EUROPOS
KOMISIJA

Briuselis, 2013 02 07
COM(2013) 48 final

2013/0027 (COD)

Pasiūlymas

EUROPOS PARLAMENTO IR TARYBOS DIREKTYVA

dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti

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

AIŠKINAMASIS MEMORANDUMAS

Siūlomos direktyvos tikslas – užtikrinti aukštą bendrą tinklų ir informacijos saugumo (TIS) lygį. Tai reiškia, kad turi būti didinamas interneto ir privačių tinklų bei informacinių sistemų, palaikančių mūsų visuomenės ir ekonomikos funkcionavimą, saugumas. To bus pasiekta reikalaujant, kad valstybės narės didintų savo parengtį ir gerintų tarpusavio bendradarbiavimą, o tokios ypatingos svarbos infrastruktūros kaip energetikos ir transporto operatoriai ir svarbiausių informacinės visuomenės paslaugų (e. prekybos platformų, socialinių tinklų ir pan.) teikėjai, taip pat viešojo administravimo institucijos imtųsi tinkamų veiksmų saugumo rizikai valdyti, o apie rimtus incidentus informuotų nacionalines kompetentingas institucijas.

Šis pasiūlymas teikiamas kartu su bendru Komisijos ir Sąjungos vyriausiosios įgaliotinės užsienio reikalams ir saugumo politikai komunikatu dėl Europos kibernetinio saugumo strategijos. Strategijos tikslas – užtikrinti saugią ir patikimą skaitmeninę aplinką, kartu remiant ir apsaugant pagrindines teises ir kitas pagrindines ES vertybes. Šis pasiūlymas yra pagrindinė strategijos dalis. Tolesni strategijoje numatyti šios srities veiksmai daugiausia bus skirti informuotumui didinti, kibernetinio saugumo produktams ir paslaugoms kurti ir investicijoms į mokslinius tyrimus ir technologinę plėtrą skatinti. Šiuos veiksmus papildys kiti veiksmai, skirti kovai su elektroniniais nusikaltimais skatinti ir ES tarptautinio kibernetinio saugumo politikai formuoti.

1.1. Pasiūlymo pagrindas ir tikslai

TIS svarba mūsų ekonomikai ir visuomenei vis labiau didėja. TIS taip pat yra svarbi patikimos aplinkos pasaulinei prekybai paslaugomis sukūrimo prielaida. Tačiau informacinėms sistemoms gali pakenkti tokie saugumo incidentai kaip žmogiškos klaidos, gamtos reiškiniai, techniniai gedimai ar piktavališki išpuoliai. Šie incidentai tampa vis didesni, dažnesni ir sudėtingesni**.** Per Komisijos viešas konsultacijas internete tema „Tinklų ir informacijos saugumo gerinimas ES“[1] nustatyta, kad praėjusiais metais 57 % respondentų susidūrė su TIS incidentais, kurie turėjo rimtų padarinių jų veiklai. TIS trūkumas gali kelti pavojų gyvybiškai svarbioms paslaugoms, kurios yra priklausomos nuo tinklų ir informacinių sistemų vientisumo. Tai gali sustabdyti įmonių veiklą, sukelti didelių finansinių nuostolių ES ekonomikai ir turėti neigiamo poveikio visuomenės gerovei.

Be to, kaip sienų neturinti ryšių priemonė, skaitmeninės informacinės sistemos, visų pirma internetas, yra tarpusavyje susijusios visose valstybėse narėse ir atlieka labai svarbų vaidmenį skatinant prekių, paslaugų ir asmenų judėjimą tarp valstybių. Didelis šių sistemų sutrikimas vienoje valstybėje narėje gali turėti poveikio kitoms valstybėms narėms ir visai ES. Todėl tinklų ir informacinių sistemų atsparumas ir stabilumas yra labai svarbūs bendrosios skaitmeninės rinkos įgyvendinimui ir sklandžiam vidaus rinkos veikimui. Incidentų tikimybė bei dažnumas ir nesugebėjimas užtikrinti veiksmingos apsaugos taip pat kenkia visuomenės pasitikėjimui tinklų ir informacinėmis paslaugomis; pavyzdžiui, per 2012 m. Eurobarometro apklausą apie kibernetinį saugumą nustatyta, kad 38 % ES interneto vartotojų nerimauja dėl mokėjimo internetu saugumo ir todėl pakeitė savo elgesį – 18 % yra mažiau linkę pirkti internetu ir 15 % yra mažiau linkę naudotis internetinės bankininkystės paslaugomis[2].

Dabartinė situacija ES, kurioje iki šiol laikomasi grynai savanoriško požiūrio, yra tokia, kad ES mastu neužtikrinama pakankama apsauga nuo TIS incidentų ir rizikos. Egzistuojančių TIS pajėgumų ir priemonių paprasčiausiai nepakanka, kad būtų tinkamai atsižvelgiama į sparčiai

[1] Viešos konsultacijos internete tema „Tinklų ir informacijos saugumo gerinimas ES“ vyko nuo 2012 m. liepos 23 d. iki spalio 15 d.

[2] Eurobarometras 390/2012.

kintančias grėsmes ir būtų užtikrintas aukštas bendras apsaugos lygis visose valstybėse narėse.

Nepaisant iniciatyvų, kurių buvo imtasi, valstybių narių pajėgumų ir parengties lygis yra labai skirtingas, todėl visoje ES susiformavo skirtingi požiūriai. Atsižvelgiant į tai, kad tinklai ir sistemos yra tarpusavyje susiję, tos valstybės narės, kuriose apsaugos lygis yra nepakankamas, mažina bendrą visos ES tinklų ir informacijos saugumą. Tokia situacija taip pat trukdo kurti tarpusavio pasitikėjimą, kuris yra būtina bendradarbiavimo ir dalijimosi informacija sąlyga. Dėl to bendradarbiavimas vyksta tik tarp mažumos valstybių narių, kurių pajėgumai yra dideli.

Todėl šiuo metu nėra veiksmingo bendradarbiavimo ir dalijimosi patikima informacija apie TIS incidentus ir riziką tarp valstybių narių mechanizmo. Tai gali lemti nekoordinuotas reguliavimo intervencijas, nenuoseklias strategijas ir skirtingus standartus, dėl kurių apsauga nuo TIS incidentų visoje ES tampa nepakankama. Taip pat gali atsirasti vidaus rinkos kliūčių, dėl kurių įmonės, vykdančios veiklą daugiau nei vienoje valstybėje narėje, patirs reikalavimų laikymosi išlaidų.

Galiausiai, rinkos dalyviai, valdantys ypatingos svarbos infrastruktūrą ar teikiantys visuomenės funkcionavimui būtinas paslaugas, nėra deramai įpareigoti taikyti rizikos valdymo priemonių ir keistis informacija su atitinkamomis institucijomis. Viena vertus, dėl šios priežasties verslo įmonėms trūksta veiksmingų paskatų vykdyti rimtą rizikos valdymą, apimantį rizikos įvertinimą ir atitinkamus veiksmus TIS užtikrinti. Kita vertus, informacija apie didelę dalį incidentų nepasiekia kompetentingų institucijų ir jie lieka nepastebėti. Tačiau informacija apie incidentus yra labai svarbi, kad valdžios institucijos reaguotų, imtųsi tinkamų švelninančių priemonių ir nustatytų tinkamus strateginius TIS prioritetus.

Pagal dabartinę reguliavimo sistemą tik telekomunikacijos įmonės privalo imtis rizikos valdymo priemonių ir pranešti apie rimtus TIS incidentus. Tačiau ir daugeliui kitų sektorių IRT yra svarbi priemonė veiklai vykdyti, todėl ir jos turėtų taip pat susirūpinti TIS. Kai kurie specifinės infrastruktūros ar paslaugų teikėjai yra itin pažeidžiami, nes jie yra labai priklausomi nuo tinkamo tinklų ir informacinių sistemų veikimo. Šiems sektoriams tenka svarbus vaidmuo teikiant pagrindines paramos paslaugas mūsų ekonomikai ir visuomenei, o jų sistemų saugumas yra labai svarbus vidaus rinkos veikimui. Tarp šių sektorių – bankininkystė, vertybinių popierių biržos, energijos gamyba, perdavimas ir paskirstymas, transportas (oro, geležinkelių, jūrų), sveikatos priežiūra, interneto paslaugos ir viešojo administravimo institucijos.

Todėl Europos Sąjungoje požiūrį į TIS reikia keisti iš esmės. Siekiant sukurti vienodas veiklos sąlygas ir pašalinti esamas įstatymų spragas, reikalingi reguliavimo įpareigojimai. Siekiant spręsti šias problemas ir didinti TIS lygį Europos Sąjungoje, siūloma direktyva keliami toliau išdėstyti tikslai.

Pirma, pasiūlymu reikalaujama, kad visos valstybės narės užtikrintų minimalų nacionalinių pajėgumų lygį ir įsteigtų kompetentingas TIS institucijas, sukurtų kompiuterinių incidentų tyrimo tarnybas (CERT) ir priimtų nacionalines TIS strategijas bei nacionalinius TIS bendradarbiavimo planus.

Antra, nacionalinės kompetentingos institucijos turėtų bendradarbiauti tinkle užtikrindamos saugų ir veiksmingą koordinavimą, įskaitant koordinuotą keitimąsi informacija, taip pat problemų nustatymą ir atsakomuosius veiksmus ES lygmeniu. Per šį tinklą valstybės narės turėtų keistis informacija ir bendradarbiauti, kad galėtų kovoti su TIS grėsmėmis ir incidentais remdamosi Europos TIS bendradarbiavimo planu.

