudzām attiecīgajām struktūrvienībām jau ir pienākums nodrošināt atbilstību pastāvošajām drošības prasībām (proti, pienākums datu pārziņiem veikt tehniskus un organizatoriskus pasākumus, lai nodrošinātu personas datu aizsardzību, tostarp TID pasākumus). Ņemti vērā arī pašreizējie ar drošību saistītie izdevumi privātajā sektorā.

Šajā priekšlikumā ir ievēroti Eiropas Savienības Pamattiesību hartā atzītie principi, jo īpaši tiesības uz privātās dzīves un saziņas neaizskaramību, personas datu aizsardzība, darījumdarbības brīvība, tiesības uz īpašumu, tiesības uz efektīvu tiesību aizsardzību tiesā un tiesības tikt uzklausītam. Šī direktīva jāīsteno saskaņā ar šīm tiesībām un principiem.

3. PRIEKŠLIKUMA JURIDISKIE ASPEKTI

3.1. Juridiskais pamats

Eiropas Savienība ir pilnvarota paredzēt pasākumus, lai izveidotu iekšējo tirgu vai nodrošinātu tā darbību saskaņā ar attiecīgajiem Līgumu noteikumiem (Līguma par Eiropas Savienības darbību (LESD) 26. pants). Saskaņā ar LESD 114. pantu Savienība var paredzēt „pasākumus, lai *tuvinātu dalībvalstu normatīvos vai administratīvos aktus*, kuri attiecas uz iekšējā tirgus izveidi un darbību".

Kā norādīts iepriekš, tīklu un informācijas sistēmām ir būtiska loma, veicinot preču un pakalpojumu apriti un personu pārvietošanos pāri robežām. Bieži vien minētās sistēmas ir savstarpēji savienotas, un internets būtībā ir globāls. Tā kā šīm sistēmām ir raksturīga transnacionāla dimensija, traucējumi vienā dalībvalstī var ietekmē arī citas dalībvalstis un ES kopumā. Tādēļ tīklu un informācijas sistēmu noturībai un stabilitātei ir būtiska nozīme iekšējā tirgus netraucētas darbības nodrošināšanā.

ES likumdevējs jau ir atzinis nepieciešamību saskaņot TID noteikumus, lai nodrošinātu iekšējā tirgus attīstību. Jo īpaši tas paredzēts Regulā Nr. 460/2004, ar ko izveido *ENISA*[23], pamatojoties uz LESD 114. pantu.

Dalībvalstu atšķirīgais TID valsts spēju, politikas un aizsardzības līmenis ir iemesls nevienlīdzībai, kas rada šķēršļus iekšējā tirgū un veido pamatojumu ES rīcībai.

3.2. Subsidiaritāte

Eiropas iejaukšanos TID jomā pamato subsidiaritātes princips.

Pirmkārt, ņemot vērā TID pārrobežu raksturu, neiejaukšanās ES līmenī radītu situāciju, kurā katra dalībvalsts rīkotos atsevišķi, neņemot vērā ES tīklu un informācijas sistēmu savstarpēju atkarību. Pienācīgs dalībvalstu koordinācijas līmenis nodrošinātu pietiekamu TID riska pārvaldību pārrobežu kontekstā, kurā tie radušies. Atšķirīgais regulējums TID jomā uzņēmumiem rada šķēršli, liedzot tiem darboties vairākās valstīs un panākt apjomradītus ietaupījumus pasaules mērogā.

Otrkārt, lai radītu vienlīdzīgus konkurences apstākļus un novērstu pašreizējās likumdošanas nepilnības, ES līmenī ir jāievieš regulatīvie pienākumi. Izmantojot pilnībā brīvprātīgu pieeju, sadarbība izveidojusies tikai to nedaudzo dalībvalstu starpā, kurās ir augsta līmeņa spējas. Lai panāktu visu dalībvalstu iesaistīšanos, jānodrošina, ka tām visām ir vajadzīgais minimālais spēju līmenis. Valdību pieņemtajiem TID pasākumiem jābūt savstarpēji saskaņotiem un koordinētiem, lai ierobežotu TID incidentu skaitu un līdz minimumam samazinātu to sekas. Apmainoties ar paraugpraksi un pastāvīgi iesaistot *ENISA*, tīklā kompetentās iestādes un Komisija sadarbosies, lai sekmētu direktīvas konsekventu piemērošanu visā ES. Turklāt saskaņoti TID politikas pasākumi var ļoti labvēlīgi ietekmēt pamattiesību efektīvu aizsardzību, jo īpaši saistībā ar tiesībām uz personas datu aizsardzību un privātās dzīves neaizskaramību. Tāpēc ES līmeņa rīcība varētu uzlabot dalībvalstu pašreizējo politikas pasākumu efektivitāti un sekmēt to turpmāku izstrādi.

Ierosinātie pasākumi ir pamatoti arī no proporcionalitātes viedokļa. Dalībvalstīm prasības noteiktas minimālajā nepieciešamajā līmenī, kas jāizpilda, lai nodrošinātu pienācīgu sagatavotību un īstenotu uz uzticēšanos balstītu sadarbību. Tas arī ļauj dalībvalstīm pienācīgi ņemt vērā savas valsts īpašos apstākļus un nodrošina kopējo ES principu samērīgu piemērošanu. Plašā piemērošanas joma ļaus dalībvalstīm īstenot direktīvu atbilstoši faktiskajiem riskiem, ar ko tās saskaras valsts līmenī un kas tiek apzināti valsts TID stratēģijā. Riska pārvaldības īstenošanas prasības izvirzītas tikai kritiskajām struktūrvienībām un paredz tādu pasākumu veikšanu, kas ir samērīgi attiecībā pret riskiem. Sabiedriskajā apspriešanā tika uzsvērts, cik svarīgi ir nodrošināt šo kritisko struktūrvienību drošību. Ziņošanas prasības attiektos vienīgi uz tādiem incidentiem, kuriem ir būtiska ietekme. Kā norādīts iepriekš, pasākumi neradītu nesamērīgas izmaksas, jo lielai daļai šo struktūrvienību un datu pārziņu jau tagad ir jāievēro prasības, kas paredzētas spēkā esošajos datu aizsardzības noteikumos, lai nodrošinātu personas datu aizsardzību.

Lai neradītu nesamērīgu slogu mazajiem apsaimniekotājiem, jo īpaši maziem un vidējiem uzņēmumiem (MVU), prasības ir samērīgas attiecībā pret risku, ko rada attiecīgā tīkla vai informācijas sistēma, un tās nevajadzētu attiecināt uz mikrouzņēmumiem. Riski visupirms jānosaka tām struktūrvienībām, uz kurām attiecas šie pienākumi, un tām arī jāizlemj, kādi pasākumi jāpieņem, lai šos riskus mazinātu.

[23] Eiropas Parlamenta un Padomes 2004. gada 10. marta Regula (EK) Nr. 460/2004, ar ko izveido Eiropas Tīklu un informācijas drošības aģentūru, OV L 077, 13.3.2004., 1. lpp.

TID incidentu un risku pārrobežu aspektu dēļ izvirzītos mērķus var labāk sasniegt ES līmenī, nevis atsevišķās dalībvalstīs. Tāpēc ES var pieņemt pasākumus saskaņā ar Līguma 5. pantā noteikto subsidiaritātes principu. Saskaņā ar proporcionalitātes principu ierosinātā direktīva paredz vienīgi tos pasākumus, kas ir vajadzīgi šo mērķu sasniegšanai.

Lai sasniegtu šos mērķus, būtu jāpilnvaro Komisija pieņemt deleģētos aktus saskaņā ar Līguma par Eiropas Savienības darbību 290. pantu attiecībā uz dažu nebūtisku pamata tiesību akta elementu papildināšanu vai grozīšanu. Komisijas priekšlikums arī cenšas atbalstīt proporcionalitātes principa piemērošanu to pienākumu īstenošanā, kuri uzlikti privātā un publiskā sektora apsaimniekotājiem.

Lai nodrošinātu vienotus nosacījumus pamata tiesību akta īstenošanai, Komisijai būtu jāpiešķir pilnvaras pieņemt īstenošanas aktus atbilstoši Līguma par Eiropas Savienības darbību 291. pantam.

Jo īpaši ņemot vērā ierosinātās direktīvas plašo darbības jomu un to, ka tā attiecas uz stingri reglamentētām jomām, kā arī juridiskās saistības, kas izriet no tās IV nodaļas, paziņojumi par transponēšanas pasākumiem būtu jāpapildina ar skaidrojošiem dokumentiem. Saskaņā ar dalībvalstu un Komisijas 2011. gada 28. septembra kopīgo politisko deklarāciju par skaidrojošiem dokumentiem dalībvalstis ir apņēmušās pamatotos gadījumos paziņojumam par transponēšanas pasākumiem pievienot vienu vai vairākus dokumentus, kuros ir paskaidrota saikne starp direktīvas elementiem un valstu pieņemto transponēšanas instrumentu atbilstošajām daļām. Attiecībā uz šo direktīvu likumdevējs uzskata, ka šādu dokumentu nosūtīšana ir pamatota.

4. IETEKME UZ BUDŽETU

Dalībvalstu sadarbība un informācijas apmaiņa būtu jāatbalsta ar drošu infrastruktūru. Priekšlikums ietekmēs ES budžetu tikai tad, ja dalībvalstis izvēlēsies pielāgot pašreizējo infrastruktūru (piemēram, *sTESTA*), uzdodot Komisijai to īstenot saskaņā ar daudzgadu finanšu shēmu (DFS) 2014.–2020. gadam. Vienreizējās izmaksas tiek lēstas 1 250 000 euro apmērā, un tās būtu jāsedz no ES budžeta, budžeta pozīcijas 09 03 02 (sekmēt valstu publisko tiešsaistes pakalpojumu starpsavienojumus un sadarbspēju, kā arī piekļuvi šādiem tīkliem – 09 03. nodaļa, Eiropas infrastruktūras savienošanas instruments – telekomunikāciju tīkli), ja vien saskaņā ar Eiropas infrastruktūras savienošanas instrumentu (EISI) ir pieejams pietiekams finansējums. Dalībvalstis var arī vienreizējās izmaksas, kas saistītas ar pašreizējās infrastruktūras pielāgošanu, segt kopīgi vai nolemt izveidot jaunu infrastruktūru un segt attiecīgās izmaksas, kas saskaņā ar aplēsēm varētu būt 10 miljonu euro gadā.

2013/0027 (COD)

Priekšlikums

EIROPAS PARLAMENTA UN PADOMES DIREKTĪVA

par pasākumiem, kas nodrošinātu vienādi augsta līmeņa tīklu un informācijas drošību visā Savienībā

EIROPAS PARLAMENTS UN EIROPAS SAVIENĪBAS PADOME,

ņemot vērā Līgumu par Eiropas Savienības darbību un jo īpaši tā 114. pantu,

ņemot vērā Eiropas Komisijas priekšlikumu,

pēc leģislatīvā akta projekta nosūtīšanas valstu parlamentiem,

ņemot vērā Eiropas Ekonomikas un sociālo lietu komitejas atzinumu[1],

pēc apspriešanās ar Eiropas Datu aizsardzības uzraudzītāju,

rīkojoties saskaņā ar parasto likumdošanas procedūru,

tā kā:

(1) Tīklu un informācijas sistēmām un pakalpojumiem ir liela nozīme sabiedrībā. To uzticamība un drošība ir būtiska saimnieciskajā darbībā, sociālās labklājības jomā un jo īpaši iekšējā tirgus darbībā.

(2) Apzinātu vai nejaušu drošības incidentu apmērs un biežums pieaug un veido nopietnu draudu tīklu un informācijas sistēmu darbībai. Šādi incidenti var kavēt ekonomisku darbību veikšanu, radīt ievērojamus finansiālus zaudējumus, apdraudēt lietotāju uzticēšanos un radīt lielus zaudējumus Savienības ekonomikā.

(3) Kā saziņas līdzeklim bez robežām digitālās informācijas sistēmām un galvenokārt internetam ir būtiska nozīme, veicinot preču, pakalpojumu brīvu apriti un personu brīvu pārvietošanos pāri robežām. Starpvalstu rakstura dēļ šo sistēmu būtiski traucējumi vienā dalībvalstī var ietekmēt arī citas dalībvalstis un Savienību kopumā. Tāpēc tīklu un informācijas sistēmu noturībai un stabilitātei ir būtiska nozīme iekšējā tirgus netraucētas darbības nodrošināšanā.

(4) Būtu jāizveido sadarbības mehānisms Savienības līmenī, lai varētu veikt informācijas apmaiņu un saskaņotu atklāšanu un reaģēšanu attiecībā uz tīklu un informācijas drošību (TID). Lai šis mehānisms būtu efektīvs un iekļaujošs, ir svarīgi, lai visām dalībvalstīm būtu minimālas spējas un stratēģija, kas nodrošina augsta līmeņa TID to teritorijā. Minimālās drošības prasības būtu jāattiecina arī uz arī valsts pārvaldes iestādēm un informācijas kritisko infrastruktūru apsaimniekotājiem, lai veicinātu riska pārvaldības kultūru un nodrošinātu ziņošanu par nopietnākajiem incidentiem.