Trečia, Pagrindų direktyvos dėl elektroninių ryšių modeliu grindžiamu pasiūlymu siekiama užtikrinti, kad būtų formuojama rizikos valdymo kultūra ir kad privatusis ir viešasis sektoriai dalintųsi informacija tarpusavyje. Pirmiau minėtų specifinių ypatingos svarbos sektorių įmonės ir viešojo administravimo institucijos turės įvertinti joms kylančią riziką ir priimti atitinkamas ir proporcingas priemones tinklų ir informacijos saugumui užtikrinti. Šie subjektai privalės pranešti kompetentingoms valdžios institucijoms apie visus incidentus, kurie kelia didelę grėsmę jų tinklų ir informacinėms sistemoms ir turi didelės neigiamos įtakos jų ypatingos svarbos paslaugų ir prekių tiekimo tęstinumui.

1.2. Bendrosios aplinkybės

Dar 2001 m. komunikate „Tinklų ir informacijos apsauga. Pasiūlymas dėl Europos politikos požiūrio“ Komisija nurodė didėjančią TIS svarbą[3]. 2006 m. buvo priimta ES saugios informacinės visuomenės strategija[4], skirta TIS kultūros kūrimui Europoje. Pagrindiniai jos elementai buvo patvirtinti Tarybos rezoliucija[5].

2009 m. kovo 30 d., Komisija priėmė komunikatą dėl ypatingos svarbos informacinės infrastruktūros apsaugos (CIIP)[6], kuriame daugiausiai dėmesio skiriama Europos apsaugai nuo kibernetinių trukdžių didinant saugumą. Komunikate paskelbtas veiksmų planas, kuriuo remiamos valstybių narių pastangos užtikrinti prevencinius ir atsakomuosius veiksmus. Veiksmų planas buvo patvirtintas 2009 m. Taline vykusios ministrų konferencijos ypatingos svarbos informacinės infrastruktūros apsaugos klausimais pirmininkaujančios valstybės narės išvadose. 2009 m. gruodžio 18 d. Taryba priėmė rezoliuciją dėl bendradarbiavimu paremto Europos požiūrio į tinklų ir informacijos saugumą[7].

2010 m. gegužės mėn. priimtoje Europos skaitmeninėje darbotvarkėje[8] ir susijusiose Tarybos išvadose[9] pabrėžiama bendra nuomonė, kad pasitikėjimas ir saugumas yra pagrindinės plataus IRT diegimo, taigi ir su pažangaus augimo aspektu susijusių strategijos „Europa 2020“[10] tikslų įgyvendinimo sąlygos. Europos skaitmeninės darbotvarkės skyriuje „Pasitikėjimas ir saugumas“ pabrėžiama, jog visos suinteresuotosios šalys turi dėti bendras pastangas, kad būtų užtikrintas IRT infrastruktūros saugumas ir atsparumas, daugiausia dėmesio skiriant prevencijai, parengčiai ir informuotumui, ir kad būtų sukurti veiksmingi ir suderinti saugumo mechanizmai. Be kita ko, Europos skaitmeninės darbotvarkės 6 pagrindinėje priemonėje reikalaujama imtis priemonių, kurių tikslas – formuoti griežtesnę aukšto lygio tinklų ir informacijos saugumo politiką.

2011 m. kovo mėn. Komunikate dėl ypatingos svarbos informacinės infrastruktūros apsaugos „Visuotinio kibernetinio saugumo užtikrinimas. Laimėjimai ir tolesni veiksmai“[11] Komisija apibendrino rezultatus, pasiektus nuo CIIP veiksmų plano priėmimo 2009 m., ir padarė išvadą, kad plano įgyvendinimas parodė, jog vien nacionalinio požiūrio į saugumo ir atsparumo uždavinių sprendimą nepakanka, ir kad Europa ir toliau turėtų stengtis, kad visoje ES būtų suformuotas nuoseklus ir bendradarbiavimu grindžiamas požiūris. Komisijai paraginus valstybes nares stiprinti TIS pajėgumus ir tarpvalstybinį bendradarbiavimą, 2011 m. CIIP komunikate paskelbta keletas veiksmų. Dauguma šių veiksmų turėjo būti įgyvendinti iki 2012 m., tačiau kol kas to nepadaryta.

---

3 COM(2001) 298.
4 COM(2006) 251 http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0251en01.pdf.
5 2007/068/01.
6 COM(2009) 149.
7 2009/C 321/01.
8 COM(2010) 245.
9 2010 m. gegužės 31 d. Tarybos išvados dėl Europos skaitmeninės darbotvarkės (10130/10).
10 COM(2010) 2020 ir 2010 m. kovo 25–26 d. Europos Vadovų Tarybos išvados (EUCO 7/10).
11 COM(2011) 163.

2011 m. gegužės 27 d. išvadose dėl CIIP Europos Sąjungos Taryba pabrėžė neatidėliotiną poreikį užtikrinti, kad IRT sistemos ir tinklai būtų atsparūs ir apsaugoti nuo visų galimų sutrukdymų, tiek atsitiktinių, tiek tyčinių, visoje ES užtikrinti aukšto lygio parengtį, saugumą ir atsparumą, atnaujinti technines kompetencijas, kad Europa galėtų imtis tinklų ir informacinės infrastruktūros apsaugos uždavinių, ir skatinti valstybių narių tarpusavio bendradarbiavimą kuriant valstybių narių bendradarbiavimo mechanizmus incidentų atveju.

1.3. Taikomos šios srities Europos Sąjungos ir tarptautinės nuostatos

Reglamentu (EB) Nr. 460/2004 Europos Bendrija 2004 m. įsteigė Europos tinklų ir informacijos apsaugos agentūrą (ENISA)[12], kurios tikslas – padėti užtikrinti aukštą TIS lygį ir kurti TIS kultūrą ES. Pasiūlymas atnaujinti ENISA mandatą buvo priimtas 2010 m. rugsėjo 30 d.[13] ir šiuo metu yra svarstomas Taryboje ir Europos Parlamente. Peržiūrėtoje elektroninių ryšių tinklų ir paslaugų bendrosios reguliavimo sistemoje[14], galiojančioje nuo 2009 m. lapkričio mėn., nustatyti saugumo įpareigojimai elektroninių ryšių paslaugų teikėjams[15]. Šie įpareigojimai turėjo būti perkelti į nacionalinę teisę iki 2011 m. gegužės mėn.

Visi rinkos dalyviai, kurie valdo duomenis (pavyzdžiui, bankai arba ligoninės), duomenų apsaugos reglamentavimo sistemos[16] yra įpareigoti įsidiegti saugumo priemones asmens duomenims apsaugoti. Taip pat pagal 2012 m. Komisijos bendrojo duomenų apsaugos reglamento pasiūlymą[17], duomenų valdytojai turėtų pranešti nacionalinėms priežiūros institucijoms apie asmens duomenų saugumo pažeidimus. Tai reiškia, kad, pavyzdžiui, apie TIS pažeidimą, kuris turi neigiamos įtakos paslaugos teikimui, bet nesukelia grėsmės asmens duomenims (pvz., IRT veiklos nutraukimas energetikos įmonėje dėl kurio nutrūksta elektros tiekimas), pranešti nereikia.

Pagal Direktyvą 2008/114 dėl Europos ypatingos svarbos infrastruktūros objektų nustatymo ir priskyrimo jiems bei būtinybės gerinti jų apsaugą vertinimo, „Europos programoje dėl ypatingos svarbos infrastruktūros objektų apsaugos (EPCIP)“[18] nustatytas bendras visapusiškas požiūris į ypatingos svarbos infrastruktūros apsaugą Europos Sąjungoje. EPCIP tikslai visiškai atitinka šį pasiūlymą ir direktyva turėtų būti taikoma nepažeidžiant Direktyvos 2008/114. EPCIP neįpareigoja operatorių pranešti apie svarbius saugumo pažeidimus ir nenumato valstybių narių bendradarbiavimo ir reagavimo į incidentus mechanizmų.

Teisėkūros institucijos šiuo metu svarsto Komisijos direktyvos dėl atakų prieš informacines sistemas[19] pasiūlymą, kuriuo siekiama suderinti tam tikro tipo elgesio kriminalizavimą. Jis taikomas tik tam tikro tipo elgesio kriminalizavimui; juo nesprendžiami TIS rizikos ir incidentų prevencijos, atsakomųjų veiksmų į TIS incidentus ir jų poveikio mažinimo klausimai. Ši direktyva turėtų būti taikoma nepažeidžiant Direktyvos dėl atakų prieš informacines sistemas.

2012 m. kovo 28 d. Komisija priėmė komunikatą dėl Europos kovos su elektroniniu nusikalstamumu centro kūrimo (EC3)[20]. Šis centras, įkurtas 2013 m. sausio 11 d., yra Europos policijos biuro (Europolo) dalis ir pagrindinis kovos su elektroniniais nusikaltimais centras

---

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

13 COM(2010) 521.

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

15 Pagrindų direktyvos 13a ir 13b straipsniai.

16 2002 m. liepos 12 d. Direktyva 2002/58.

17 COM(2012) 11.

18 COM(2006) 786 http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0786en01.pdf.

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

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

Europos Sąjungoje. EC3 paskirtis yra sutelkti Europos patirtį elektroninių nusikaltimų srityje, siekiant paremti valstybių narių gebėjimų stiprinimą, teikti paramą valstybėms narėms tiriant elektroninius nusikaltimus ir bendradarbiaujant su Eurojustu tapti subjektu, išreiškiančiu Europos elektroninių nusikaltimų tyrėjų, dirbančių teisėsaugos ir teisminėse institucijose, požiūrį.

Europos institucijos, agentūros ir įstaigos sudarė savo kompiuterinių incidentų tyrimo tarnybą, vadinamą ES CERT.

Tarptautiniu mastu ES užsiima kibernetinio saugumo klausimais tiek dvišaliu, tiek daugiašaliu lygmeniu. 2010 m. EU ir JAV aukščiausio lygio susitikime[21] buvo įsteigta ES ir JAV kibernetinio saugumo ir kovos su elektroniniais nusikaltimais darbo grupė. ES taip pat aktyviai dalyvauja kituose daugiašaliuose forumuose, kaip antai Ekonominio bendradarbiavimo ir plėtros organizacijoje (EBPO), Jungtinių Tautų Generalinėje Asamblėjoje (JTGA), Tarptautinėje telekomunikacijų sąjungoje (ITU), Europos saugumo ir bendradarbiavimo organizacijoje (ESBO), pasaulio aukščiausiojo lygio susitikime informacinės visuomenės klausimais (WSIS) ir interneto valdymo forume (IVF).