(5) Lai aptvertu visus attiecīgos incidentus un riskus, šī direktīva būtu jāpiemēro visām tīklu un informācijas sistēmām. Valsts pārvaldes iestādēm un tirgus dalībniekiem uzticētos pienākumus tomēr nebūtu jāattiecina uz uzņēmumiem, kas nodrošina publisko komunikāciju tīklus vai sniedz publiski pieejamus elektronisko komunikāciju

[1] OV C […]., […]., […]. lpp.

pakalpojumus Eiropas Parlamenta un Padomes 2002. gada 7. marta Direktīvas 2002/21/EK par kopējiem reglamentējošiem noteikumiem attiecībā uz elektronisko komunikāciju tīkliem un pakalpojumiem (pamatdirektīva)[2] nozīmē, uz kuriem attiecas konkrētas drošības un integritātes prasības, kas noteiktas minētās direktīvas 13.a pantā, un minētie pienākumi nebūtu jāattiecina arī uz uzticamības pakalpojumu sniedzējiem.

(6) Esošās spējas nav pietiekamas, lai Savienībā nodrošinātu augsta līmeņa TID. Dalībvalstīm ir ļoti atšķirīgu līmeņu sagatavotība, kas nozīmē, ka Eiropas Savienībā tiek izmantotas atšķirīgas pieejas. Tas Savienībā rada nevienlīdzīgu patērētāju un uzņēmumu aizsardzības līmeni un pazemina TID kopējo līmeni. Savukārt kopīgu minimālo prasību trūkums valsts pārvaldes iestādēm un tirgus dalībniekiem padara neiespējamu efektīva vispārēja sadarbības mehānisma izveidi Savienības līmenī.

(7) Tāpēc, lai efektīvi reaģētu uz tīklu un informācijas sistēmu drošības problēmām, ir nepieciešama Savienības līmeņa vispārēja pieeja, kurā iekļautas kopīgas minimālās prasības attiecībā uz spēju veidošanu un plānošanu, informācijas apmaiņa un darbību koordinēšana, un kopīgas minimālās drošības prasības visiem attiecīgajiem tirgus dalībniekiem un valsts pārvaldes iestādēm.

(8) Šīs direktīvas noteikumiem nebūtu jāskar iespēja katrai dalībvalstij veikt vajadzīgos pasākumus, lai nodrošinātu savu būtisko drošības interešu aizsardzību, sabiedrisko kārtību un sabiedrības drošību, ļautu izmeklēt un atklāt noziedzīgus nodarījumus un sodīt par tiem. Saskaņā ar LESD 346. pantu dalībvalstīm nav jāsniedz informācija, kuras izpaušanu tās atzīst par būtisku savas drošības interešu apdraudējumu.

(9) Lai panāktu un uzturētu vienādi augsta līmeņa tīklu un informācijas sistēmu drošību, katrai dalībvalstij būtu vajadzīga valsts TID stratēģija, kurā noteikti stratēģiskie mērķi un konkrēti politikas pasākumi, kas jāievieš. Valsts līmenī ir jāizstrādā pamatprasībām atbilstīgi TID sadarbības plāni, lai panāktu tādu reaģēšanas spēju līmeni, kas incidentu gadījumos ļautu efektīvi un lietderīgi sadarboties valsts un Savienības līmenī.

(10) Lai varētu efektīvi īstenot noteikumus, kas pieņemti saskaņā ar šo direktīvu, katrā dalībvalstī būtu jāizveido vai jānosaka struktūra, kas atbildētu par TID jautājumu koordināciju un darbotos kā kontaktpunkts pārrobežu sadarbībai Savienības mērogā. Šīm iestādēm būtu jāpiešķir pietiekami tehniskie, finanšu un cilvēkresursi, lai nodrošinātu, ka tās efektīvi un produktīvi var veikt tām uzticētos uzdevumus un tādējādi sasniegt šīs direktīvas mērķus.

(11) Visās dalībvalstīs ir jābūt atbilstošam aprīkojumam gan tehnisko, gan organizatorisko spēju ziņā, lai novērstu un atklātu tīklu un informācijas sistēmu incidentus un riskus, reaģētu uz tiem un tos mazinātu. Tāpēc visās dalībvalstīs būtu jāizveido labi funkcionējošas, pamatprasībām atbilstošas datorapdraudējumu reaģēšanas vienības, lai nodrošinātu efektīvas un saderīgas spējas incidentu risināšanai un risku novēršanai un efektīvas sadarbības nodrošināšanai Savienības līmenī.

(12) Balstoties uz Dalībvalstu Eiropas forumā (*EFMS*) panākto ievērojamo progresu diskusiju un politikas paraugprakses apmaiņas veicināšanā, tostarp principu izstrādē attiecībā uz Eiropas sadarbību kiberkrīžu jomā, dalībvalstīm un Komisijai vajadzētu izveidot tīklu, lai panāktu pastāvīgu komunikāciju starp tām un palīdzētu īstenot to sadarbību. Šai drošajai un efektīvajai sadarbības sistēmai būtu jāļauj īstenot strukturētu un koordinētu informācijas apmaiņu, atklāšanu un reaģēšanu Savienības līmenī.

[2] OV L 108, 24.4.2002., 33. lpp.

(13) Eiropas Tīklu un informācijas drošības aģentūrai (*ENISA*) būtu jāpalīdz dalībvalstīm un Komisijai, sniedzot savas zināšanas un konsultācijas un sekmējot apmaiņu ar paraugpraksi. Jo īpaši Komisijai būtu jāapspriežas ar *ENISA* saistībā ar šīs direktīvas piemērošanu. Lai nodrošinātu efektīvu un savlaicīgu informāciju dalībvalstīm un Komisijai, sadarbības tīklā būtu jāievieš agrīnā brīdināšana par incidentiem un riskiem. Lai uzlabotu spējas un zināšanas dalībvalstu vidū, sadarbības tīklam būtu jākalpo arī kā paraugprakses apmaiņas instrumentam, palīdzot tā dalībniekiem veidot spējas, vadot salīdzinošās izvērtēšanas un TID mācību organizēšanu.

(14) Būtu jāievieš droša informācijas apmaiņas infrastruktūra, lai sadarbības tīklā varētu apmainīties ar sensitīvu un konfidenciālu informāciju. Neskarot dalībvalstu pienākumu ziņot par Savienības mēroga incidentiem un riskiem sadarbības tīklam, piekļuve konfidenciālai informācijai no citām dalībvalstīm būtu jāpiešķir dalībvalstij tikai tad, ja tā pierāda, ka tās tehniskie, finanšu un cilvēkresursi un procesi, kā arī to komunikācijas infrastruktūra nodrošina efektīvu un drošu to līdzdalību tīklā.

(15) Tā kā tīklu un informācijas sistēmu lielākā daļa tiek privāti apsaimniekota, ir būtiska publiskā un privātā sektora sadarbība. Tirgus dalībnieki būtu jāmudina izmantot savus neformālās sadarbības mehānismus, lai nodrošinātu TID. Tiem būtu jāsadarbojas arī ar publisko sektoru un jāapmainās ar informāciju un paraugpraksi, par to saņemot operatīvo atbalstu incidenta gadījumā.

(16) Lai nodrošinātu pārredzamību un pienācīgi informētu ES iedzīvotājus un tirgus dalībniekus, kompetentajām iestādēm būtu jāizveido kopīga tīmekļa vietne nekonfidenciālas informācijas publicēšanai par incidentiem un riskiem.

(17) Ja informācija tiek uzskatīta par konfidenciālu saskaņā ar Savienības un valsts noteikumiem par uzņēmējdarbības konfidencialitāti, šādu konfidencialitāti nodrošina, veicot šajā direktīvā noteiktos pasākumus un īstenojot tajā izvirzītos mērķus.

(18) Īpaši balstoties uz valstu krīžu pārvaldības pieredzi un sadarbībā ar *ENISA*, Komisijai un dalībvalstīm būtu jāizstrādā Savienības TID sadarbības plāns, kurā tiktu noteikti sadarbības mehānismi, lai novērstu riskus un incidentus. Minētais plāns būtu pienācīgi jāņem vērā agrīnās brīdināšanas īstenošanā sadarbības tīklā.

(19) Agrīnās brīdināšanas izmantošana tīklā būtu nepieciešama tikai tad, ja attiecīgā incidenta vai riska pakāpe un bīstamība ir vai var kļūt tik būtiska, ka ir nepieciešama informācija vai reaģēšanas saskaņošana Savienības līmenī. Agrīnie brīdinājumi tādējādi būtu jāattiecina tikai uz faktiskiem vai iespējamiem incidentiem vai riskiem, kas strauji attīstītās, pārsniedz valstu reaģēšanas spēju vai skar vairāk par vienu dalībvalsti. Lai varētu veikt pienācīgu novērtējumu, visa informācija, kas ir svarīga riska vai incidenta novērtējumam, būtu jāpaziņo sadarbības tīklam.

(20) Saņemot agrīno brīdinājumu un tā novērtējumu, kompetentajām iestādēm būtu jāvienojas par saskaņotu reaģēšanu saskaņā ar Savienības TID plānu. Kompetentās iestādes un Komisija būtu jāinformē par valsts līmenī pieņemtiem pasākumiem sakarā ar saskaņotu reaģēšanu.

(21) Ņemot vērā TID problēmu globālo raksturu, ir ciešāk jāsadarbojas starptautiskā līmenī, lai uzlabotu drošības standartus un informācijas apmaiņu un veicinātu vienotu vispārēju pieeju TID jautājumiem.

(22) TID nodrošināšanas pienākumi lielā mērā ir valsts pārvaldes iestāžu un tirgus dalībnieku uzdevums. Būtu jāattīsta un jāpopularizē riska pārvaldības kultūra, kas ietver riska novērtējumu un faktiskajiem riskiem atbilstīgu drošības pasākumu īstenošanu, un tas būtu jādara, izmantojot atbilstošas regulatīvas prasības un

brīvprātīgu nozares praksi. Vienlīdzīgu konkurences apstākļu radīšana arī ir būtiska sadarbības tīklu efektīvai darbībai, lai nodrošinātu visu dalībvalstu efektīvu sadarbību.

(23) Direktīvā 2002/21/EK ir prasība, ka uzņēmumiem, kuri nodrošina publiskus elektronisko komunikāciju tīklus vai sniedz publiski pieejamus elektronisko komunikāciju pakalpojumus, jāveic atbilstoši pasākumi, lai garantētu savu integritāti un drošību, un ir paredzētas drošības pārkāpumu un integritātes zuduma paziņošanas prasības. Eiropas Parlamenta un Padomes 2002. gada 12. jūlija Direktīvā 2002/58/EK par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (direktīva par privāto dzīvi un elektronisko komunikāciju)[3] ir prasība publiski pieejamu elektronisko sakaru pakalpojumu sniedzējiem veikt atbilstīgus tehniskus un organizatoriski pasākumus, lai garantētu savu pakalpojumu drošību.

(24) Šie pienākumi būtu jāpaplašina, attiecinot tos ne tikai uz elektronisko komunikāciju nozari, bet arī uz galvenajiem informācijas sabiedrības pakalpojumu sniedzējiem, kā noteikts Eiropas Parlamenta un Padomes 1998. gada 22. jūnija Direktīvā 98/34/EK, ar ko nosaka informācijas sniegšanas kārtību tehnisko standartu un noteikumu jomā[4], jo minētie pakalpojumu sniedzēji nodrošina pamatu pakārtotiem informācijas sabiedrības pakalpojumiem vai tiešsaistes darbībai, piemēram, e-tirdzniecības platformām, interneta maksājumu vārtejām, sociālajiem tīkliem, meklētājprogrammām, mākoņdatošanas pakalpojumiem, lietotņu veikaliem. Šo pakalpojumu, kas padara iespējamu informācijas sabiedrību, traucējumi kavē citu informācijas sabiedrības pakalpojumu sniegšanu, kuru būtiski komponenti ir iepriekš minētie pakalpojumi. Programmatūras izstrādātāji un iekārtu ražotāji nav informācijas sabiedrības pakalpojumu sniedzēji un tādējādi tiek izslēgti. Minētie pienākumi būtu jāattiecina arī uz valsts pārvaldes iestādēm un kritiskās infrastruktūras apsaimniekotājiem, kas ļoti daudz izmanto informācijas un komunikāciju tehnoloģijas un kas ir būtiski svarīgu ekonomisko un sociālo funkciju – piemēram, elektrības un gāzes, transporta, kredītiestāžu, biržas pakalpojumu un veselības aprūpes – nodrošināšanā. Šo tīklu un informācijas sistēmu traucējumi varētu ietekmēt iekšējo tirgu.

(25) Tehniski un organizatoriski pasākumi, kas noteikti valsts pārvaldes iestādēm un tirgus dalībniekiem, nedrīkstētu saturēt prasību, ka konkrēta komercinformācija un komunikāciju tehnoloģijas produkts jākonstruē, jāizstrādā vai jāražo kādā konkrētā veidā.