2. KONSULTACIJŲ SU SUINTERESUOTOSIOMIS ŠALIMIS IR POVEIKIO VERTINIMO REZULTATAI

2.1. Konsultacijos su suinteresuotosiomis šalimis ir tiriamųjų duomenų naudojimas

Viešos konsultacijos dėl TIS didinimo ES vyko internetu nuo 2012 m. liepos 23 d. iki spalio 15 d. Komisija iš viso gavo 160 atsakymų į interneto klausimyną.

Pagrindinis rezultatas buvo tas, kad suinteresuotosios šalys parodė iš esmės remiančios bendrą poreikį didinti TIS visoje ES. Be kita ko,: 82,8 % respondentų išreiškė nuomonę, kad ES vyriausybės turėtų daryti daugiau, kad užtikrintų aukštą TIS lygį; 82,8 % laikėsi nuomonės, kad informacijos ir sistemų vartotojai nežino apie TIS grėsmes ir incidentus; 66,3 % iš principo pritartų tam, kad būtų įvestas norminis reikalavimas valdyti TIS riziką, o 84,8 % sakė, kad tokie reikalavimai turėtų būti nustatyti ES lygmeniu. Daugelis respondentų mano, kad visų pirma svarbu priimti TIS reikalavimus šiuose sektoriuose: bankininkystės ir finansų (91,1 %), energetikos (89,4 %), transporto (81,7 %), sveikatos priežiūros (89,4%), interneto paslaugų (89,1%) ir viešojo administravimo (87,5%). Respondentai taip pat mano, kad jeigu būtų įvestas reikalavimas pranešti nacionalinei kompetentingai institucijai apie TIS pažeidimus, jis turėtų būti nustatytas ES lygmeniu (65,1%), ir patvirtino, kad jis taip pat turėtų būti taikomas viešojo administravimo institucijoms (93,5%). Galiausiai, respondentai patvirtino, kad reikalavimas įgyvendinti TIS rizikos valdymą, atitinkantį šiuolaikinį technikos išsivystymo lygį, jiems nesudarytų labai didelių papildomų išlaidų (63,4%) kaip ir reikalavimas pranešti apie saugumo pažeidimus (72,3%).

Su valstybėmis narėmis buvo konsultuojamasi įvairios sudėties Taryboje, valstybių narių Europos forume (EFMS), 2012 m. liepos 6 d. Komisijos ir Europos išorės veiksmų tarnybos surengtoje konferencijoje kibernetinio saugumo klausimais ir specialiuose dvišaliuose susitikimuose, surengtuose atskirų valstybių narių prašymu.

Aptarimai su privačiuoju sektoriumi taip pat buvo surengti įgyvendinant Europos viešojo ir privačiojo sektorių partnerystę atsparumui užtikrinti[22] ir dvišaliuose susitikimuose. Kalbant apie viešąjį sektorių, Komisija ES institucijoms surengė aptarimus su ENISA ir CERT.

---

21 http://europa.eu/rapid/press-release_SPEECH-10-597_lt.htm.

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

2.2. Poveikio vertinimas

Komisija atliko trijų politikos variantų poveikio vertinimą:

1 variantas. Įprasta veikla (bazinis scenarijus): toliau laikomasi dabartinio požiūrio;

2 variantas. Reguliavimo variantas, kurį sudaro teisės akto, kuriuo įkuriama bendra ES teisinė sistema, skirta TIS atsižvelgiant į valstybių narių gebėjimus, bendradarbiavimo ES lygmeniu mechanizmai ir pagrindiniams privačiojo sektoriaus rinkos dalyviams ir viešojo administravimo institucijoms taikomi reikalavimai, pasiūlymas;

3 variantas. Mišrusis variantas, pagal kurį savanoriškos iniciatyvos, susijusios su valstybių narių TIS gebėjimais ir bendradarbiavimo ES lygmeniu mechanizmais, derinamos su pagrindiniams privačiojo sektoriaus rinkos dalyviams ir viešojo administravimo institucijoms taikomais teisės aktų reikalavimais.

Komisija nusprendė, kad 2 variantas turėtų didžiausią teigiamą poveikį, nes būtų gerokai sustiprinta ES vartotojų, įmonių ir vyriausybių apsauga nuo TIS incidentų. Visų pirma, valstybėms narėms nustatyti įpareigojimai užtikrintų deramą parengtį nacionaliniu lygmeniu ir sustiprintų abipusį pasitikėjimą, kuris yra būtina veiksmingo bendradarbiavimo ES lygmeniu sąlyga. Sukūrus bendradarbiavimo ES lygmeniu mechanizmus pasinaudojant tinklu būtų užtikrinta nuosekli ir koordinuota apsauga ir atsakomieji veiksmai į tarpvalstybinius TIS incidentus ir riziką. Nustačius viešojo administravimo institucijoms ir pagrindiniams privačiojo sektoriaus rinkos dalyviams taikytinus reikalavimus įgyvendinti TIS rizikos valdymą, būtų sukurtos stiprios paskatos veiksmingai valdyti saugumo riziką. Įpareigojimas pranešti apie didelį poveikį turinčius TIS incidentus sustiprintų gebėjimą reaguoti į incidentus ir puoselėtų skaidrumą. Be to, įvedusi tvarką savo viduje, ES galėtų išplėsti veiklą tarptautiniu mastu ir tapti dar patikimesne bendradarbiavimo dvišaliu ir daugiašaliu lygmenimis partnere. Taip ES turėtų dar daugiau galimybių skatinti pagrindines teises ir pagrindines ES vertybes užsienyje.

Kiekybinis įvertinimas parodė, kad pasirinkus 2 variantą valstybėms narėms netektų prisiimti neproporcingai didelės naštos. Privačiojo sektoriaus išlaidos taip pat būtų ribotos, nes daugelis ūkio subjektų jau dabar privalo laikytis galiojančių saugumo reikalavimų (visų pirma įpareigojimo duomenų valdytojams imtis techninių ir organizacinių priemonių siekiant apsaugoti asmens duomenis, įskaitant TIS priemones). Taip pat buvo atsižvelgta į dabartines privačiojo sektoriaus išlaidas saugumui.

Šis pasiūlymas parengtas laikantis Europos Sąjungos pagrindinių teisių chartijoje pripažintų principų, visų pirma, teisės į tai, kad būtų gerbiamas privatus gyvenimas ir bendravimas, asmens duomenų apsaugos, laisvės užsiimti verslu, teisės į nuosavybę, teisės į veiksmingą teisės gynimo priemonę, kuria galima būtų naudotis teisme, ir teisės būti išklausytam. Ši direktyva turi būti įgyvendinta atsižvelgiant į tokias teises ir principus.

3. TEISINIAI PASIŪLYMO ASPEKTAI

3.1. Teisinis pagrindas

Europos Sąjunga turi teisę priimti priemones, kurių tikslas – sukurti vidaus rinką arba užtikrinti jos veikimą laikantis atitinkamų sutarčių nuostatų (Sutarties dėl Europos Sąjungos veikimo (SESV) 26 straipsnis). Pagal SESV 114 straipsnį ES gali priimti „priemones valstybių narių įstatymų ir kitų teisės aktų nuostatoms, skirtoms vidaus rinkos sukūrimui ar veikimui, suderinti“.

Kaip minėta pirmiau, tinklų ir informacinės sistemos atlieka esminį vaidmenį skatinant tarpvalstybinį prekių, paslaugų ir asmenų judėjimą. Jie dažnai būna susiję tarpusavyje, o

internetas iš esmės yra visuotinis. Turint omenyje šioms sistemoms būdingą tarptautinį pobūdį, sutrikimas vienoje valstybėje narėje gali turėti poveikio kitoms valstybėms narėms ir visai ES. Todėl tinklų ir informacinių sistemų atsparumas ir stabilumas yra būtinas sklandžiam vidaus rinkos veikimui užtikrinti.

ES teisės aktų leidėjas jau pripažino poreikį suderinti TIS taisykles, kad būtų užtikrinta vidaus rinkos plėtra. Visų pirma, toks buvo SESV 114 straipsniu grindžiamo Reglamento 460/2004, įsteigiančio Europos tinklų ir informacijos apsaugos agentūrą[23], tikslas.

Dėl skirtumų, kurių susidarė dėl nevienodų valstybių narių nacionalinių gebėjimų, politikos ir apsaugos lygio TIS srityje, atsirado kliūčių vidaus rinkai ir pagrindas ES imtis veiksmų.

3.2. Subsidiarumas

Europos įsikišimas TIS srityje yra grindžiamas subsidiarumo principu.

Pirma, turint omenyje tarpvalstybinį TIS pobūdį, ES nesikišimo atveju susidarytų situacija, kai kiekviena valstybė narė veiktų pavieniui, neatsižvelgdama į ES tinklų ir informacinių sistemų tarpusavio priklausomybę. Tinkamas valstybių narių bendradarbiavimo lygis leistų užtikrinti, kad TIS rizika būtų gerai valdoma tarpvalstybiniu lygmeniu, kuriuo ji kyla. TIS taisyklių skirtumai trukdo įmonėms, norinčioms vykdyti veiklą keliose šalyse ir neleidžia pasiekti visuotinės masto ekonomijos.