(26) Valsts pārvaldes iestādēm un tirgus dalībniekiem būtu jānodrošina to kontrolēto tīklu un sistēmu drošība. Tie galvenokārt būtu privāti tīkli un sistēmas, kas tiek pārvaldīti vai nu ar iekšējā IT personāla palīdzību vai kuru drošība tiek nodrošināta, izmantojot ārpakalpojumus. Drošības un paziņošanas pienākumiem būtu jāattiecas uz attiecīgiem tirgus dalībniekiem un valsts pārvaldes iestādēm neatkarīgi no tā, vai tie veic savu tīklu un informācijas sistēmu uzturēšanu iekšēji vai izmanto ārpakalpojumus.

(27) Lai izvairītos no pārmērīga finansiāla un administratīva sloga radīšanas maziem uzņēmumiem un lietotājiem, prasībām būtu jābūt samērīgām ar risku, ko rada attiecīgā tīklu vai informācijas sistēma, ņemot vērā jaunākos sasniegumus šajā jomā. Šīs prasības nebūtu jāattiecina uz mikrouzņēmumiem.

(28) Kompetentajām iestādēm būtu jāpievērš pienācīga uzmanība neformālu un uzticamu informācijas apmaiņas kanālu saglabāšanai starp tirgus dalībniekiem un starp publisko un privāto sektoru. Kad incidenti, par kuriem ziņots kompetentajām iestādēm, tiek

[3] OV L 201, 31.7.2002., 37. lpp.
[4] OV L 204, 21.7.1998., 37. lpp.

publiskoti, būtu jāatrod atbilstošs līdzsvars starp sabiedrības interesēm būt informētai par draudiem un iespējamiem reputācijas un komerciāliem zaudējumiem valsts pārvaldes iestādēm un tirgus dalībniekiem, kuri ziņo par incidentiem. Īstenojot ziņošanas pienākumus, kompetentajām iestādēm būtu jāpievērš īpaša uzmanība nepieciešamībai saglabāt stingru konfidencialitāti attiecībā uz informāciju par produktu vājajām vietām, pirms tiek publiskota informācija par atbilstošiem drošības uzlabojumiem.

(29) Kompetento iestāžu rīcībā vajadzētu būt nepieciešamajiem līdzekļiem to pienākumu veikšanai, tostarp pilnvarām saņemt pietiekamu informāciju no tirgus dalībniekiem un valsts pārvaldes iestādēm, lai novērtētu tīklu un informācijas sistēmu drošības līmeni, kā arī uzticamiem un visaptverošiem datiem par faktiskiem incidentiem, kas ir ietekmējuši tīklu un informācijas sistēmu darbību.

(30) Daudzos gadījumos incidenta pamatā ir noziedzīgas darbības. Par incidenta krimināło raksturu var rasties aizdomas, pat ja sākumā tā pierādījumi nav pietiekami skaidri. Šajā situācijā atbilstošai sadarbībai starp kompetentajām iestādēm un tiesībaizsardzības iestādēm būtu jāveido daļa no efektīvas un visaptverošas reaģēšanas uz drošības incidentu draudiem. Konkrēti, drošas un noturīgākas drošības vides veicināšanai nepieciešama sistemātiska ziņošana tiesībaizsardzības iestādēm par tādiem incidentiem, par kuru nopietno krimināło raksturu ir radušās aizdomas. Incidentu nopietnais krimināłais raksturs būtu jāizvērtē, ņemot vērā ES tiesību aktus par kibernoziegumiem.

(31) Incidentu dēļ daudzos gadījumos ir apdraudēti personas dati. Šajā sakarā kompetentajām iestādēm un datu aizsardzības iestādēm būtu jāsadarbojas un jāapmainās ar informāciju visos attiecīgos jautājumos, lai novērstu personas datu aizsardzības pārkāpumus, kas rodas incidentu dēļ. Dalībvalstis ievieš pienākumu ziņot par drošības incidentiem veidā, kas samazina administratīvo slogu, ja drošības incidents ir arī personas datu aizsardzības pārkāpums saskaņā ar Eiropas Parlamenta un Padomes Regulu par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti[5]. Sazinoties ar kompetentajām iestādēm un datu aizsardzības iestādēm, *ENISA* varētu palīdzēt, izstrādājot informācijas apmaiņas mehānismus un standartformas, izvairoties no nepieciešamības ieviest divas paziņojuma standartformas. Vienota paziņojuma standartforma atvieglotu ziņošanu par incidentiem, kuri rada draudus personas datu aizsardzībai, un tādējādi mazinātu administratīvo slogu uzņēmumiem un valsts pārvaldes iestādēm.

(32) Drošības prasību standartizācija ir tirgus virzīts process. Lai nodrošinātu drošības standartu vienveidīgu piemērošanu, dalībvalstīm būtu jāveicina atbilstība konkrētiem standartiem, lai nodrošinātu augstu drošības līmeni Savienības mērogā. Šim nolūkam varētu būt nepieciešams izstrādāt saskaņotus standartus, kas būtu jādara saskaņā ar Eiropas Parlamenta un Padomes 2012. gada 25. oktobra Regulu (ES) Nr. 1025/2012 par Eiropas standartizāciju, ar ko groza Padomes Direktīvas 89/686/EEK un 93/15/EEK un Eiropas Parlamenta un Padomes Direktīvas 94/9/EK, 94/25/EK, 95/16/EK, 97/23/EK, 98/34/EK, 2004/22/EK, 2007/23/EK, 2009/23/EK un 2009/105/EK, un ar ko atceļ Padomes Lēmumu 87/95/EEK un Eiropas Parlamenta un Padomes Lēmumu Nr. 1673/2006/EK[6].

(33) Komisijai būtu periodiski jāpārskata šī direktīva, jo īpaši lai noteiktu izmaiņu veikšanas nepieciešamību, ņemot vērā mainīgos tehnoloģiskos vai tirgus apstākļus.

---

5 SEC(2012) 72 final.

6 OV L 316, 14.11.2012., 12. lpp.

(34) Lai nodrošinātu sadarbības tīkla pienācīgu darbību, būtu jādeleģē Komisijai pilnvaras pieņemt tiesību aktus saskaņā ar Līguma par Eiropas Savienības darbību 290. pantu attiecībā uz tādu kritēriju noteikšanu, kas jāievēro dalībvalstīm, lai tām varētu atļaut piedalīties drošā informācijas apmaiņas sistēmā, attiecībā uz tādu notikumu papildu precizēšanu, kuru gadījumā nepieciešama agrīnā brīdināšana, un attiecībā uz tādu apstākļu definēšanu, kādos tirgus dalībniekiem un valsts pārvaldes iestādēm ir pienākums ziņot par incidentiem.

(35) Ir īpaši svarīgi, lai Komisija, veicot sagatavošanas darbus, atbilstīgi apspriestos, tostarp ekspertu līmenī. Komisijai, sagatavojot un izstrādājot deleģētos aktus, būtu jānodrošina vienlaicīga, savlaicīga un atbilstīga attiecīgo dokumentu nosūtīšana Eiropas Parlamentam un Padomei.

(36) Lai nodrošinātu vienotus nosacījumus šīs direktīvas īstenošanai, būtu jāpiešķir Komisijai īstenošanas pilnvaras attiecībā uz sadarbību starp kompetentajām iestādēm un Komisiju sadarbības tīklā, piekļuvi drošai informācijas apmaiņas infrastruktūrai, Savienības TID sadarbības plānu, formātiem un procedūrām, kas piemērojamas sabiedrības informēšanai par incidentiem, kā arī attiecībā uz standartiem un/vai tehniskajām specifikācijām, kas attiecas uz TID. Šīs pilnvaras būtu jāīsteno saskaņā ar Eiropas Parlamenta un Padomes 2011. gada 16. februāra Regulu (ES) Nr. 182/2011, ar ko nosaka normas un vispārīgus principus par dalībvalstu kontroles mehānismiem, kuri attiecas uz Komisijas īstenošanas pilnvaru izmantošanu[7].

(37) Piemērojot šo direktīvu, Komisijai būtu vajadzības gadījumā jāsazinās ar attiecīgām nozaru komitejām un attiecīgām struktūrām, kas izveidotas ES līmenī jo īpaši enerģētikas, transporta un veselības aprūpes jomā.

(38) Informācija, ko kompetentā iestāde uzskata par konfidenciālu saskaņā ar Savienības un valsts noteikumiem par uzņēmējdarbības konfidencialitāti, būtu jāsniedz Komisijai un citām kompetentajām iestādēm tikai tad, ja šāda informācijas apmaiņa ir obligāti nepieciešama šīs direktīvas piemērošanai. Sniegtā informācija būtu jāierobežo atbilstīgi un samērīgi šādas informācijas apmaiņas nolūkam.

(39) Lai nodrošinātu informācijas apmaiņu par riskiem un incidentiem sadarbības tīklā un atbilstību prasībām paziņot par incidentiem valsts kompetentajām iestādēm, var būt nepieciešama personas datu apstrāde. Šāda personas datu apstrāde ir nepieciešama, lai sasniegtu šajā direktīvā izvirzītos sabiedrībai svarīgos mērķus, un tādējādi ir likumīga saskaņā ar Direktīvas 95/46/EK 7. pantu. Attiecībā uz šiem likumīgajiem mērķiem tas nerada nesamērīgu un nepieļaujamu iejaukšanos, kas apdraud Pamattiesību hartas 8. pantā garantēto personas datu aizsardzības tiesību būtību. Piemērojot šo direktīvu, pēc vajadzības būtu jāpiemēro Eiropas Parlamenta un Padomes 2001. gada 30. maija Regula (EK) Nr. 1049/2001 par publisku piekļuvi Eiropas Parlamenta, Padomes un Komisijas dokumentiem[8]. Ja datus apstrādā Savienības iestādes un struktūras, šādai apstrādei šīs direktīvas ieviešanas nolūkā vajadzētu būt saskaņā ar Eiropas Parlamenta un Padomes 2000. gada 18. decembra Regulu (EK) Nr. 45/2001 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Kopienas iestādēs un struktūrās un par šādu datu brīvu apriti.

(40) Tā kā šīs direktīvas mērķus, proti, nodrošināt augsta līmeņa TID Savienībā, nevar pietiekami labi sasniegt atsevišķās dalībvalstīs un to rīcības ietekmes dēļ var labāk sasniegt Savienības līmenī, Savienība var pieņemt pasākumus saskaņā ar Līguma par

[7] OV L 55, 28.2.2011., 13. lpp.
[8] OV L 145, 31.5.2001., 43. lpp.

Eiropas Savienību 5. pantā noteikto subsidiaritātes principu. Saskaņā ar minētajā pantā noteikto proporcionalitātes principu šajā direktīva paredzēti vienīgi tie pasākumi, kas ir vajadzīgi minēto mērķu sasniegšanai.

(41) Šajā direktīvā ir respektētas pamattiesības un ievēroti principi, kas atzīti Eiropas Savienības Pamattiesību hartā, galvenokārt tiesības uz privātās dzīves un saziņas neaizskaramību, tiesības uz personas datu aizsardzību, darījumdarbības brīvība, tiesības uz īpašumu, tiesības uz efektīvu tiesību aizsardzību un tiesības tikt uzklausītam. Šī direktīva jāīsteno, ievērojot minētās tiesības un principus.

IR PIEŅĒMUŠI ŠO DIREKTĪVU.

I NODAĻA

VISPĀRĪGI NOTEIKUMI

1. pants

Priekšmets un darbības joma

1. Šajā direktīvā ir paredzēti pasākumi, lai nodrošinātu vienādi augsta līmeņa tīklu un informācijas drošību (turpmāk „TID") Savienībā.

2. Minētajam nolūkam ar šo direktīvu:

(a) nosaka pienākumus visām dalībvalstīm attiecībā uz risku un incidentu, kas ietekmē tīklu un informācijas sistēmas, novēršanu, risināšanu un reaģēšanu uz tiem;

(b) izveido sadarbības mehānismu starp dalībvalstīm, lai nodrošinātu vienotu šīs direktīvas piemērošanu Savienībā un vajadzības gadījumā saskaņotu un efektīvu risku un incidentu, kas ietekmē tīklu un informācijas sistēmas, risināšanu un reaģēšanu uz tiem;

(c) nosaka drošības prasības tirgus dalībniekiem un valsts pārvaldes iestādēm.

3. Drošības prasības, kas paredzētas 14. pantā, neattiecas nedz uz uzņēmumiem, kuri nodrošina publisko komunikāciju tīklus vai sniedz publiski pieejamus elektronisko komunikāciju pakalpojumus Direktīvas 2002/21/EK nozīmē un kuriem jāievēro īpašās drošības un integritātes prasības, kas noteiktas minētās direktīvas 13.a un 13.b pantā, nedz uz uzticamības pakalpojumu sniedzējiem.

4. Šī direktīva neskar ES tiesību aktus par kibernoziegumiem un Padomes 2008. gada 8. decembra Direktīvu 2008/114/EK par to, lai apzinātu un noteiktu Eiropas Kritiskās infrastruktūras un novērtētu vajadzību uzlabot to aizsardzību[9].

5. Šī direktīva neskar arī Eiropas Parlamenta un Padomes 1995. gada 24. oktobra Direktīvu 95/46/EK par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti[10], Eiropas Parlamenta un Padomes 2002. gada 12. jūlija Direktīvu 2002/58/EK par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē un Eiropas Parlamenta un Padomes Regulu par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti[11].