Antra, norint sudaryti vienodas veiklos sąlygas ir pašalinti teisės aktų spragas, reikalingi ES lygmens reguliavimo įpareigojimai. Dėl išskirtinai savanoriško požiūrio bendradarbiavimas vyksta tik tarp mažumos valstybių narių, kurių pajėgumai yra dideli. Siekiant įtraukti visas valstybes nares, būtina užtikrinti, kad jos visos turėtų reikalaujamą minimalų pajėgumų lygį. Vyriausybių priimtos TIS priemonės turi derėti tarpusavyje ir būti koordinuojamos siekiant suvaldyti ir kiek įmanoma sumažinti TIS incidentų pasekmes. Pasikeisdamos gerąja patirtimi ir nuolat įtraukdamos ENISA, kompetentingos institucijos ir Komisija tinkle bendradarbiaus, kad palengvintų vienodą direktyvos įgyvendinimą visoje ES.Be to, suderinta tinklų ir informacijos saugumo politika gali turėti didelį teigiamą poveikį tam, kad būtų veiksmingai saugomos pagrindinės teisės, ypač teisė į asmens duomenų ir privatumo apsaugą. Todėl veikiant ES lygmeniu būtų padidintas esamos nacionalinės politikos veiksmingumas ir paskatintas jos vystymas.

Siūlomos priemonės taip pat yra pagrįstos proporcingumo požiūriu. Valstybėms narėms nustatyti minimalūs reikalavimai, kad būtų užtikrinta atitinkama parengtis ir sudarytos sąlygos pasitikėjimu grindžiamam bendradarbiavimui. Taip valstybėms narėms suteikiama galimybė deramai atsižvelgti į nacionalinius ypatumus ir užtikrinama, kad bendri ES principai būtų taikomi proporcingai. Tokia plati taikymo sritis suteiks galimybę valstybėms narėms įgyvendinti direktyvą atsižvelgiant į faktinę riziką, kylančią nacionaliniu lygmeniu, kaip nustatyta nacionalinėje TIS strategijoje. Reikalavimai įgyvendinti rizikos valdymo priemones skirti tik ypatingos svarbos ūkio subjektams, o numatytos priemonės atitinka riziką. Viešų konsultacijų metu buvo pabrėžta, kaip svarbu užtikrinti šių ypatingos svarbos ūkio subjektų saugumą. Pranešimo reikalavimai būtų taikomi tik didelio poveikio incidentams. Kaip nurodyta pirmiau, dėl šių priemonių nebūtų patirta neproporcingai didelių išlaidų, nes daugelis šių ūkio subjektų kaip duomenų valdytojai jau dabar pagal galiojančias duomenų apsaugos taisykles privalo užtikrinti asmens duomenų apsaugą.

Siekiant išvengti neproporcingai didelės naštos mažiems operatoriams, visų pirma MVĮ, reikalavimai atitinka riziką, kurią kelia atitinkama tinklų ar informacinė sistema, ir jie

[23] 2004 m. kovo 10 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 460/2004, įsteigiantis Europos tinklų ir informacijos apsaugos agentūrą (OL L 077, 2004 03 13, p. 1).

neturėtų būti taikomi labai mažoms įmonėms. Pirmiausia riziką turi nustatyti ūkio subjektai, kuriems taikomi šie įpareigojimai, ir kurie turės nuspręsti, kokių priemonių imtis, kad tą riziką sumažinti.

Atsižvelgiant į TIS incidentų ir rizikos tarpvalstybinį pobūdį, minėtus tikslus lengviau įgyvendinti ES lygmeniu nei valstybėms narėms pavieniui. Todėl ES gali patvirtinti priemones vadovaudamasi subsidiarumo principu, nustatytu Europos Sąjungos sutarties 5 straipsnyje. Pagal proporcingumo principą siūlomoje direktyvoje nenumatoma nieko, kas nėra būtina siekiant šių tikslų.

Norint pasiekti šių tikslų, Komisijai turėtų būti suteikti įgaliojimai priimti deleguotuosius aktus pagal Sutarties dėl Europos Sąjungos veikimo 290 straipsnį, kad būtų papildytos arba pakeistos tam tikros neesminės pagrindinio teisės akto nuostatos. Komisijos pasiūlymu taip pat siekiama, kad proporcingumo procesas būtų taikomas privatiesiems ir vešiesiems operatoriams įgyvendinant savo įsipareigojimus.

Siekiant užtikrinti vienodas pagrindinio teisės akto įgyvendinimo sąlygas, Komisija turėtų būti įgaliota priimti įgyvendinimo teisės aktus pagal Sutarties dėl Europos Sąjungos veikimo 291 straipsnį.

Visų pirma atsižvelgiant į plačią siūlomos direktyvos taikymo sritį, į tai, kad ji susijusi su griežtai reglamentuojamomis sritimis, ir į teisinius įpareigojimus, numatytus jos IV skyriuje, prie pranešimo apie perkėlimo į nacionalinę teisę priemones turėtų būti pridėti aiškinamieji dokumentai. Pagal 2011 m. rugsėjo 28 d. valstybių narių ir Komisijos bendrą politinį pareiškimą dėl aiškinamųjų dokumentų valstybės narės įsipareigojo pagrįstais atvejais prie pranešimų apie savo perkėlimo į nacionalinę teisę priemones pridėti vieną ar daugiau dokumentų, kuriuose paaiškinamas direktyvos nuostatų ir nacionalinių perkėlimo priemonių atitinkamų dalių tarpusavio ryšys. Šios direktyvos atveju teisės aktų leidėjas laikosi nuomonės, kad tokių dokumentų perdavimas yra pagrįstas.

4. POVEIKIS BIUDŽETUI

Valstybių narių bendradarbiavimas ir keitimasis informacija turi būti paremtas saugia infrastruktūra. Pasiūlymas turės poveikio ES biudžetui tik jei valstybės narės nuspręs pritaikyti esamą infrastruktūrą (pvz., sTESTA) ir paves Komisijai tai įgyvendinti pagal 2014–2020 m. DFP. Numatoma, kad vienkartinės išlaidos sudarys 1 250 000 EUR ir kad jos bus apmokėtos iš ES biudžeto, biudžeto eilutė 09.03.02 (skatinti nacionalinių internetu teikiamų viešųjų paslaugų sujungimą ir sąveiką bei prieigą prie tokių tinklų – 09.03 skyrius, Europos infrastruktūros tinklų priemonė – ryšių tinklai), su sąlyga, kad bus pakankamai lėšų pagal EITP. Kita galimybė – valstybėms narėms pasidalinti vienkartines esamos infrastruktūros pritaikymo išlaidas arba nuspręsti kurti naują infrastruktūrą ir prisiimti išlaidas, kurios turėtų sudaryti maždaug 10 mln. EUR per metus.

2013/0027 (COD)

Pasiūlymas

EUROPOS PARLAMENTO IR TARYBOS DIREKTYVA

dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti

EUROPOS PARLAMENTAS IR EUROPOS SĄJUNGOS TARYBA,

atsižvelgdami į Sutartį dėl Europos Sąjungos veikimo, ypač į jos 114 straipsnį,

atsižvelgdami į Europos Komisijos pasiūlymą,

perdavus teisėkūros procedūra priimamo akto projektą nacionaliniams parlamentams,

atsižvelgdami į Europos ekonomikos ir socialinių reikalų komiteto nuomonę[1],

pasikonsultavę su Europos duomenų apsaugos priežiūros pareigūnu,

taikydami įprastą teisėkūros procedūrą,

kadangi:

(1) tinklų ir informacinėms sistemoms ir paslaugoms tenka gyvybiškai svarbus vaidmuo visuomenėje. Jų patikimumas ir saugumas yra labai svarbūs ekonominei veiklai bei socialinei gerovei ir, visų pirma, vidaus rinkos veikimui;

(2) tyčinių ir atsitiktinių saugumo incidentų mastas ir dažnumas didėja ir kelia didelę grėsmę tinklų ir informacinių sistemų veikimui. Tokie incidentai gali trukdyti vykdyti ekonominę veiklą, sukelti didelių finansinių nuostolių, pakirsti naudotojų pasitikėjimą ir padaryti didelę žalą Sąjungos ekonomikai;

(3) kaip komunikacijos priemonė be sienų, skaitmeninės informacinės sistemos ir, visų pirma, internetas vaidina labai svarbų vaidmenį skatinant tarpvalstybinį prekių, paslaugų ir asmenų judėjimą. Dėl tokio tarpvalstybinio pobūdžio didelis šių sistemų sutrikimas vienoje valstybėje narėje gali turėti neigiamo poveikio kitoms valstybėms narėms ir visai Sąjungai. Todėl tinklų ir informacinių sistemų atsparumas ir stabilumas yra būtinas, kad vidaus rinka veiktų sklandžiai;

(4) reikėtų Sąjungos lygmeniu sukurti bendradarbiavimo mechanizmą, kad būtų galima keistis informacija ir koordinuotai nustatyti tinklų ir informacijos saugumo (TIS) problemas ir imtis atsakomųjų veiksmų. Kad toks mechanizmas būtų veiksmingas ir visaapimantis, visos valstybės narės turėtų turėti minimalių pajėgumų ir strategiją, užtikrinančią aukštą TIS lygį jų teritorijoje. Siekiant skatinti rizikos valdymo kultūrą ir užtikrinti, kad būtų pranešama apie pačius didžiausius incidentus, minimalūs saugumo reikalavimai taip pat turėtų būti taikomi viešojo administravimo institucijoms ir ypatingos svarbos informacinės infrastruktūros operatoriams;

(5) siekiant aprėpti visus reikšmingus incidentus ir rizikos rūšis, ši direktyva turėtų būti taikoma visoms tinklų ir informacinėms sistemoms. Tačiau viešojo administravimo institucijoms ir rinkos dalyviams taikomi įpareigojimai neturėtų būti taikomi nei

[1] OL C […], […], p. […].