6. Informācijas apmaiņai sadarbības tīklā saskaņā ar III nodaļu un paziņošanai par TID incidentiem saskaņā ar 14. pantu var būt nepieciešama personas datu apstrāde.

---

9 OV L 345, 23.12.2008., 75. lpp.

10 OV L 281, 23.11.1995., 31. lpp.

11 SEC(2012) 72 final.

Dalībvalsts atļauj šādu apstrādi, kas ir nepieciešama šajā direktīvā izvirzīto sabiedrībai svarīgo mērķu sasniegšanai, saskaņā ar Direktīvas 95/46/EK 7. pantu un Direktīvu 2002/58/EK, kā noteikts valsts tiesību aktos.

2. pants

Obligātā saskaņošana

Dalībvalstis netiek kavētas pieņemt vai saglabāt spēkā noteikumus, kas nodrošina augstāku drošības līmeni, neskarot dalībvalstu saistības saskaņā ar Savienības tiesību aktiem.

3. pants

Definīcijas

Šajā direktīvā piemēro šādas definīcijas:

(1) „tīklu un informācijas sistēma" ir:

(a) elektronisko komunikāciju tīkls Direktīvas 2002/21/EK nozīmē un

(b) jebkura ierīce vai savstarpēji savienotu vai saistītu ierīču kopums, no kurām viena vai vairākas ierīces saskaņā ar programmu veic automātisku datorizētu datu apstrādi, kā arī

(c) datorizēti dati, ko a) un b) apakšpunktā minētie elementi glabā, apstrādā, iegūst vai sūta to darbībai, izmantošanai, aizsardzībai un uzturēšanai;

(2) „drošība" ir tīklu un informācijas sistēmu spēja noteiktā uzticamības līmenī pretoties nejaušiem gadījumiem vai nelikumīgām un ļaunprātīgām darbībām, kas apdraud glabājamo vai pārraidāmo datu un šo tīklu un informācijas sistēmu piedāvāto vai ar to starpniecību pieejamo saistīto pakalpojumu pieejamību, autentiskumu, integritāti un konfidencialitāti;

(3) „risks" ir jebkāds apstāklis vai notikums, kas var negatīvi ietekmēt drošību;

(4) „incidents" ir jebkāds apstāklis vai notikums, kas faktiski negatīvi ietekmē drošību;

(5) „informācijas sabiedrības pakalpojums" ir pakalpojums Direktīvas 98/34/EK 1. panta 2. punkta nozīmē;

(6) „TID sadarbības plāns" ir plāns, kurā noteikta organizatorisko funkciju, pienākumu un procedūru sistēma, lai saglabātu vai atjaunotu tīklu un informācijas sistēmu darbību, ja pastāv risks vai notiek incidents, kurš tos ietekmē;

(7) „incidenta risināšana" ir visas procedūras, kas ļauj veikt analīzi par incidentu, to ierobežot un reaģēt uz to;

(8) „tirgus dalībnieks" ir:

(a) tādu informācijas sabiedrības pakalpojumu sniedzējs, kuri ļauj sniegt citus informācijas sabiedrības pakalpojumus un kuru nepilnīgs saraksts ir iekļauts II pielikumā;

(b) tādas kritiskās infrastruktūras apsaimniekotājs, kura ir būtiska svarīgu ekonomisko un sabiedrisko darbību nodrošināšanai tādās jomās kā enerģētika, transports, banku nozare, birža un veselības aprūpe, kuru nepilnīgs saraksts ir iekļauts II pielikumā;

(9) „standarts" ir standarts, kas minēts Regulā (ES) Nr. 1025/2012;

(10) „specifikācija” ir specifikācija, kas minēta Regulā (ES) Nr. 1025/2012;

(11) „uzticamības pakalpojumu sniedzējs” ir fiziska vai juridiska persona, kura sniedz jebkādu elektronisku pakalpojumu, kas ietver elektronisko parakstu, elektronisko zīmogu, elektronisko laika zīmogu, elektronisko dokumentu, elektronisko piegādes pakalpojumu, tīmekļa vietņu autentifikācijas un elektronisko sertifikātu (tostarp elektroniskā paraksta un elektroniskā zīmoga sertifikātu) radīšanu, pārbaudi, validāciju, apstrādi un saglabāšanu.

II NODAĻA

VALSTU TĪKLU UN INFORMĀCIJAS DROŠĪBAS SISTĒMAS

4. pants

Princips

Dalībvalstis savā teritorijā saskaņā ar šo direktīvu nodrošina augstu tīklu un informācijas sistēmu drošības līmeni.

5. pants

Valsts TID stratēģija un valsts TID sadarbības plāns

1. Katra dalībvalsts pieņem valsts TID stratēģiju, kurā definēti stratēģiskie mērķi un konkrēti politikas un reglamentējoši pasākumi, lai panāktu un saglabātu augsta līmeņa tīklu un informācijas drošību. Valsts TID stratēģijā ietver jo īpaši šādus jautājumus:

(a) definēti stratēģijas mērķi un prioritātes, pamatojoties uz jaunāko risku un incidentu analīzi;

(b) pārvaldības sistēma, ar kuru varētu sasniegt stratēģijas mērķus un prioritātes, tostarp skaidri noteiktas vadības iestāžu un citu attiecīgo dalībnieku funkcijas un pienākumi;

(c) noteikti vispārējie pasākumi attiecībā uz sagatavotību, reaģēšanu un atkopi, tostarp sadarbības mehānismi starp publisko un privāto sektoru;

(d) norāde par izglītības, izpratnes veidošanas un apmācības programmām;

(e) pētniecības un izstrādes plāni un apraksts, kā šie plāni atspoguļo noteiktās prioritātes.

2. Valsts TID stratēģijā ietilpst valsts TID sadarbības plāns, kurā ievērotas vismaz šādas prasības:

(a) riska novērtēšanas plāns, kas ļautu apzināt riskus un novērtēt iespējamo incidentu ietekmi;

(b) noteiktas dažādu plāna īstenošanā iesaistīto dalībnieku funkcijas un pienākumi;

(c) tādu sadarbības un komunikācijas procesu definīcija, kuri nodrošina novēršanu, atklāšanu, reaģēšanu, labošanu un atkopi, un kuri ir modulēti atbilstīgi brdinājumu līmenim;

(d) ceļvedis par TID mācībām un apmācībām plāna nostiprināšanai, apstiprināšanai un testēšanai. Gūtās atziņas tiks dokumentētas un iekļautas plāna papildinājumos.

3. Valsts TID stratēģiju un valsts TID sadarbības plānu nosūta Komisijai viena mēneša laikā pēc to pieņemšanas.

6. pants

Par tīklu un informācijas sistēmu drošību atbildīgā valsts kompetentā iestāde

1. Katra dalībvalsts ieceļ valsts kompetento iestādi, kura atbild par tīklu un informācijas sistēmu drošību (turpmāk „kompetentā iestāde").

2. Kompetentās iestādes uzrauga šīs direktīvas piemērošanu valsts līmenī un palīdz nodrošināt tās konsekventu piemērošanu visā Savienībā.

3. Dalībvalstis nodrošina, ka kompetentajām iestādēm ir pietiekami tehniskie, finanšu un cilvēkresursi, lai nodrošinātu, ka tās efektīvi un produktīvi var veikt tām uzticētos uzdevumus un tādējādi sasniegt šīs direktīvas mērķus. Dalībvalstis nodrošina efektīvu, produktīvu un drošu kompetento iestāžu sadarbību, izmantojot tīklu, kas minēts 8. pantā.

4. Dalībvalstis nodrošina, ka kompetentās iestādes saņem paziņojumus par incidentiem no valsts pārvaldes iestādēm un tirgus dalībniekiem, kā norādīts 14. panta 2. punktā, un tām tiek piešķirtas īstenošanas un izpildes pilnvaras, kā norādīts 15. pantā.

5. Kompetentās iestādes vajadzības gadījumā apspriežas un sadarbojas ar attiecīgajām tiesībaizsardzības valsts iestādēm un datu aizsardzības iestādēm.

6. Katra dalībvalsts nekavējoties paziņo Komisijai ieceltās kompetentās iestādes nosaukumu, tās uzdevumus un visas turpmākās izmaiņas šajā informācijā. Katra dalībvalsts publisko savas ieceltās kompetentās iestādes nosaukumu.

7. pants

Datorapdraudējumu reaģēšanas vienība

1. Katra dalībvalsts izveido datorapdraudējumu reaģēšanas vienību (turpmāk „*CERT*"), kas ir atbildīga par incidentu un risku risināšanu saskaņā ar labi definētu procesu, kurš atbilst I pielikuma 1. punktā noteiktajām prasībām. *CERT* var izveidot kompetentajā iestādē.

2. Dalībvalstis nodrošina, ka *CERT* ir atbilstoši tehniskie, finanšu un cilvēkresursi, lai tās varētu efektīvi veikt savus pienākumus, kas izklāstīti I pielikuma 2. punktā.

3. Dalībvalstis nodrošina, ka *CERT* izmanto drošu un noturīgu komunikācijas un informācijas infrastruktūru valsts līmenī, kas ir saderīga un sadarbspējīga ar drošu informācijas apmaiņas sistēmu, kas minēta 9. pantā.

4. Dalībvalstis informē Komisiju par *CERT* resursiem un pilnvarām, kā arī par incidentu risināšanas procesu.

5. *CERT* darbojas kompetentās iestādes uzraudzībā, kura regulāri pārskata tās resursu atbilstību, pilnvaras un efektivitāti incidentu risināšanas procesā.

III NODAĻA

KOMPETENTO IESTĀŽU SADARBĪBA

8. pants

Sadarbības tīkls

1. Kompetentās iestādes un Komisija veido tīklu (turpmāk „sadarbības tīkls"), kas sadarbojas tādu risku un incidentu novēršanā, kuri ietekmē tīklu un informācijas sistēmas.

2. Sadarbības tīkls nodrošina pastāvīgu saziņu starp Komisiju un kompetentajām iestādēm. Eiropas Tīklu un informācijas drošības aģentūra (*ENISA*) pēc pieprasījuma palīdz sadarbības tīklam, sniedzot savas zināšanas un konsultācijas.

3. Sadarbības tīklā kompetentās iestādes:

(a) izplata agrīnus brīdinājumus par riskiem un incidentiem saskaņā ar 10. pantu;

(b) nodrošina saskaņotu reaģēšanu saskaņā ar 11. pantu;

(c) regulāri kopīgā tīmekļa vietnē publicē nekonfidenciālu informāciju par aktuālajiem agrīnajiem brīdinājumiem un saskaņotu reaģēšanu;

(d) ja to pieprasa kāda dalībvalsts vai Komisija, kopīgi apspriež un novērtē vienu vai vairākas valsts TID stratēģijas un valsts TID sadarbības plānus, kas minēti 5. pantā, šīs direktīvas darbības jomā.

(e) ja to pieprasa kāda dalībvalsts vai Komisija, kopīgi apspriež un novērtē *CERT* efektivitāti, jo īpaši tad, ja tiek veiktas TID mācības Savienības mērogā;

(f) sadarbojas un apmainās ar informāciju par visiem attiecīgiem jautājumiem ar Eiropas kibernoziedzības centru Eiropolā un ar citām attiecīgajām Eiropas iestādēm, jo īpaši tādās jomās kā datu aizsardzība, enerģētika, transports, banku nozare, biržas un veselības aprūpe;

(g) savā starpā un ar Komisiju apmainās ar informāciju un paraugpraksi un palīdz viena otrai spēju veidošanā saistībā ar TID;

(h) organizē regulāras salīdzinošās izvērtēšanas par spējām un sagatavotību;

(i) organizē TID mācības Savienības līmenī un, ja nepieciešams, piedalās starptautiskās TID mācībās.

4. Pieņemot īstenošanas aktus, Komisija nosaka vajadzīgo kārtību, lai atvieglotu sadarbību starp kompetentajām iestādēm un Komisiju, kas minēta 2. un 3. punktā. Minētos īstenošanas aktus pieņem saskaņā ar 19. panta 2. punktā minēto konsultēšanās procedūru.

9. pants

Droša informācijas apmaiņas sistēma

1. Apmaiņa ar sensitīvu un konfidenciālu informāciju sadarbības tīklā notiek, izmantojot drošu infrastruktūru.

2. Komisija ir pilnvarota pieņemt deleģētos aktus saskaņā ar 18. pantu attiecībā uz tādu kritēriju noteikšanu, kuri jāizpilda, lai dalībvalstij tiktu atļauts piedalīties drošā informācijas apmaiņas sistēmā par šādiem jautājumiem:

(a) drošas un noturīgas komunikācijas un informācijas infrastruktūras, kura ir saderīga un sadarbspējīga ar sadarbības tīkla drošo infrastruktūru saskaņā ar 7. panta 3. punktu, pieejamība valsts līmenī un

(b) atbilstīgu tehnisko, finanšu un cilvēkresursu un procesu pastāvēšana, lai tās kompetentā iestāde un *CERT* varētu efektīvi, produktīvi un droši piedalīties drošā informācijas apmaiņas sistēmā saskaņā ar 6. panta 3. punktu, 7. panta 2. punktu un 7. panta 3. punktu.