įmonėms, teikiančioms viešųjų ryšių tinklų arba viešai prieinamas elektroninių ryšių paslaugas, apibrėžtas 2002 m. kovo 7 d. Europos Parlamento ir Tarybos direktyvoje 2002/21/EB 2002 dėl elektroninių ryšių tinklų ir paslaugų bendrosios reguliavimo sistemos (Pagrindų direktyva)[2], kurioms taikomi specifiniai saugumo ir vientisumo reikalavimai, nustatyti tos direktyvos 13a straipsnyje, nei patikimumo užtikrinimo paslaugų teikėjams;

(6) esamų pajėgumų nepakanka, kad būtų galima užtikrinti aukštą TIS lygį Sąjungoje. Valstybių narių parengties lygis yra labai skirtingas, todėl visoje ES susiformavo skirtingi požiūriai. Dėl to vartotojų ir verslo įmonių apsaugos lygis yra nevienodas, o tai kenkia bendram Sąjungos TIS lygiui. Tai, kad nėra nustatyta bendrų minimalių reikalavimų viešojo administravimo institucijoms ir rinkos dalyviams, savo ruožtu neleidžia sukurti visuotinio veiksmingo bendradarbiavimo Sąjungos lygmeniu mechanizmo;

(7) todėl norint veiksmingai spręsti tinklų ir informacinių sistemų saugumo problemas, reikalingas visuotinis požiūris Sąjungos lygmeniu, apimantis bendrus minimalius pajėgumų stiprinimo ir planavimo reikalavimus, keitimąsi informacija bei veiksmų koordinavimą ir bendrus visiems atitinkamiems rinkos dalyviams ir viešojo administravimo institucijoms taikytinus minimalius saugumo reikalavimus;

(8) šios direktyvos nuostatos neturėtų trukdyti kiekvienai valstybei narei imtis reikalingų priemonių savo pagrindiniams saugumo interesams ir viešajai politikai apsaugoti ir visuomenės saugumui užtikrinti ir turėtų leisti atskleisti ir tirti kriminalinius nusikaltimus ir už juos traukti baudžiamojon atsakomybėm. Pagal SESV 346 straipsnį jokia valstybė narė neprivalo teikti informacijos, kurios atskleidimas, jos nuomone, prieštarauja gyvybiniams jos saugumo interesams;

(9) kad būtų pasiektas ir išlaikytas bendras aukštas tinklų ir informacinių sistemų saugumo lygis, kiekviena valstybė narė turėtų turėti nacionalinę TIS strategiją, kurioje būtų apibrėžti strateginiai tikslai ir konkretūs politikos veiksmai, kuriuos reikia įgyvendinti. Nacionaliniu lygmeniu turi būti parengti pagrindinius reikalavimus atitinkantys TIS bendradarbiavimo planai, kad būtų pasiektas toks pajėgumų parengties lygis, kad incidentų atveju būtų efektyviai ir veiksmingai bendradarbiaujama nacionaliniu ir Sąjungos lygmeniu;

(10) siekiant sudaryti sąlygas veiksmingai įgyvendinti pagal šią direktyvą priimtas nuostatas, kiekvienoje valstybėje narėje turėtų būti įsteigta arba paskirta institucija, atsakinga už TIS klausimų koordinavimą, kuri būtų pagrindinis tarpvalstybinio bendradarbiavimo Sąjungos lygmeniu centras. Šioms institucijoms turėtų būti skirta pakankamai techninių, finansinių ir žmogiškųjų išteklių, siekiant užtikrinti, kad jos galėtų efektyviai ir veiksmingai vykdyti joms pavestas užduotis ir taip įgyvendinti šios direktyvos tikslus;

(11) visos valstybės narės turėtų būti tinkamai pasirengusios – turėti tiek techninių, tiek organizacinių pajėgumų, kad galėtų užkirsti kelią tinklų ir informacinių sistemų incidentams bei rizikai, juos nustatyti, sušvelninti arba imtis atsakomųjų veiksmų. Todėl siekiant garantuoti efektyvius ir suderinamus pajėgumus incidentams spręsti bei rizikai šalinti, taip pat siekiant užtikrinti veiksmingą bendradarbiavimą Sąjungos lygmeniu, visose valstybėse narėse turėtų būti įkurtos pagrindinius reikalavimus atitinkančios gerai veikiančios kompiuterinių incidentų tyrimo tarnybos;

---

[2] OL L 108, 2002 4 24, p. 33.

(12) pasinaudodamos reikšminga pažanga, padaryta valstybių narių Europos forume (EFMS) skatinant diskusijas ir keitimąsi gerąja politikos patirtimi, įskaitant Europos bendradarbiavimo kibernetinių krizių atveju principų parengimą, valstybės narės ir Komisija turėtų sukurti tinklą, kuris suteiktų galimybę joms nuolat bendrauti ir paremtų jų bendradarbiavimą. Toks saugus ir efektyvus bendradarbiavimo mechanizmas turėtų sudaryti sąlygas struktūrizuotai ir koordinuotai keistis informacija, nustatyti incidentus ir imtis atsakomųjų veiksmų Sąjungos lygmeniu;

(13) Siekdama padėti valstybėms narėms ir Komisijai, Europos tinklų ir informacijos apsaugos agentūra (ENISA) turėtų dalytis savo žiniomis, konsultuoti ir palengvinti keitimąsi gerąja patirtimi. Taikydama šią direktyvą Komisija visų pirma turėtų tartis su ENISA. Siekiant užtikrinti, kad informacija veiksmingai ir laiku būtų perduodama valstybėms narėms ir Komisijai, išankstiniai perspėjimai apie incidentus ir riziką turėtų būti perduodami bendradarbiavimo tinkle. Siekiant gerinti pajėgumus ir žinias valstybėse narėse, bendradarbiavimo tinklas taip pat turėtų būti keitimosi gerąja patirtimi priemonė, padedanti jo nariams stiprinti pajėgumus, vadovauti organizuojant tarpusavio vertinimus ir TIS pratybas;

(14) turėtų būti sukurta saugi dalijimosi informacija infrastruktūra, kuri sudarytų sąlygas bendradarbiavimo tinkle keistis slapta ir konfidencialia informacija. Neapribojant jų įpareigojimo pranešti apie Sąjungos masto incidentus ir riziką bendradarbiavimo tinklui, prieiga prie kitų valstybių narių konfidencialios informacijos valstybėms narėms turėtų būti suteikta tik jei jos įrodo, kad jų techniniai, finansiniai ir žmoniškieji ištekliai bei procesai ir jų ryšių infrastruktūra leidžia užtikrinti efektyvų, veiksmingą ir saugų jų dalyvavimą tinkle;

(15) kadangi daugumą tinklų ir informacinių sistemų valdo privatūs operatoriai, labai svarbus viešojo ir privačiojo sektorių bendradarbiavimas. Rinkos dalyviai turėtų būti skatinami taikyti savo neformalius bendradarbiavimo mechanizmus, kad užtikrintų TIS. Jie taip pat turėtų bendradarbiauti su viešuoju sektoriumi ir dalintis informacija ir gerąja patirtimi mainais į operatyvinę paramą incidentų atveju;

(16) siekdamos užtikrinti skaidrumą ir tinkamai informuoti ES piliečius bei rinkos dalyvius, kompetentingos institucijos turėtų sukurti bendrą interneto svetainę, kurioje būtų skelbiama nekonfidenciali informacija apie incidentus ir riziką;

(17) kai pagal Sąjungos ir nacionalines verslo konfidencialumo taisykles informacija laikoma konfidencialia, toks konfidencialumas turėtų būti užtikrintas vykdant šioje direktyvoje numatytą veiklą ir įgyvendinant jos tikslus;

(18) remdamosi visų pirma nacionalinių krizių valdymo patirtimi ir bendradarbiaudamos su ENISA, Komisija ir valstybės narės turėtų parengti Sąjungos TIS bendradarbiavimo planą, kuriame būtų nustatyti kovos su rizika ir incidentais bendradarbiavimo mechanizmai. Į šį planą turėtų būti deramai atsižvelgiama taikant išankstinio perspėjimo sistemą bendradarbiavimo tinkle;

(19) pranešimo apie išankstinį perspėjimą tinkle turėtų būti reikalaujama tik kai incidento arba atitinkamos rizikos mastas ir galimas poveikis yra arba gali tapti tokie dideli, kad informavimas ir atsakomųjų veiksmų koordinavimas Europos lygmeniu būtų būtini. Todėl išankstiniai perspėjimai turėtų būti teikiami tik įvykus incidentui arba susidarius rizikai, kurie sparčiai didėja, viršija nacionalinius atsakomųjų veiksmų pajėgumus arba turi poveikio daugiau negu vienai valstybei narei, arba jei yra tokių incidentų ar rizikos tikimybė. Siekiant sudaryti sąlygas tinkamam įvertinimui, visa informacija, kuri yra svarbi vertinant riziką arba incidentą, turėtų būti perduota į bendradarbiavimo tinklą;

(20) gavusios išankstinį perspėjimą ir jo įvertinimą, kompetentingos institucijos turėtų susitarti dėl koordinuotų atsakomųjų veiksmų pagal Sąjungos TIS bendradarbiavimo planą. Kompetentingos institucijos bei Komisija turėtų būti informuotos apie priemones, kurių imtasi nacionaliniu lygmeniu atsižvelgiant į atsakomuosius veiksmus;

(21) turint omenyje visuotinį TIS problemų pobūdį, reikalingas glaudesnis tarptautinis bendradarbiavimas, kuris leistų pagerinti saugumo standartus ir keitimąsi informacija, skatinti bendrą visuotinį požiūrį į TIS problemas;

(22) atsakomybė už TIS užtikrinimą visų pirma tenka viešojo administravimo institucijoms ir rinkos dalyviams. Rizikos valdymo kultūra, apimanti rizikos įvertinimą ir esamą riziką atitinkančių saugumo priemonių įgyvendinimą, turėtų būti skatinama ir plėtojama taikant atitinkamus teisės aktų reikalavimus ir savanorišką pramonės praktiką. Kad bendradarbiavimo tinklas, kuriuo užtikrinamas efektyvus visų valstybių narių bendradarbiavimas, efektyviai veiktų, būtina sudaryti vienodas veiklos sąlygas;

(23) Direktyvoje 2002/21/EB reikalaujama, kad įmonės, teikiančios viešųjų elektroninių ryšių tinklų arba viešai prieinamas elektroninių ryšių paslaugas, imtųsi atitinkamų priemonių, kad apsaugotų savo saugumą ir vientisumą, ir nustatomas reikalavimas pranešti apie saugumo pažeidimą ir vientisumo praradimą. 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyvoje 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių)[3] reikalaujama, kad viešai prieinamų elektroninių ryšių paslaugų teikėjas imtųsi atitinkamų techninių ir organizacinių priemonių, kad išlaikytų savo paslaugų saugumą;

(24) tokie įpareigojimai turėtų būti taikomi ne tik elektroninių ryšių sektoriui, bet ir svarbiausiems informacinės visuomenės paslaugų teikėjams, kaip apibrėžta 1998 m. birželio 22 d. Europos Parlamento ir Tarybos direktyvoje 98/34/EB nustatančioje informacijos apie techninius standartus ir reglamentus ir informacinės visuomenės paslaugų taisykles teikimo tvarką[4], kuriomis grindžiamos vartotojams skirtos informacinės visuomenės paslaugos ar internetinė veikla, kaip antai e. prekybos platformas, mokėjimo internetu tinklų sąsajas, socialinius tinklus, paieškos sistemas, nuotolinių kompiuterinių išteklių paslaugas, programų parduotuves. Šių svarių informacinės visuomenės paslaugų sutrikimas neleistų teikti kitų informacinės visuomenės paslaugų, kurioms jos yra labai svarbios. Programinės įrangos kūrėjai ir kompiuterinės technikos gamintojai nėra informacinės visuomenės paslaugų teikėjai, todėl jiems šie įpareigojimai netaikomi. Šie įpareigojimai taip pat turėtų būti taikomi viešojo administravimo institucijoms ir operatoriams ypatingos svarbos infrastruktūros, kuri labai priklauso nuo informacinių ir ryšių technologijų ir yra labai svarbi gyvybinėms ekonominėms ir visuomeninėms funkcijoms palaikyti, kaip antai elektros ir dujų, transporto, kredito įstaigų, biržų ir sveikatos. Tokių tinklų ir informacinių sistemų veiklos sutrikimas turėtų neigiamo poveikio vidaus rinkai;

(25) taikant viešojo administravimo institucijoms ir rinkos dalyviams nustatytas technines ir organizacines priemones neturėtų būti reikalaujama, kad tam tikru būdu būtų sukurtas, suprojektuotas ir pagamintas konkretus komercinis informacinių ir ryšių technologijų produktas;

---

[3] OL L 201, 2002 7 31, p. 37.

[4] OL L 204, 1998 7 21, p. 37.

(26) viešojo administravimo institucijos ir rinkos dalyviai turėtų užtikrinti jų kontroliuojamų tinklų ir sistemų saugumą. Tai visų pirma būtų privatūs tinklai ir sistemos, kurias valdo jų vidaus IT personalas arba kurių saugumas užtikrinamas perkant paslaugas iš šalies. Saugumo ir pranešimų teikimo įpareigojimai turėtų būti taikomi atitinkamiems rinkos dalyviams ir viešojo administravimo institucijoms, nepriklausomai nuo to, ar jie vykdo savo tinklų ir informacinių sistemų priežiūrą patys, ar perka šias paslaugas iš šalies;

(27) siekiant išvengti neproporcingai didelės finansinės ir administracinės naštos mažiems operatoriams ir naudotojams, reikalavimai turėtų būti proporcingi rizikai, kurią kelia atitinkama tinklų ar informacinė sistema, atsižvelgiant į tokių priemonių modernumą. Šie reikalavimai neturėtų būti taikomi labai mažoms įmonėms;

(28) kompetentingos institucijos turėtų skirti pakankamai dėmesio neformalių ir patikimų dalijimosi informacija tarp rinkos dalyvių ir tarp viešojo bei privačiojo sektorių kanalų išsaugojimui. Viešinant incidentus, apie kuriuos pranešama kompetentingoms institucijoms, turėtų būti išlaikoma pusiausvyra tarp poreikio visuomenę informuoti apie pavojus ir galimos žalos viešojo administravimo institucijų ir rinkos dalyvių, pranešančių apie incidentus, reputacijai bei komercinei veiklai; Įgyvendindamos įpareigojimus teikti pranešimus, kompetentingos institucijos turėtų atkreipti ypatingą dėmesį į poreikį griežtai užtikrinti, kad informacija apie produkto pažeidžiamumą liktų konfidenciali iki tol, kai bus paskelbtos atitinkamos saugumo priemones.

(29) kompetentingos institucijos turėtų turėti reikiamas priemones jų pareigoms atlikti, įskaitant įgaliojimus gauti pakankamai informacijos iš rinkos dalyvių ir viešojo administravimo institucijų, kad galėtų įvertinti tinklų ir informacinių sistemų saugumo lygį, taip pat patikimus ir išsamius duomenis apie įvykusius incidentus, kurie turėjo poveikio tinklų ir informacinių sistemų veikimui;

(30) daugeliu atvejų incidentas yra susijęs su kriminaline veika. Kriminalinį incidentų pobūdį galima įtarti netgi tuomet, kai jį patvirtinantys įrodymai nuo pat pradžių nėra pakankamai aiškūs. Tokioje situacijoje tinkamas kompetentingų institucijų ir teisėsaugos institucijų bendradarbiavimas turėtų būti veiksmingų ir visapusių atsakomųjų veiksmų į saugumo incidentų grėsmę dalis. Siekiant skatinti saugią ir lankstesnę aplinką, teisėsaugos institucijoms visų pirma reikia nuolat pranešti apie incidentus, jei įtariama, kad jie yra sunkaus kriminalinio pobūdžio. Sunkus kriminalinis incidentų pobūdis turėtų būti įvertintas atsižvelgiant į ES teisės aktus elektroninių nusikaltimų srityje;

(31) daugeliu atvejų dėl incidentų kyla pavojus asmens duomenims. Todėl kompetentingos institucijos ir duomenų apsaugos institucijos turėtų bendradarbiauti ir keistis informacija visais su tuo susijusiais klausimais, kad galėtų imtis dėl incidentų įvykusių asmens duomenų pažeidimų nagrinėjimo. Kai saugumo incidentas kartu yra ir asmens duomenų pažeidimas pagal Europos Parlamento ir Tarybos reglamentą dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo[5] valstybės narės įpareigojimą pranešti apie saugumo incidentus vykdo taip, kad administracinė našta būtų minimali. Bendradarbiaudama su kompetentingomis institucijomis ir duomenų apsaugos institucijomis, ENISA galėtų kurti keitimosi informacija mechanizmus bei šablonus; taip būtų išvengta poreikio turėti du pranešimo šablonus. Įvedus tokį vieną bendrą pranešimo šabloną, būtų paprasčiau teikti pranešimus apie incidentus, dėl kurių pažeistas asmens duomenų saugumas, ir sumažėtų verslo įmonių ir viešojo administravimo institucijų administracinė našta;

[5] SEC(2012) 72 *final*.

(32) saugumo reikalavimų standartizavimas yra rinkos principais grindžiamas procesas. Norėdamos užtikrinti vienodą saugumo standartų taikymą, valstybės narės turėtų skatinti nurodytų standartų laikymąsi ar atitiktį, kad Sąjungos mastu būtų užtikrintas aukštas saugumo lygis. Šiuo tikslu gali būti būtina parengti suderintus standartus laikantis 2012 m. spalio 25 d. Europos Parlamento ir Tarybos reglamento (ES) Nr. 1025/2012 dėl Europos standartizacijos, kuriuo iš dalies keičiamos Tarybos direktyvos 89/686/EEB ir 93/15/EEB ir Europos Parlamento ir Tarybos direktyvos 94/9/EB, 94/25/EB, 95/16/EB, 97/23/EB, 98/34/EB, 2004/22/EB, 2007/23/EB, 2009/23/EB ir 2009/105/EB ir panaikinamas Tarybos sprendimas 87/95/EEB ir Europos Parlamento ir Tarybos sprendimas Nr. 1673/2006/EB Tekstas svarbus EEE[6];

(33) Komisija turėtų reguliariai peržiūrėti šią direktyvą, pirmiausia stengdamasi nustatyti, ar reikia ją keisti atsižvelgiant į besikeičiančias technologines ar rinkos sąlygas;

(34) siekiant sudaryti sąlygas bendradarbiavimo tinklui tinkamai veikti, pagal Sutarties dėl Europos Sąjungos veikimo 290 straipsnį Komisijai turėtų būti perduoti įgaliojimai priimti teisės aktus, kuriuose būtų nustatyti kriterijai, kuriuos turi atitikti valstybė narė, kad galėtų dalyvauti saugaus dalijimosi informacija sistemoje, toliau patikslinamos aplinkybės, dėl kurių reikalingas išankstinis perspėjimas, ir nustatomos aplinkybės, kuriomis rinkos dalyviai ir viešojo administravimo institucijos turi pranešti apie incidentus;

(35) ypač svarbu, kad Komisija parengiamųjų darbų metu tinkamai konsultuotųsi, įskaitant konsultacijas ekspertų lygiu. Rengdama ir sudarydama deleguotuosius aktus Komisija turėtų užtikrinti, kad susiję dokumentai būtų vienu metu, laiku ir tinkamai persiųsti Europos Parlamentui ir Tarybai;

(36) siekiant užtikrinti vienodas šios direktyvos įgyvendinimo sąlygas, Komisijai turėtų būti suteikti įgyvendinimo įgaliojimai, susiję su kompetentingų institucijų ir Komisijos bendradarbiavimu bendradarbiavimo tinkle, prieiga prie saugios dalijimosi informacija infrastruktūros, Sąjungos TIS bendradarbiavimo planu, visuomenės informavimui apie incidentus taikomais formatais bei procedūromis ir su TIS susijusiais standartais ir (arba) techninėmis sąlygomis. Tais įgaliojimais turėtų būti naudojamasi laikantis 2011 m. vasario 16 d. Europos Parlamento ir Tarybos reglamento (ES) Nr. 182/2011, kuriuo nustatomos valstybių narių vykdomos Komisijos naudojimosi įgyvendinimo įgaliojimais kontrolės mechanizmų taisyklės ir bendrieji principai[7];

(37) taikydama šią direktyvą Komisija turėtų veikti kartu su atitinkamais sektorių komitetais ir atitinkamomis ES lygmeniu įsteigtomis institucijomis, visų pirma, energetikos, transporto ir sveikatos srityse.