3. Komisija, izmantojot īstenošanas aktus, pieņem lēmumus par dalībvalstu pieeju šai drošajai infrastruktūrai saskaņā ar kritērijiem, kas minēti 2. un 3. punktā. Šos

īstenošanas aktus pieņem saskaņā ar 19. panta 3. punktā minēto pārbaudes procedūru.

10. pants

Agrīnā brīdināšana

1. Kompetentās iestādes vai Komisija sadarbības tīklā nodrošina agrīno brīdināšanu par tiem riskiem un incidentiem, kas atbilst vismaz vienam no šādiem nosacījumiem:

   (a) tie strauji palielinās vai var strauji palielināties pēc apjoma;

   (b) tie pārsniedz vai var pārsniegt valsts reaģēšanas spēju;

   (c) tie ietekmē vai var ietekmēt vairāk nekā vienu dalībvalsti.

2. Agrīnajos brīdinājumos kompetentās iestādes un Komisija paziņo visu to rīcībā esošo attiecīgo informāciju, kas var noderēt riska vai incidenta novērtēšanā.

3. Pēc dalībvalsts pieprasījuma vai pēc savas iniciatīvas Komisija var pieprasīt dalībvalstij sniegt visu attiecīgo informāciju par konkrētu risku vai incidentu.

4. Ja ir aizdomas, ka riskam vai incidentam, uz kuru attiecas agrīnā brīdināšana, ir krimināls raksturs, kompetentās iestādes vai Komisija informē Eiropas kibernoziedzības centru Eiropolā.

5. Komisija ir pilnvarota pieņemt deleģētos aktus saskaņā ar 18. pantu attiecībā uz turpmākajiem precizējumiem par riskiem un incidentiem, kuru gadījumā nepieciešama agrīnā brīdināšana, kas minēta 1. punktā.

11. pants

Saskaņota reaģēšana

1. Pēc agrīnās brīdināšanas, kas minēta 10. pantā, kompetentās iestādes pēc attiecīgās informācijas izvērtēšanas vienojas par saskaņotu reaģēšanu atbilstīgi Savienības TID sadarbības plānam, kas minēts 12. pantā.

2. Dažādos pasākumus, kas pieņemti valsts līmenī sakarā ar saskaņotu reaģēšanu, paziņo sadarbības tīklam.

12. pants

Savienības TID sadarbības plāns

1. Komisija ir pilnvarota, izmantojot īstenošanas aktus, pieņemt Savienības TID sadarbības plānu. Minētos īstenošanas aktus pieņem saskaņā ar 19. panta 3. punktā minēto pārbaudes procedūru.

2. Savienības TID plānā tiek noteikts:

   (a) 10. panta īstenošanas nolūkā:

      – formāts un procedūras attiecībā uz kompetento iestāžu īstenotas saderīgas un salīdzināmas informāciju iegūšanu un apmaiņu par riskiem un incidentiem,

      – procedūras un kritēriji sadarbības tīkla īstenotam risku un incidentu novērtējumam.

(b) kārtība, kas jāievēro, īstenojot saskaņotu reaģēšanu atbilstīgi 11. pantam, tostarp funkciju, pienākumu un sadarbības procedūru noteikšana;

(c) ceļvedis par TID mācībām un apmācībām plāna nostiprināšanai, apstiprināšanai un testēšanai.

(d) zināšanu nodošanas programma starp dalībvalstīm saistībā ar spēju veidošanu un savstarpēju mācīšanos;

(e) programma izpratnes veidošanai un apmācībām starp dalībvalstīm.

3. Savienības TID sadarbības plānu pieņem ne vēlāk kā vienu gadu pēc šīs direktīvas stāšanās spēkā un regulāri pārskata.

13. pants

Starptautiskā sadarbība

Neskarot sadarbības tīkla iespēju veidot neformālu starptautisko sadarbību, Savienība var slēgt starptautiskus nolīgumus ar trešām valstīm vai starptautiskām organizācijām, ļaujot tām piedalīties vai organizējot to dalību atsevišķos sadarbības tīkla pasākumos. Šādā nolīgumā ņem vērā vajadzību nodrošināt pienācīgu tādu personas datu aizsardzību, kuri cirkulē sadarbības tīklā.

IV NODAĻA

VALSTS PĀRVALDES IESTĀŽU UN TIRGUS DALĪBNIEKU TĪKLU UN INFORMĀCIJAS SISTĒMU DROŠĪBA

14. pants

Drošības prasības un incidentu paziņošana

1. Dalībvalstis nodrošina to, ka valsts pārvaldes iestādes un tirgus dalībnieki veic attiecīgus tehniskus un organizatoriskus pasākumus, lai pārvaldītu to tīklu un informācijas sistēmu drošības riskus, kurus tās kontrolē un izmanto savā darbībā. Ņemot vērā jaunākos tehniskos sasniegumus, ar šiem pasākumiem garantē novērtētajam riskam atbilstīgu drošības pakāpi. Jo īpaši veic pasākumus, lai novērstu un mazinātu tādu incidentu sekas, kas ietekmē to tīklu un informācijas sistēmu saistībā ar to sniegtajiem pamatpakalpojumiem, un tādējādi nodrošinātu tādu pakalpojumu nepārtrauktību, kas ir atkarīgi no šiem tīkliem un informācijas sistēmām.

2. Dalībvalstis nodrošina to, ka valsts pārvaldes iestādes un tirgus dalībnieki paziņo kompetentajai iestādei par incidentiem, kuriem ir būtiska ietekme uz to sniegto pamatpakalpojumu drošību.

3. Prasības, kas noteiktas 1. un 2. punktā, attiecas uz visiem tirgus dalībniekiem, kas sniedz pakalpojumus Eiropas Savienībā.

4. Kompetentā iestāde var informēt sabiedrību vai arī prasīt, lai to izdara valsts pārvaldes iestādes un tirgus dalībnieki, ja tā uzskata, ka incidenta publiskošana ir sabiedrības interesēs. Kompetentā iestāde reizi gadā iesniedz sadarbības tīklam kopsavilkuma ziņojumu par saņemtajiem paziņojumiem un rīcību, kas īstenota saskaņā ar šo punktu.

5. Komisija ir pilnvarota pieņemt deleģētos aktus saskaņā ar 18. pantu attiecībā uz apstākļu noteikšanu, kuros valsts pārvaldes iestādēm un tirgus dalībniekiem ir jāpaziņo par incidentiem.

6. Ievērojot visus deleģētos aktus, kas pieņemti saskaņā ar 5. punktu, kompetentās iestādes var pieņemt pamatnostādnes un vajadzības gadījumā izdot instrukcijas par apstākļiem, kādos valsts pārvaldes iestādēm un tirgus dalībniekiem ir jāinformē par incidentiem.

7. Komisija ir pilnvarota, izmantojot īstenošanas aktus, noteikt formātus un procedūras, ko piemēro šā panta 2. punkta vajadzībām. Šos īstenošanas aktus pieņem saskaņā ar 19. panta 3. punktā minēto pārbaudes procedūru.

8. Šā panta 1. un 2. punkts neattiecas uz mikrouzņēmumiem, kā noteikts Komisijas 2003. gada 6. maija Ieteikumā 2003/361/EK par mikrouzņēmumu, mazo un vidējo uzņēmumu definīciju[12].

15. pants

Īstenošana un izpilde

1. Dalībvalstis nodrošina, ka kompetentajām iestādēm ir visas vajadzīgās pilnvaras, lai izmeklētu gadījumus, kad valsts pārvaldes iestādes vai tirgus dalībnieki neveic savus 14. pantā noteiktos pienākumus, un to ietekmi uz tīklu un informācijas sistēmu drošību.

2. Dalībvalstis nodrošina, ka kompetentās iestādes ir pilnvarotas pieprasīt tirgus dalībniekiem un valsts pārvaldes iestādēm:

   (a) sniegt informāciju, kas vajadzīga tīklu un informācijas sistēmu drošības novērtēšanai, tostarp informēt par dokumentētu drošības politiku;

   (b) īstenot drošības revīziju, ko veic kvalificēta neatkarīga struktūra vai valsts iestāde, un darīt tās rezultātus pieejamus kompetentajai iestādei.

3. Dalībvalstis nodrošina, ka kompetentās iestādes ir pilnvarotas izdot saistošas instrukcijas tirgus dalībniekiem un valsts pārvaldes iestādēm.

4. Kompetentās iestādes paziņo tiesībaizsardzības iestādēm par incidentiem, par kuru krimināls raksturu rodas aizdomas.

5. Kompetentās iestādes strādā ciešā sadarbībā ar personas datu aizsardzības iestādēm, risinot incidentus, kuru rezultātā notiek personas datu aizsardzības pārkāpumi.

6. Dalībvalstis nodrošina, ka visus pienākumus, kas uzticēti valsts pārvaldes iestādēm un tirgus dalībniekiem saskaņā ar šo nodaļu, var pārsūdzēt tiesā.

16. pants

Standartizācija

1. Lai nodrošinātu 14. panta 1. punkta vienādu īstenošanu, dalībvalstis veicina tādu standartu un/vai specifikāciju izmantošanu, kas attiecas uz tīklu un informācijas drošību.

2. Komisija, izmantojot īstenošanas aktus, izveido 1. punktā minēto standartu sarakstu. Šo sarakstu publicē *Eiropas Savienības Oficiālajā Vēstnesī*.

[12] OV L 124, 20.5.2003., 36. lpp.

V NODAĻA
NOBEIGUMA NOTEIKUMI

17. pants

Sankcijas

1. Dalībvalstis paredz noteikumus par sankcijām, kas piemērojamas par to valsts noteikumu pārkāpumiem, kuri pieņemti saskaņā ar šo direktīvu, un veic visus vajadzīgos pasākumus, lai nodrošinātu minēto sankciju īstenošanu. Paredzētajām sankcijām jābūt efektīvām, samērīgām un preventīvām. Dalībvalstis paziņo par šiem noteikumiem Komisijai vēlākais līdz šīs direktīvas transponēšanas dienai un nekavējoties paziņo tai par jebkuriem turpmākiem grozījumiem, kas šos noteikumus ietekmē.

2. Dalībvalstis nodrošina, ka tad, ja drošības incidents ir saistīts ar personas datiem, paredzētās sankcijas atbilst sankcijām, kas noteiktas Eiropas Parlamenta un Padomes Regulā par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti[13].

18. pants

Deleģēšanas īstenošana

1. Pilnvaras pieņemt deleģētos aktus Komisijai piešķir, ievērojot šā panta nosacījumus.

2. Pilnvaras pieņemt deleģētos aktus, kas minētas 9. panta 2. punktā, 10. panta 5. punktā un 14. panta 5. punktā, tiek piešķirtas Komisijai. Komisija sagatavo ziņojumu par pilnvaru deleģēšanu vēlākais deviņus mēnešus pirms piecu gadu laikposma beigām. Pilnvaru deleģējumu automātiski pagarina uz tāda paša ilguma laikposmiem, ja vien Eiropas Parlaments vai Padome neiebilst pret šādu pagarinājumu vēlākais trīs mēnešus pirms katra laikposma beigām.

3. Eiropas Parlaments vai Padome jebkurā brīdī var atsaukt 9. panta 2. punktā, 10. panta 5. punktā un 14. panta 5. punktā minēto pilnvaru deleģējumu. Ar lēmumu par atsaukšanu izbeidz tajā norādīto pilnvaru deleģēšanu. Lēmums stājas spēkā nākamajā dienā pēc tā publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī* vai vēlākā dienā, kas tajā norādīta. Tas neietekmē spēkā esošo deleģēto aktu spēkā esību.

4. Tiklīdz Komisija pieņem deleģēto aktu, tā par to paziņo vienlaikus Eiropas Parlamentam un Padomei.

5. Saskaņā ar 9. panta 2. punktu, 10. panta 5. punktu un 14. panta 5. punktu pieņemtie deleģētie akti stājas spēkā tikai tad, ja divos mēnešos no dienas, kad minētais akts paziņots Eiropas Parlamentam un Padomei, ne Eiropas Parlaments, ne Padome nav izteikuši iebildumus, vai ja pirms minētā laikposma beigām gan Eiropas Parlaments, gan Padome ir informējuši Komisiju par savu lēmumu neizteikt iebildumus. Pēc Eiropas Parlamenta vai Padomes iniciatīvas šo periodu pagarina par diviem mēnešiem.

19. pants

Komitejas procedūra

[13] SEC(2012) 72 final.

1. Komisijai palīdz komiteja (Tīklu un informācijas drošības komiteja). Minētā komiteja ir komiteja Regulas (ES) Nr. 182/2011 izpratnē.

2. Ja ir atsauce uz šo punktu, piemēro Regulas (ES) Nr. 182/2011 4. pantu.

3. Ja ir atsauce uz šo punktu, piemēro Regulas (ES) Nr. 182/2011 5. pantu.

20. pants

Pārskatīšana

Komisija periodiski pārskata šīs direktīvas darbību un iesniedz ziņojumu Eiropas Parlamentam un Padomei. Pirmo ziņojumu iesniedz ne vēlāk kā trīs gadus pēc transponēšanas datuma, kas minēts 21. pantā. Šajā nolūkā Komisija var prasīt, lai dalībvalstis tai sniegtu informāciju bez liekas kavēšanās.