(38) informacija, kurią kompetentinga institucija laiko konfidencialia pagal Sąjungos ir nacionalines verslo konfidencialumo taisykles, turėtų būti keičiamasi su Komisija ir kitomis kompetentingomis institucijomis tik kai toks apsikeitimas yra tikrai būtinas šios direktyvos taikymui. Keičiamasi tik tokia informacija, kuri atitinka keitimosi tikslą ir yra jam svarbi;

(39) dalijantis informacija apie riziką ir incidentus bendradarbiavimo tinkle ir laikantis reikalavimų pranešti nacionalinėms kompetentingoms institucijoms apie incidentus gali tekti tvarkyti asmens duomenis. Toks asmens duomenų tvarkymas yra reikalingas tam, kad būtų įgyvendinti bendro intereso tikslai, kurių siekiama šia direktyva, todėl pagal Direktyvos 95/46/EB 7 straipsnį jis yra teisėtas. Atsižvelgiant į šiuos teisėtus

[6] OL L 316, 2012 11 14, p. 12.
[7] OL L 55, 2011 2 28, p. 13.

tikslus, jis nėra laikomas neproporcingu ir netoleruotinu kišimusi, iš esmės pažeidžiančiu teisę į asmens duomenų apsaugą, garantuojamą Pagrindinių teisių chartijos 8 straipsniu. Taikant šią direktyvą turėtų būti laikomasi 2001 m. gegužės 30 d. Europos Parlamento ir Tarybos reglamento (EB) Nr. 1049/2001 dėl galimybės visuomenei susipažinti su Europos Parlamento, Tarybos ir Komisijos dokumentais[8]. Kai Sąjungos institucijos ir įstaigos tvarko duomenis, toks tvarkymas šios direktyvos įgyvendinimo tikslais turėtų atitikti 2000 m. gruodžio 18 d. Europos Parlamento ir Tarybos reglamentą (EB) Nr. 45/2001 dėl asmenų apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo;

(40) kadangi šios direktyvos tikslo, t. y. užtikrinti aukštą TIS lygį Sąjungoje, valstybės narės negali tinkamai pasiekti pačios ir kadangi dėl veiksmų poveikio jų geriau siekti Sąjungos lygiu, laikydamasi Europos Sąjungos sutarties 5 straipsnyje nustatyto subsidiarumo principo Sąjunga gali patvirtinti priemones. Pagal tame straipsnyje nustatytą proporcingumo principą šia direktyva neviršijama to, kas būtina nurodytiems tikslams pasiekti.

(41) ši Direktyva parengta laikantis Europos Sąjungos pagrindinių teisių chartijoje pripažintų pagrindinių teisių ir principų, visų pirma teisės į tai, kad būtų gerbiamas privatus gyvenimas ir bendravimas, asmens duomenų apsaugos, laisvės užsiimti verslu, teisės į nuosavybę, teisės į veiksmingą teisės gynimo priemonę, kuria galima būtų naudotis teisme ir teisės būti išklausytam. Ši direktyva turi būti įgyvendinta atsižvelgiant į šias teises ir principus,

PRIĖMĖ ŠIĄ DIREKTYVĄ:

I SKYRIUS

BENDROSIOS NUOSTATOS

1 straipsnis

Dalykas ir taikymo sritis

1. Šioje direktyvoje nustatomos priemonės aukštam bendram tinklų ir informacinių sistemų saugumo (toliau – TIS) lygiui visoje Sąjungoje užtikrinti.

2. Šiuo tikslu šia direktyva:

(a) nustatomi įpareigojimai visoms valstybėms narėms, susiję su tinklų ir informacinėms sistemoms poveikio turinčios rizikos ir incidentų prevencija, valdymu ir atsakomaisiais veiksmais;

(b) sukuriamas valstybių narių bendradarbiavimo mechanizmas, skirtas užtikrinti vienodą šios direktyvos taikymą visoje Sąjungoje ir, kai reikia, koordinuotą ir efektyvų tinklų ir informacinėms sistemoms poveikio turinčių rizikos ir incidentų valdymą ir atsakomuosius veiksmus;

(c) nustatomi saugumo reikalavimai rinkos dalyviams ir viešojo administravimo institucijoms.

3. 14 straipsnyje nustatyti saugumo reikalavimai netaikomi nei įmonėms, teikiančioms viešųjų ryšių tinklų arba viešai prieinamas elektroninių ryšių paslaugas, apibrėžtas Direktyvoje 2002/21/EB, kurioms taikomi specifiniai saugumo ir vientisumo

[8] OL L 145, 2001 5 31, p. 43.

reikalavimai, nustatyti tos direktyvos 13a ir 13b straipsniuose, nei patikimumo užtikrinimo paslaugų teikėjams.

4. Šia direktyva nepažeidžiami ES teisės aktai elektroninių nusikaltimų srityje ir 2008 m. gruodžio 8 d. Tarybos direktyva 2008/114/EC dėl Europos ypatingos svarbos infrastruktūros objektų nustatymo ir priskyrimo jiems bei būtinybės gerinti jų apsaugą vertinimo[9]

5. Be to, šia direktyva nepažeidžiama 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva (95/46/EB) dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo[10], 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje ir Europos Parlamento ir Tarybos reglamentas dėl asmenų apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo[11].

6. Dalijantis informacija bendradarbiavimo tinkle pagal III skyrių ir teikiant pranešimus apie TIS incidentus pagal 14 straipsnį, gali reikėti tvarkyti asmens duomenis. Pagal Direktyvos 95/46/EB 7 straipsnį ir Direktyvą 2002/58/EB, kaip perkelta į nacionalinę teisę, valstybė narė suteikia įgaliojimus taip tvarkyti duomenis, kai tai reikalinga, kad būtų įgyvendinti bendro intereso tikslai, kurių siekiama šia direktyva.

2 straipsnis

Minimalus suderinimas

Valstybėms narėms nedraudžiama priimti ir laikytis nuostatų, užtikrinančių aukštesnį saugumo lygį, nepažeidžiant jų įpareigojimų pagal Sąjungos teisės aktus.

3 straipsnis

Apibrėžtys

Šioje direktyvoje vartojamų terminų apibrėžtys:

(1) Tinklų ir informacinė sistema – tai:

(a) elektroninių ryšių tinklas, apibrėžtas Direktyvoje 2002/21/EB ir

(b) bet koks prietaisas arba grupė tarpusavyje sujungtų arba susijusių prietaisų, iš kurių vienas ar daugiau pagal programą automatiškai apdoroja kompiuterinius duomenis, taip pat

(c) kompiuteriniai duomenys, saugomi, tvarkomi, atkuriami arba perduodami a ir b punktuose nurodytomis priemonėmis jų valdymo, naudojimo, apsaugos ir priežiūros tikslais;

(2) saugumas – tai tinklų ir informacinės sistemos pajėgumas tam tikru patikimumo lygiu išlikti atspariai atsitiktiniams ar tyčiniams veiksmams, keliantiems pavojų saugomų ar perduodamų duomenų arba susijusių siūlomų ar per tuos tinklus arba sistemas gaunamų paslaugų prieinamumui, autentiškumui, vientisumui ir slaptumui;

(3) rizika – tai bet kokios aplinkybės ar įvykis, galintys turėti neigiamą poveikį saugumui;

---

[9] OL L 345, 2008 12 23, p. 75.
[10] OL L 281, 1995 11 23, p. 31.
[11] SEC(2012) 72 *final*.

(4) incidentas – tai bet kokios aplinkybės ar įvykis, turintys neigiamą poveikį saugumui;

(5) informacinės visuomenės paslauga – tai paslauga, apibrėžta Direktyvos 98/34/EB 1 straipsnio 2 dalyje;

(6) TIS bendradarbiavimo planas – tai planas, pagal kurį sukuriama organizacinių vaidmenų, atsakomybės pasidalijimo ir procedūrų sistema, skirta tinklų ir informacinių sistemų veiklai palaikyti arba atkurti, kilus rizikai ar įvykus incidentui, turintiems neigiamo poveikio;

(7) incidentų valdymas – visos procedūros, padedančios incidentą ištirti, suvaldyti ir imtis atsakomųjų veiksmų;

(8) rinkos dalyvis – tai:

(a) informacinės visuomenės paslaugų teikėjas, kuris suteikia galimybę teikti kitas informacinės visuomenės paslaugas, kurių neišsamus sąrašas pateikiamas II priede;

(b) ypatingos svarbos infrastruktūra, kuri yra būtina gyvybiškai svarbiai ekonominei ir visuomeninei energetikos, transporto, bankininkystės, biržų ir sveikatos sričių veiklai, kurios neišsamus sąrašas pateikiamas II priede, palaikyti, operatorius.

(9) standartas – tai standartas, apibrėžtas Reglamente (ES) Nr. 1025/2012;

(10) specifikacija – tai specifikacija, nurodyta Reglamente (ES) Nr. 1025/2012;

(11) patikimumo užtikrinimo paslaugų teikėjas – tai fizinis arba juridinis asmuo, teikiantis elektronines paslaugas, kurias sudaro elektroninių parašų, elektroninių spaudų, elektroninių laiko žymų, elektroninių dokumentų, elektroninio pristatymo paslaugų, svetainių tapatumo nustatymo priemonių ir elektroninių sertifikatų, įskaitant elektroninių parašų ir elektroninių spaudų sertifikatu, kūrimas tikrinimas, tvirtinimas, tvarkymas ir saugojimas.

II SKYRIUS

NACIONALINĖS TINKLŲ IR INFORMACIJOS SAUGUMO SISTEMOS

4 straipsnis

Principas

Pagal šią direktyvą valstybės narės savo teritorijoje užtikrina aukštą tinklų ir informacinių sistemų saugumo lygį.