21. pants

Transponēšana

1. Dalībvalstis vēlākais [pusotru gadu pēc dienas, kurā pieņemta direktīva,] pieņem un publicē normatīvos un administratīvos aktus, kas vajadzīgi, lai izpildītu šīs direktīvas prasības. Dalībvalstis tūlīt dara zināmu Komisijai minēto noteikumu tekstu.

   Tās piemēro minētos noteikumus no [pusotru gadu pēc pieņemšanas].

   Kad dalībvalstis pieņem minētos aktus, tajos iekļauj atsauci uz šo direktīvu, vai arī šādu atsauci pievieno to oficiālajai publikācijai. Dalībvalstis nosaka, kā izdarāma šāda atsauce.

2. Dalībvalstis dara Komisijai zināmus savu tiesību aktu galvenos noteikumus, ko tās pieņem jomā, uz kuru attiecas šī direktīva.

22. pants

Stāšanās spēkā

Šī direktīva stājas spēkā [divdesmitajā] dienā pēc tās publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī.*

23. pants

Adresāti

Šī direktīva ir adresēta dalībvalstīm.

Briselē,

Eiropas Parlamenta vārdā —	*Padomes vārdā —*
priekšsēdētājs	*priekšsēdētājs*

I PIELIKUMS

Datorapdraudējumu reaģēšanas vienības (*CERT*) pienākumi un uzdevumi

CERT pienākumus un uzdevumus atbilstīgi un skaidri nosaka un atbalsta valstu politika un/vai regulējums. Tie iekļauj šādus elementus:

(1) *CERT* pienākumi:

(a) *CERT* nodrošina tās komunikāciju pakalpojumu pieejamību, novēršot atsevišķu informācijas ķēdes punktu kļūdainu darbību, un tām ir vairāki saziņas līdzekļi, kas ļauj ar tām sazināties un nodrošina saziņu ar citiem. Turklāt saziņas kanāli ir skaidri norādīti un labi zināmi attiecīgām personām un sadarbības partneriem.

(b) *CERT* īsteno un pārvalda drošības pasākumus, lai nodrošinātu savas saņemtās un apstrādātās informācijas konfidencialitāti, integritāti, pieejamību un autentiskumu.

(c) *CERT* biroji un izmantotās informācijas sistēmas atrodas drošās vietās.

(d) izveido pakalpojumu vadības kvalitātes sistēmu, lai pārraudzītu Eiropas *CERT* darbību un nodrošinātu stabilu uzlabojumu procesu. Tā balstās uz skaidri definētiem rādītājiem, kuros iekļauti drošības līmeņi un galvenie darbības rādītāji.

(e) Darbības nepārtrauktība:

- *CERT* ir jāaprīko ar atbilstīgu sistēmu pieprasījumu pārvaldībai un novirzīšanai, lai atvieglotu nodošanu,
- *CERT* ir pietiekams skaits darbinieku, lai nodrošinātu pieejamību jebkurā brīdī,
- *CERT* izmanto infrastruktūru, kurai ir nodrošināta nepārtrauktība. Šajā nolūkā *CERT* tiek izveidotas dublējošās sistēmas un rezerves darba telpa, lai nodrošinātu pastāvīgu piekļuvi sakaru līdzekļiem.

(2) *CERT* uzdevumi

(a) *CERT* uzdevumos ietilpst vismaz šādi uzdevumi:

- incidentu uzraudzība valsts līmenī,
- agrīnās brīdināšanas, brīdināšanas, paziņojumu un informācijas izplatīšanas nodrošināšana ieinteresētajām personām par riskiem un incidentiem,
- reaģēšana uz incidentiem,
- dinamiskas risku un incidentu analīzes un situācijas apzināšanas nodrošināšana,
- plašas sabiedrības informētības sekmēšana par riskiem, kas saistīti ar tiešsaistes darbībām,
- kampaņu organizēšana par TID;

(b) *CERT* izveido sadarbību ar privāto sektoru.

(c) Lai atvieglotu sadarbību, *CERT* veicina arī kopīgas vai standartizētas prakses ieviešanu un izmantošanu attiecībā uz:

- incidentu un risku risināšanas procedūrām,
- incidentu, risku un informācijas klasifikācijas shēmām,
- rādītāju taksonomiju,

– informācijas apmaiņas formātiem par riskiem, incidentiem un sistēmu nosaukumu noteikumiem.

II PIELIKUMS

Tirgus dalībnieku saraksts

Minēts 3. panta 8. punkta a) apakšpunktā:

1. e-tirdzniecības platformas;

2. interneta maksājumu vārtejas;

3. sociālie tīkli;

4. meklētājprogrammas;

5. mākoņdatošanas pakalpojumi;

6. lietotņu veikali.

Minēts 3. panta 8. punkta b) apakšpunktā:

1. Enerģētika:

- elektroenerģijas un gāzes piegādātāji;
- elektroenerģijas un/vai gāzes sadales sistēmu operatori un mazumtirgotāji galapatērētājiem;
- dabasgāzes pārvades sistēmas operatori, uzglabāšanas operatori un sašķidrinātas dabasgāzes operatori;
- elektroenerģijas pārvades sistēmas operatori;
- naftas pārvadi un naftas uzglabāšana;
- elektroenerģijas un gāzes tirgus dalībnieki;
- naftas un dabasgāzes ražošanas operatori, pārstrādes un attīrīšanas iekārtas.

2. Transports:

- gaisa pārvadātāji (kravas un pasažieru gaisa pārvadājumi);
- jūras pārvadātāji (jūras un piekrastes ūdeņu pasažieru pārvadājumu uzņēmumi un jūras un piekrastes ūdeņu kravas pārvadājumu uzņēmumi);
- dzelzceļš (infrastruktūras pārvaldītāji, integrētie uzņēmumi un dzelzceļa pārvadājumu operatori);
- lidostas;
- ostas;
- satiksmes vadības kontroles operatori;
- papildu loģistikas pakalpojumi (a) noliktavu un uzglabāšanas pakalpojumi, b) kravu iekraušana un izkraušana un c) citas transporta palīgdarbības).

3. Banku nozare: kredītiestādes saskaņā ar Direktīvas 2006/48/EK 4. panta 1. punktu.

4. Finanšu tirgus infrastruktūras: biržas un centrālas mijieskaita darījumu starpniekiestādes.

5. Veselības aprūpes nozare: veselības aprūpes iestādes (tostarp slimnīcas un privātas klīnikas) un citas struktūras, kas iesaistītas veselības aprūpes nodrošināšanā.

TIESĪBU AKTA PRIEKŠLIKUMA FINANŠU PĀRSKATS

1. PRIEKŠLIKUMA/INICIATĪVAS KONTEKSTS

1.1. Priekšlikuma/iniciatīvas nosaukums

1.2. Attiecīgās politikas joma(s) *ABM*/*ABB* struktūrā

1.3. Priekšlikuma/iniciatīvas būtība

1.4. Mērķi

1.5. Priekšlikuma/iniciatīvas pamatojums

1.6. Ilgums un finansiālā ietekme

1.7. Paredzētie pārvaldības veidi

2. PĀRVALDĪBAS PASĀKUMI

2.1. Uzraudzības un ziņošanas noteikumi

2.2. Pārvaldības un kontroles sistēma

2.3. Krāpšanas un pārkāpumu apkarošanas pasākumi

3. PRIEKŠLIKUMA/INICIATĪVAS PAREDZAMĀ FINANSIĀLĀ IETEKME

3.1. Attiecīgās daudzgadu finanšu shēmas izdevumu kategorijas un budžeta izdevumu pozīcijas

3.2. Paredzamā ietekme uz izdevumiem

3.2.1. Paredzamās ietekmes uz izdevumiem kopsavilkums

3.2.2. Paredzamā ietekme uz darbības apropriācijām

3.2.3. Paredzamā ietekme uz administratīvajām apropriācijām

3.2.4. Saderība ar kārtējo daudzgadu finanšu shēmu

3.2.5. Trešo personu dalība finansējumā

3.3. Paredzamā ietekme uz ieņēmumiem

TIESĪBU AKTA PRIEKŠLIKUMA FINANŠU PĀRSKATS

1. PRIEKŠLIKUMA/INICIATĪVAS KONTEKSTS

1.1. Priekšlikuma/iniciatīvas nosaukums

Priekšlikums Eiropas Parlamenta un Padomes direktīvai par pasākumiem, kas nodrošinātu augsta līmeņa tīklu un informācijas drošību visā Savienībā

1.2. Attiecīgās politikas jomas *ABM*/*ABB* struktūrā[37]

- 09 – komunikāciju tīkli, saturs un tehnoloģijas

1.3. Priekšlikuma/iniciatīvas būtība

☒ Priekšlikums/iniciatīva attiecas uz **jaunu darbību**

☐ Priekšlikums/iniciatīva attiecas uz **jaunu darbību, pamatojoties uz izmēģinājuma projektu/sagatavošanas darbību**[38]

☐ Priekšlikums/iniciatīva attiecas uz **esošas darbības pagarināšanu**

☐ Priekšlikums/iniciatīva attiecas uz **darbību, kas pārveidota jaunā darbībā**

1.4. Mērķi

1.4.1. Komisijas daudzgadu stratēģiskie mērķi, kurus plānots sasniegt ar priekšlikumu/iniciatīvu

Šī direktīvas priekšlikuma mērķis ir nodrošināt vienādi augsta līmeņa tīklu un informācijas drošību (TID) visā ES.

1.4.2. Konkrētie mērķi un attiecīgās ABM/ABB darbības

Priekšlikumā paredzēti pasākumi, kas nodrošinātu vienādi augsta līmeņa tīklu un informācijas drošību visā Savienībā.

Konkrētie mērķi ir:

1. Dalībvalstīs ieviest minimālo TID līmeni un tādējādi uzlabot vispārējo sagatavotības un reaģēšanas līmeni.

2. ES līmenī uzlabot sadarbību TID jautājumos, lai efektīvi apkarotu pārrobežu incidentus un apdraudējumus. Tiks izveidota droša informācijas apmaiņas infrastruktūra, lai kompetentās iestādes varētu apmainīties ar sensitīvu un konfidenciālu informāciju.

3. Izveidot riska pārvaldības kultūru un uzlabot informācijas apmaiņu starp privāto un publisko sektoru.

Attiecīgās *ABM*/*ABB* darbības

Direktīva attiecas uz struktūrvienībām (uzņēmumiem un organizācijām, tostarp dažiem MVU) dažādās nozarēs (enerģētika, transports, kredītiestādes un biržas, veselības aprūpe un galveno interneta pakalpojumu nodrošinātāji), kā arī valsts pārvaldes iestādēm. Tajā reglamentēts jautājums par saikni ar tiesībaizsardzību un datu aizsardzību, un TID aspektiem ārējās attiecībās.

- 09 – komunikāciju tīkli, saturs un tehnoloģijas

- 02 – uzņēmējdarbība

- 32 – enerģētika

- 06 – mobilitāte un transports

---

37 *ABM* — budžeta līdzekļu vadība pa darbības jomām. *ABB* — budžeta līdzekļu sadale pa darbības jomām.

38 Kā paredzēts Finanšu regulas 49. panta 6. punkta attiecīgi a) vai b) apakšpunktā.

- 17 – veselības un patērētāju aizsardzība

- 18 – iekšlietas

- 19 – ārējās attiecības

- 33 – tiesiskums

- 12 – iekšējais tirgus

1.4.3. Paredzamie rezultāti un ietekme

Norādīt, kāda ir priekšlikuma/iniciatīvas iecerētā ietekme uz finansējuma saņēmējiem/mērķgrupām.

Būtiski uzlabotos ES patērētāju, uzņēmumu un valdību aizsardzība pret TID incidentiem, apdraudējumiem un riskiem.

Plašāka informācija izklāstīta šim tiesību akta priekšlikumam pievienotā Komisijas dienestu darba dokumenta „Ietekmes novērtējums" 8.2. iedaļā (otrā risinājuma ietekme – regulatīvā pieeja).

1.4.4. Rezultātu un ietekmes rādītāji

Norādīt priekšlikuma/iniciatīvas īstenošanas uzraudzībā izmantojamos rādītājus.

Uzraudzības un novērtēšanas rādītāji izklāstīti ietekmes novērtējuma 10. iedaļā.

1.5. Priekšlikuma/iniciatīvas pamatojums

1.5.1. Īstermiņa vai ilgtermiņa vajadzības

Katrai dalībvalstij būtu jāievieš:

- valsts TID stratēģija;

- TID sadarbības plāns;

- par TID atbildīgā valsts kompetentā iestāde; un

- Datorapdraudējumu reaģēšanas vienība (*CERT*)

ES līmenī dalībvalstīm būtu jāsadarbojas, izmantojot tīklu.

Valsts pārvaldes iestādēm un galvenajiem privātā sektora dalībniekiem būtu jāveic TID riska pārvaldība un jāziņo kompetentajām iestādēm par TID incidentiem, kuriem ir būtiska ietekme.

1.5.2. ES iesaistīšanās pievienotā vērtība

Ņemot vērā TID pārrobežu raksturu, atšķirības attiecīgajos tiesību aktos un politikā uzņēmumiem rada šķēršļi, liedzot tiem darboties vairākās valstīs un panākt apjomradītus ietaupījumus pasaules mērogā. Neiejaukšanās ES līmenī radītu situāciju, kad katra dalībvalsts rīkotos atsevišķi, neņemot vērā tīklu un informācijas sistēmu savstarpēju atkarību.

Tāpēc izvirzītos mērķus var labāk sasniegt ES līmenī, nevis atsevišķās dalībvalstīs.

1.5.3. Līdzīgas līdzšinējās pieredzes rezultātā gūtās atziņas

Priekšlikuma izstrādē ir izmantota analīze, saskaņā ar kuru secināts, ka jāievieš regulatīvie pienākumi, lai radītu vienlīdzīgus konkurences apstākļus un novērstu pašreizējās likumdošanas nepilnības. Šajā jomā, izmantojot pilnībā brīvprātīgo pieeju, sadarbība izveidojusies tikai to nedaudzo dalībvalstu starpā, kurās ir augsta līmeņa spējas.

1.5.4. Saderība un iespējamā sinerģija ar citiem attiecīgajiem instrumentiem

Priekšlikums ir pilnībā saderīgs ar Eiropas digitalizācijas programmu Eiropai un attiecīgi ar stratēģiju „Eiropa 2020”. Tas arī atbilst ES tiesiskajam regulējumam par elektroniskajām komunikācijām, ES direktīvai par Eiropas kritisko infrastruktūru un ES Datu aizsardzības direktīvai, un papildina šos aktus.

Priekšlikums pievienots Komisijas paziņojumam par Eiropas kiberdrošības stratēģiju, ko sagatavojusi Komisija un Savienības Augstā pārstāve ārlietās un drošības politikas jautājumos, un ir tā būtiska sastāvdaļa.

1.6. Ilgums un finansiālā ietekme

– ☐ Ierobežota ilguma priekšlikums/iniciatīva

– ☐ Priekšlikuma/iniciatīvas darbības laiks: [DD.MM.]GGGG.–[DD.MM.]GGGG.

– ☐ Finansiālā ietekme: GGGG.– GGGG.

– ☒ Beztermiņa priekšlikums/iniciatīva

– Transponēšanas periods sāksies uzreiz pēc pieņemšanas (saskaņā ar aplēsēm 2015. gadā) un ilgs 18 mēnešus. Tomēr direktīvas īstenošana tiks sākta pēc tās pieņemšanas, un saskaņa ar to būs jāizveido droša infrastruktūra, veicinot dalībvalstu sadarbību.

– Pēc tam turpinās normāla darbība.

1.7. Paredzētie pārvaldības veidi[39]

– ☒ Komisijas īstenota centralizēta tieša pārvaldība

– ☒ Centralizēta netieša pārvaldība, izpildes uzdevumus deleģējot:

– ☐izpildaģentūrām

– ☒ Kopienu izveidotām struktūrām[40]

– ☐ valstu publiskā sektora struktūrām vai struktūrām, kas veic valsts pārvaldes uzdevumus

– ☐ personām, kurām ir uzticēts veikt īpašas darbības saskaņā ar Līguma par Eiropas Savienību V sadaļu un kuras ir noteiktas attiecīgā pamataktā Finanšu regulas 49. panta nozīmē

– ☐ Dalīta pārvaldība ar dalībvalstīm

– ☐ Decentralizēta pārvaldība kopā ar trešām valstīm

– ☐ Pārvaldība kopā ar starptautiskām organizācijām, tostarp Eiropas Kosmosa aģentūru

Ja norādīti vairāki pārvaldības veidi, sniedziet papildu informāciju iedaļā „Piezīmes”.

Piezīmes
Kopienu izveidota decentralizēta aģentūra *ENISA* var palīdzēt dalībvalstīm un Komisijai direktīvas īstenošanā, pamatojoties uz savām pilnvarām un to resursu pārcelšanu, kuri minētajai aģentūrai paredzēti atbilstīgi DFS 2014.–2020. gadam.

[39] Skaidrojumus par pārvaldības veidiem un atsauces uz Finanšu regulu skatīt *BudgWeb* tīmekļa vietnē: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.htmlhttp://www.cc.cec/budg/man/budgmanag/budgmanag_en.html.

[40] Kā paredzēts Finanšu regulas 185. pantā.

2. PĀRVALDĪBAS PASĀKUMI

2.1. Uzraudzības un ziņošanas noteikumi

Norādīt periodiskumu un nosacījumus.

Komisija regulāri pārskatīs direktīvas darbību un iesniegs ziņojumus Eiropas Parlamentam un Padomei.

Komisija arī izvērtēs, vai dalībvalstīs direktīva transponēta pareizi.

EISI priekšlikumā paredzēta arī iespēja izvērtēt projektu izpildes metodes un to īstenošanas ietekmi, lai novērtētu, vai ir sasniegti mērķi, ieskaitot mērķus, kas skar vides aizsardzību.

2.2. Pārvaldības un kontroles sistēma

2.2.1. Apzinātie riski

- Novēlota projekta īstenošana saistībā ar drošas infrastruktūras izveidi

2.2.2. Paredzētās kontroles metodes

Nolīgumos un lēmumos, ar ko īsteno darbības saskaņā ar EISI, tiks paredzēta uzraudzība un finanšu kontrole, ko veic Komisija vai Komisijas pilnvarots pārstāvis, kā arī revīzijas, ko veic Revīzijas palāta, pārbaudes uz vietas, ko veic Eiropas Birojs krāpšanas apkarošanai (OLAF).

2.2.3. Kontroļu izmaksas un ieguvumi un iespējamais neatbilstību līmenis

Ex ante un *ex post* kontroles, kas balstītas uz riskiem, un iespējas veikt pārbaudes uz vietas nodrošinās, ka kontroles izmaksas ir samērīgas.

2.3. Krāpšanas un pārkāpumu apkarošanas pasākumi

Norādīt esošos vai plānotos novēršanas un aizsardzības pasākumus.

Komisija veic atbilstošus pasākumus, lai nodrošinātu, ka, īstenojot saskaņā ar šo direktīvu finansētas darbības, Savienības finansiālās intereses tiek aizsargātas, piemērojot aizsargpasākumus pret krāpšanu, korupciju un jebkādām citām nelikumīgām darbībām, veicot efektīvas pārbaudes un, ja ir atklāti pārkāpumi, atgūstot nepamatoti izmaksātās summas un attiecīgā gadījumā piemērojot iedarbīgus, samērīgus un preventīvus sodus.

Komisijai vai tās pārstāvjiem un Revīzijas palātai ir tiesības, pārbaudot dokumentus un veicot pārbaudes uz vietas, revidēt visus dotāciju saņēmējus, līgumslēdzējus un apakšuzņēmējus, kuri šīs programmas ietvaros ir saņēmuši Savienības līdzekļus.

Eiropas Birojs krāpšanas apkarošanai (OLAF) var veikt inspekcijas un pārbaudes uz vietas attiecībā uz uzņēmējiem, uz kuriem tieši vai netieši attiecas šāds finansējums, saskaņā ar Regulā (Euratom, EK) Nr. 2185/96 noteiktajām procedūrām, lai noteiktu, vai saistībā ar dotāciju līgumu vai dotāciju lēmumu, vai līgumu, kas attiecas uz Savienības finansējumu, ir notikusi krāpšana, korupcija vai jebkādas citas nelikumīgas darbības, kas ietekmē Savienības finansiālās intereses.

Neskarot iepriekš minētos punktus, sadarbības nolīgumos ar trešām valstīm un starptautiskām organizācijām, dotāciju nolīgumos, dotāciju lēmumos un līgumos, kas izriet no šīs regulas īstenošanas, nepārprotami nosaka Komisijas, Revīzijas palātas un OLAF pilnvaras veikt šādas revīzijas, inspekcijas un pārbaudes uz vietas.

EISI paredzēts, ka dotāciju un iepirkumu līgumu pamatā būs standarta modeļi, kuros būs izklāstīti vispārpiemērojamie krāpšanas apkarošanas pasākumi.

3. PRIEKŠLIKUMA/INICIATĪVAS PAREDZAMĀ FINANSIĀLĀ IETEKME

3.1. Attiecīgās daudzgadu finanšu shēmas izdevumu kategorijas un budžeta izdevumu pozīcijas

- Esošās budžeta izdevumu pozīcijas

Sarindotas pa daudzgadu finanšu shēmas izdevumu kategorijām un budžeta pozīcijām

Daudzgadu finanšu shēmas izdevumu kategorija	Budžeta pozīcija	Izdevumu veids	Iemaksas			
	Numurs [Izdevumu kategorija……...…….]	Dif./nedif. (41)	no EBTA valstīm[42]	no kandidātvalstīm[43]	no trešām valstīm	Finanšu regulas 18. panta 1. punkta aa) apakšpunkta nozīmē
	09 03 02 sekmēt valstu publisko tiešsaistes pakalpojumu starpsavienojumus un sadarbspēju, kā arī piekļuvi šādiem tīkliem	Dif.	NĒ	NĒ	NĒ	NĒ

- No jauna veidojamās budžeta pozīcijas (nepiemēro)

Sarindotas pa daudzgadu finanšu shēmas izdevumu kategorijām un budžeta pozīcijām

Daudzgadu finanšu shēmas izdevumu kategorija	Budžeta pozīcija	Izdevumu veids	Iemaksas			
	Numurs [Izdevumu kategorija.....….]	Dif./nedif.	no EBTA valstīm	no kandidātvalstīm	no trešām valstīm	Finanšu regulas 18. panta 1. punkta aa) apakšpunkta nozīmē
	[XX.YY.YY.YY]		JĀ/NĒ	JĀ/NĒ	JĀ/NĒ	JĀ/NĒ

41 Dif. – diferencētās apropriācijas, nedif. – nediferencētās apropriācijas.

42 EBTA – Eiropas Brīvās tirdzniecības asociācija.

43 Kandidātvalstis un attiecīgā gadījumā potenciālās kandidātvalstis no Rietumbalkāniem.

3.2. Paredzamā ietekme uz izdevumiem

3.2.1. Paredzamās ietekmes uz izdevumiem kopsavilkums

Miljonos EUR (3 zīmes aiz komata)

Daudzgadu finanšu shēmas izdevumu kategorija:	1	Gudra un iekļaujoša izaugsme

ĢD: <…….>			2015* [44]	**2016.** gads	**2017.** gads	**2018.** gads	Nākamie gadi (2019–2021) un turpmāk			**KOPĀ**
• Darbības apropriācijas										
09 03 02	Saistības	(1)	1,250**	0,000						**1,250**
	Maksājumi	(2)	0,750	0,250	0,250					**1,250**
Administratīvās apropriācijas, kas tiek finansētas no konkrētu programmu piešķīrumiem[45]			**0,000**							**0,000**
Budžeta pozīcijas numurs		(3)	**0,000**							**0,000**
KOPĀ — <…….> ĢD apropriācijas	Saistības	=1+1a +3	1,250	0,000						**1,250**
	Maksājumi	=2+2a +3	0,750	0,250	0,250					**1,250**

• KOPĀ — Darbības apropriācijas	Saistības	(4)	1,250	0,000						**1,250**
	Maksājumi	(5)	0,750	0,250	0,250					**1,250**

[44] N gads ir gads, kurā sāk īstenot priekšlikumu/iniciatīvu.

[45] Tehniskais un/vai administratīvais atbalsts un ES programmu un/vai darbību īstenošanas atbalsta izdevumi (kādreizējās „*BA*” pozīcijas), netiešā pētniecība, tiešā pētniecība.

• KOPĀ — Administratīvās apropriācijas, kas tiek finansētas no konkrētu programmu piešķīrumiem		(6)	**0,000**							
KOPĀ — Daudzgadu finanšu shēmas **1. IZDEVUMU KATEGORIJAS apropriācijas**	Saistības	=4+ 6	1,250	0,000						**1,250**
	Maksājumi	=5+ 6	0,750	0,250	0,250					**1,250**

* Precīzs termiņš būs atkarīgs no tā, kurā datumā likumdevēja iestāde pieņems priekšlikumu (t.i., ja direktīva tiks apstiprināta 2014. gadā, pašreizējās infrastruktūras pielāgošana sāktos 2015. gadā, bet citos gadījumos vienu gadu vēlāk).

** Ja dalībvalstis izvēlas izmantot pašreizējo infrastruktūru un pielāgošanas vienreizējās izmaksas segt no ES budžeta, kā skaidrots 1.4.3. un 1.7. punktā, tad saskaņā ar aplēsēm izmaksas tīkla pielāgošanai, lai atbalstītu dalībvalstu sadarbību saskaņā ar direktīvas III nodaļu (agrīnā brīdināšana, saskaņota reaģēšana utt.), ir EUR 1 250 000. Šī summa ir nedaudz lielāka par ietekmes novērtējumā minēto („aptuveni 1 miljons euro”), jo šajā gadījumā precīzāk aprēķināti šādai infrastruktūrai vajadzīgie pamatelementi. Vajadzīgie pamatelementi un ar tiem saistītās izmaksas aprēķinātas atbilstīgi Kopīgā pētniecības centra aplēsēm, pamatojoties uz tā pieredzi līdzīgu sistēmu izstrādāšanā citās jomās, piemēram, sabiedrības veselības jomā, un šim aprēķinam vajadzētu būt šādam: TID paredzēta ātrās brīdināšanas un paziņojumu sistēma (EUR 275 000); informācijas apmaiņas platforma (EUR 400 000); agrīnās brīdināšanas un reaģēšanas sistēma (EUR 275 000); ārkārtas situāciju centrs (EUR 300 000); kopējā summa ir EUR 1 250 000. Sīkāku īstenošanas plānu paredzēts iekļaut topošajā priekšizpētē, kas tiek veikta saskaņā ar konkrētu līgumu „SMART 2012/0010”, proti, „priekšizpētes un sagatavošanās darbības, lai īstenotu Eiropas Agrīnās brīdināšanas un reaģēšanas sistēmu pret kiberuzbrukumiem un infrastruktūras darbības pārrāvumiem”.

Gadījumā, ja priekšlikums/iniciatīva ietekmē vairākas izdevumu kategorijas

• KOPĀ — Darbības apropriācijas	Saistības	(4)	0,000	0,000						
	Maksājumi	(5)	0,000	0,000						
• KOPĀ — Administratīvās apropriācijas, kas tiek finansētas no konkrētu programmu piešķīrumiem		(6)	**0,000**	**0,000**						
KOPĀ — Daudzgadu finanšu shēmas **1.–4. IZDEVUMU KATEGORIJAS apropriācijas** (Pamatsumma)	Saistības	=4+ 6	1,250	0,000						1,250
	Maksājumi	=5+ 6	0,750	0,250	0,250					1,250

Daudzgadu finanšu shēmas izdevumu kategorija	**5**	„Administratīvie izdevumi”

Miljonos EUR (3 zīmes aiz komata)

		2015. gads	**2016.** gads	**2017.** gads	**2018.** gads	Nākamie gadi (2019–2021) un turpmāk			**KOPĀ**
CNECT ĢD									
• Cilvēkresursi		0,572	0,572	0,572	0,572	0,572	0,572	**0,572**	**4,004**
• Pārējie administratīvie izdevumi		0,318	0,118	0,318	0,118	0,318	0,118	**0,118**	**1,426**
KOPĀ — CNECT **ĢD**	Apropriācijas	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**

KOPĀ — Daudzgadu finanšu shēmas 5**. IZDEVUMU KATEGORIJAS apropriācijas**	(Saistību summa = maksājumu summa)	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**

Miljonos EUR (3 zīmes aiz komata)

		2015. gads[46]	**2016.** gads	**2017.** gads	**2018.** gads	Nākamie gadi (2019–2021) un turpmāk			**KOPĀ**
KOPĀ — Daudzgadu finanšu shēmas **5. IZDEVUMU KATEGORIJAS apropriācijas**	Saistības	2,140	0,690	0,890	0,690	0,890	0,690	0,690	**6,680**
	Maksājumi	1,640	0,940	1,140	0,690	0,890	0,690	0,690	**6,680**

[46] N gads ir gads, kurā sāk īstenot priekšlikumu/iniciatīvu.

3.2.2. Paredzamā ietekme uz darbības apropriācijām

– ☐ Priekšlikums/iniciatīva neparedz darbības apropriāciju izmantošanu

– ☑ Priekšlikums/iniciatīva paredz darbības apropriāciju izmantošanu šādā veidā:

– Saistību apropriācijas miljonos EUR (3 zīmes aiz komata)

Norādīt mērķus un rezultātus ⇩			**2015.** gads*		**2016.** gads		**2017.** gads		**2018.** gads		Nākamie gadi (2019–2021) un turpmāk						**KOPĀ**	
	REZULTĀTI																	
	Rezultāta veids[47]	Rezultātu vidējās izmaksas	Daudzums	Izmaksas	Daudzums	Izmaksas	Daudzums	Izmaksas	Daudzums	Izmaksas	Daudzums	Izmaksas	Daudzums	Izmaksas	Daudzums	Izmaksas	Kopējais rezultātu daudzums	Kopējās izmaksas
KONKRĒTAIS MĒRĶIS NR. 2[48] Droša informācijas apmaiņas infrastruktūra																		
- Rezultāts	Infrastruktūras pielāgošana																	
Starpsumma — konkrētais mērķis Nr. 2			1	1.250**													1	1.250
KOPĒJĀS IZMAKSAS				1.250														1.250

47 Rezultāti ir attiecīgie produkti un pakalpojumi (piemēram, finansēto studentu apmaiņas braucienu skaits, uzbūvēto ceļu garums km utt.).

48 Konkrētie mērķi, kas norādīti 1.4.2. punktā.

* Precīzs termiņš būs atkarīgs no tā, kurā datumā likumdevēja iestāde pieņems priekšlikumu (t.i., ja direktīva tiks apstiprināta 2014. gadā, pašreizējās infrastruktūras pielāgošana sāktos 2015. gadā, bet citos gadījumos vienu gadu vēlāk).

** Sk. 3.2.1. punktu.

3.2.3. Paredzamā ietekme uz administratīvajām apropriācijām

3.2.3.1. Kopsavilkums

– ☐ Priekšlikums/iniciatīva neparedz administratīvo apropriāciju izmantošanu

– ☑ Priekšlikums/iniciatīva paredz administratīvo apropriāciju izmantošanu šādā veidā:

Miljonos EUR (3 zīmes aiz komata)

	2015. gads[49]	**2016.** gads	**2017.** gads	**2018.** gads	Nākamie gadi (2019–2021) un turpmāk			**KOPĀ**
Daudzgadu finanšu shēmas 5. IZDEVUMU KATEGORIJA								
Cilvēkresursi	0,572	0,572	0,572	0,572	0,572	0,572	0,572	**4,004**
Pārējie administratīvie izdevumi	0,318	0,118	0,318	0,118	0,318	0,118	0,118	**1,426**
Starpsumma — Daudzgadu finanšu shēmas 5. IZDEVUMU KATEGORIJA	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**
Ārpus daudzgadu finanšu shēmas 5. IZDEVUMU KATEGORIJAS[50]								
Cilvēkresursi	0.000	0.000						**0,000**
Citi administratīvie izdevumi								
Starpsumma — Ārpus daudzgadu finanšu shēmas 5. IZDEVUMU KATEGORIJAS	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**
KOPĀ	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**

Nepieciešamās administratīvās apropriācijas tiks nodrošinātas, izmantojot apropriācijas, kuras jau piešķirtas darbības pārvaldībai un/vai tiks pārgrupētas, vajadzības gadījumā izmantojot vadošajam ĢD gada budžeta sadales procedūrā piešķirtos papildu resursus un ņemot vērā budžeta ierobežojumus.

49 Year N is the year in which implementation of the proposal/initiative starts.

50 Tehniskais un/vai administratīvais atbalsts un ES programmu un/vai darbību īstenošanas atbalsta izdevumi (kādreizējās „*BA*" pozīcijas), netiešā pētniecība, tiešā pētniecība.

Eiropas Tīklu un informācijas drošības aģentūra (*ENISA*) var palīdzēt dalībvalstīm un Komisijai direktīvas īstenošanā, pamatojoties uz savām pilnvarām un to resursu pārcelšanu, kuri minētajai aģentūrai paredzēti atbilstīgi DFS 2014.–2020. gadam, t.i., bez jebkādiem papildu budžeta vai cilvēku resursu piešķīrumiem.

3.2.3.2. Paredzamās cilvēkresursu vajadzības

– ☐ Priekšlikums/iniciatīva neparedz cilvēkresursu izmantošanu

– ☑ Priekšlikums/iniciatīva paredz cilvēkresursu izmantošanu šādā veidā:

Principā papildu darbaspēks nebūtu vajadzīgs. Vajadzīgo cilvēkresursu apjoms būs ļoti neliels, un tas tiks nodrošināts, izmantojot tā ĢD darbiniekus, kuri jau ir iesaistīti konkrētās darbības pārvaldībā.

Paredzamais apjoms izsakāms veselos skaitļos (vai maksimāli ar vienu zīmi aiz komata)

	2015. gads	**2016.** gads	**2017.** gads	**2018.** gads	Nākamie gadi (2019–2021) un turpmāk		
• Štatu sarakstā ietvertās amata vietas (ierēdņi un pagaidu darbinieki)							
09 01 01 01 (Galvenā mītne un Komisijas pārstāvniecības)	4	4	4	4	4	4	4
XX 01 01 02 (Delegācijas)							
XX 01 05 01 (Netiešā pētniecība)							
10 01 05 01 (Tiešā pētniecība)							
• Ārštata darbinieki (izsakot ar pilnslodzes ekvivalentu – *FTE*[51])							
09 01 02 01 (*CA*, *INT*, *SNE*, ko finansē no vispārīgajām apropriācijām)	1	1	1	1	1	1	1
XX 01 02 02 (*CA*, *INT*, *JED*, *LA* un *SNE* delegācijās)							
XX 01 04 yy[52] - Galvenā mītne[53]							
XX 01 04 yy[52] - Delegācijas							
XX 01 05 02 (*CA*, *INT*, *SNE* — netiešā pētniecība)							
10 01 05 02 (*CA*, *INT*, *SNE* — tiešā pētniecība)							
Citas budžeta pozīcijas (precizēt)							
KOPĀ	**5**	**5**	**5**	**5**	**5**	**5**	**5**

XX ir attiecīgā politikas joma vai budžeta sadaļa.

Cilvēkresursu vajadzības tiks nodrošinātas, izmantojot CNECT ĢD darbiniekus, kuri jau ir iesaistīti konkrētās darbības pārvaldībā un/vai ir pārgrupēti attiecīgajā ģenerāldirektorātā, vajadzības gadījumā izmantojot vadošajam ĢD gada budžeta sadales procedūrā piešķirtos papildu resursus un ņemot vērā budžeta ierobežojumus.

Eiropas Tīklu un informācijas drošības aģentūra (*ENISA*) var palīdzēt dalībvalstīm un Komisijai direktīvas īstenošanā, pamatojoties uz savām pašreizējām pilnvarām un to resursu pārcelšanu, kuri minētajai aģentūrai paredzēti atbilstīgi DFS 2014.–2020. gadam, t.i., bez jebkādiem papildu budžeta vai cilvēku resursu piešķīrumiem.

51 *CA* — līgumdarbinieki; *INT* — pagaidu darbinieki; *JED* — jaunākie eksperti delegācijās; *LA* — vietējie darbinieki; *SNE* — valstu norīkotie eksperti.

52 Saskaņā ar robežlielumiem attiecībā uz ārštata darbiniekiem, ko finansē no darbības apropriācijām (kādreizējām „*BA*" pozīcijām).

53 Galvenokārt struktūrfondi, Eiropas Lauksaimniecības fonds lauku attīstībai (ELFLA) un Eiropas Zivsaimniecības fonds (EZF).

Veicamo uzdevumu apraksts

Ierēdņi un pagaidu darbinieki	- Deleģēto tiesību aktu sagatavošana saskaņā ar 14. panta 3. punktu - Īstenošanas tiesību aktu sagatavošana saskaņā ar 8. pantu, 9. panta 2. punktu, 12. pantu, 14. panta 5. punktu un 16. pantu - Gan politikas, gan operatīvā līmeņa sadarbības sekmēšana, izmantojot tīklu - Iesaistīšanās starptautiskajās sarunās un starptautisku nolīgumu iespējama noslēgšana
Ārštata darbinieki	Pēc vajadzības sniegt atbalstu visos minētajos uzdevumos

3.2.4. Saderība ar kārtējo daudzgadu finanšu shēmu

– ☑ Priekšlikums/iniciatīva atbilst kārtējai daudzgadu finanšu shēmai

– ☐ Pieņemot priekšlikumu/iniciatīvu, jāpārplāno attiecīgā izdevumu kategorija daudzgadu finanšu shēmā

Šī priekšlikuma aplēstā finansiālā ietekme uz darbības izdevumiem būs tādā gadījumā, ja dalībvalstis izvēlēsies pielāgot pašreizējo infrastruktūru, uzdodot Komisiju īstenot tās pielāgošanu saskaņā ar DFS 2014.–2020. gadam. Saistītās vienreizējās izmaksas būtu jāsedz no EISI, ja vien ir pieejams pietiekams finansējums. Dalībvalstis var arī kopīgi segt infrastruktūras pielāgošanas izmaksas vai jaunas infrastruktūras izveides izmaksas.

– ☐ Pieņemot priekšlikumu/iniciatīvu, jāpiemēro elastības instruments vai jāpārskata daudzgadu finanšu shēma[54].

Neattiecas.

3.2.5. Trešo personu dalība finansējumā

– Priekšlikums/iniciatīva neparedz trešo personu līdzfinansējumu

3.3. Paredzamā ietekme uz ieņēmumiem

– ☑ Priekšlikums/iniciatīva finansiāli neietekmē ieņēmumus

[54] Skatīt Iestāžu nolīguma 19. un 24. punktu.