5 straipsnis

Nacionalinė TIS strategija ir nacionalinis TIS bendradarbiavimo planas

1. Kiekviena valstybė narė priima nacionalinę TIS strategiją, kuria nustatomi strateginiai tikslai ir konkrečios politikos ir reguliavimo priemonės, skirtos aukšto lygio tinklų ir informacinių sistemų saugumui pasiekti ir palaikyti. Nacionalinėje TIS strategijoje visų pirma aptariami šie klausimai:

(a) strategijos tikslų ir prioritetų nustatymas remiantis naujausia rizikos ir incidentų analize;

(b) valdymo sistema, skirta strateginiams tikslams ir prioritetams pasiekti, įskaitant aiškų valdžios organų ir kitų svarbių subjektų vaidmenų ir atsakomybės nustatymą;

(c) bendrųjų parengties, atsakomųjų veiksmų ir atkūrimo priemonių, įskaitant viešojo ir privačiojo sektorių bendradarbiavimo mechanizmus, nustatymas;

(d) švietimo, informuotumo didinimo ir mokymo programų nurodymas;

(e) mokslinių tyrimų ir plėtros planai ir aprašymas, kaip šie planai atsispindi nustatytuose prioritetuose.

2. Nacionalinė TIS strategija apima nacionalinį TIS bendradarbiavimo planą, atitinkantį bent jau šiuos reikalavimus:

(a) rizikos įvertinimo planas, skirtas rizikai nustatyti ir galimų incidentų poveikiui įvertinti;

(b) plano įgyvendinime dalyvaujančių subjektų vaidmenų ir atsakomybės nustatymas;

(c) bendradarbiavimo ir ryšių procesų, užtikrinančių incidentų prevenciją, nustatymą, atsakomuosius veiksmus, remontą bei atkūrimą ir sumoduliuotų pagal pavojaus lygį, nustatymas;

(d) TIS pratybų ir mokymo gairės planui sustiprinti, patvirtinti ir išbandyti. Įgyta patirtis registruojama ir įtraukiama į atnaujintą planą.

3. Komisija informuojama apie nacionalinę TIS strategiją ir nacionalinį TIS bendradarbiavimo planą per vieną mėnesį nuo jų priėmimo.

6 straipsnis

Nacionalinė tinklų ir informacinių sistemų saugumo kompetentinga institucija

1. Kiekviena valstybė narė paskiria nacionalinę tinklų ir informacinių sistemų saugumo kompetentingą instituciją („kompetentinga institucija“).

2. Kompetentingos institucijos stebi šios direktyvos taikymą nacionaliniu lygmeniu ir padeda nuosekliai ją taikyti visoje Sąjungoje.

3. Valstybės narės užtikrina, kad kompetentingos institucijos turėtų pakankamai techninių, finansinių ir žmogiškųjų išteklių, kad galėtų efektyviai ir veiksmingai vykdyti joms pavestas užduotis ir taip įgyvendinti šios direktyvos tikslus. Valstybės narės užtikrina efektyvų, veiksmingą ir saugų kompetentingų institucijų bendradarbiavimą 8 straipsnyje nurodytame tinkle.

4. Valstybės narės užtikrina, kad kompetentingos institucijos gautų pranešimus apie incidentus iš viešojo administravimo institucijų ir rinkos dalyvių, kaip nurodyta 14 straipsnio 2 dalyje, ir kad joms būtų suteikti 15 straipsnyje nurodyti įgyvendinimo ir vykdymo užtikrinimo įgaliojimai.

5. Kompetentingos institucijos tariasi ir bendradarbiauja, kai tai aktualu, su atitinkamomis nacionalinėmis teisėtvarkos institucijomis ir duomenų apsaugos institucijomis.

6. Kiekviena valstybė narė nedelsdama praneša Komisijai apie kompetentingos institucijos paskyrimą, jos užduotis ir visus vėlesnius jų pakeitimus. Kiekviena valstybė narė apie kompetentingos institucijos paskyrimą skelbia viešai.

7 straipsnis

Kompiuterinių incidentų tyrimo tarnybos

1. Kiekviena valstybė narė įkuria kompiuterinių incidentų tyrimo tarnybą (toliau – CERT), atsakingą už incidentų ir rizikos valdymą taikant tiksliai nustatytą procesą, kuris atitinka I priedo 1 dalyje nustatytus reikalavimus. CERT gali būti įsteigta pačioje kompetentingoje institucijoje.

2. Valstybės narės užtikrina, kad CERT turėtų pakankamai techninių, finansinių ir žmogiškųjų išteklių, kad galėtų efektyviai vykdyti užduotis, nustatytas I priedo 2 dalyje.

3. Valstybės narės užtikrina, kad nacionaliniu lygmeniu CERT remtųsi saugia ir atsparia ryšių ir informacine infrastruktūra, kuri atitiktų 9 straipsnyje nurodytą saugią dalijimosi informacija sistemą ir būtų su ja sąveiki.

4. Valstybės narės informuoja Komisiją apie kompiuterinių incidentų tyrimo tarnybų išteklius ir įgaliojimus, taip pat apie jų incidentų valdymo procesą.

5. CERT veiklą prižiūri kompetentinga institucija, kuri reguliariai įvertina, ar ji turi pakankamai išteklių, taip pat jos įgaliojimus ir incidentų valdymo proceso efektyvumą.

III SKYRIUS

KOMPETENTINGŲ INSTITUCIJŲ BENDRADARBIAVIMAS

8 straipsnis

Bendradarbiavimo tinklas

1. Kompetentingos institucijos ir Komisija sukuria tinklą (toliau – bendradarbiavimo tinklas), skirtą bendradarbiauti sprendžiant problemas, susijusias su rizika ir incidentais, kurie turi įtakos tinklų ir informacinėms sistemoms.

2. Bendradarbiavimo tinklas užtikrina, kad Komisija ir kompetentingos institucijos nuolat palaikytų ryšius. Gavusi prašymą Europos tinklų ir informacijos apsaugos agentūra (ENISA) padeda bendradarbiavimo tinklui savo žiniomis ir patarimais.

3. Bendradarbiavimo tinkle kompetentingos institucijos:

   (a) skelbia išankstinius perspėjimus apie riziką ir incidentus pagal 10 straipsnį;

   (b) užtikrina koordinuotus atsakomuosius veiksmus pagal 11 straipsnį;

   (c) bendroje svetainėje reguliariai skelbia nekonfidencialią informaciją apie nuolat teikiamus išankstinius perspėjimus ir koordinuotus atsakomuosius veiksmus;

   (d) vienos valstybės narės ar Komisijos prašymu pagal šią direktyvą drauge aptaria ir įvertina vieną ar daugiau nacionalinių TIS strategijų ir nacionalinių TIS bendradarbiavimo planų, nurodytų 5 straipsnyje;

   (e) valstybės narės ar Komisijos prašymu drauge aptaria ir įvertina CERT efektyvumą, ypač kai TIS pratybos vykdomos Sąjungos lygmeniu;

   (f) visais aktualiais klausimais bendradarbiauja ir keičiasi informacija su Europolo Europos kovos su elektroniniu nusikalstamumu centru ir su kitomis susijusiomis Europos įstaigomis, ypač duomenų apsaugos, energetikos, transporto, bankininkystės, vertybinių popierių biržų ir sveikatos srityse;

   (g) keičiasi informacija ir geriausia patirtimi tarpusavyje ir su Komisija ir viena kitai padeda didinti su NIS susijusius gebėjimus;

(h) reguliariai rengia gebėjimų ir pasirengimo tarpusavio vertinimą;

(i) Sąjungos lygmeniu rengia TIS pratybas ir prireikus dalyvauja tarptautinėse TIS pratybose.

4. Komisija įgyvendinimo aktais nustato reikiamą modalumą, siekdama palengvinti kompetentingų institucijų ir Komisijos bendradarbiavimą pagal 2 ir 3 dalis. Tokie įgyvendinimo aktai priimami pagal 19 straipsnio 2 dalyje nurodytą konsultavimosi procedūrą.

9 straipsnis

Saugi dalijimosi informacija sistema

1. Slapta ir konfidencialia informacija bendradarbiavimo tinkle keičiamasi naudojantis saugia infrastruktūra.

2. Komisija įgaliojama pagal 18 straipsnį priimti deleguotuosius aktus, kuriais nustatomi kriterijai, kuriuos turi įvykdyti valstybė narė, kad būtų įgaliota dalyvauti saugioje dalijimosi informacija sistemoje, ir kurie susiję su:

(a) saugia ir atsparia nacionalinio lygmens ryšių ir informacijos infrastruktūra, kuri būtų suderinama ir sąveiki su bendradarbiavimo tinklo saugia infrastruktūra pagal 7 straipsnio 3 dalį; ir

(b) pakankamais jų kompetentingos institucijos ir CERT techniniais, finansiniais ir žmogiškaisiais ištekliais ir procesais, kurie leistų veiksmingai, našiai ir saugiai dalyvauti saugioje dalijimosi informacija sistemoje pagal 6 straipsnio 3 dalį, 7 straipsnio 2 dalį ir 7 straipsnio 3 dalį.

3. Komisija įgyvendinimo aktais priima sprendimus dėl valstybių narių prieigos prie saugios infrastruktūros pagal 2 ir 3 dalyse nurodytus kriterijus. Tokie įgyvendinimo aktai priimami pagal 19 straipsnio 3 dalyje nurodytą nagrinėjimo procedūrą.

10 straipsnis

Išankstiniai perspėjimai

1. Kompetentingos institucijos arba Komisija bendradarbiavimo tinkle pateikia išankstinį perspėjimą apie riziką ir incidentus, kurie atitinka bent vieną iš toliau išvardytų sąlygų:

(a) jų mastas sparčiai auga arba gali išaugti;

(b) į juos atsakyti nacionalinių reagavimo pajėgumų nepakanka arba gali nepakakti;

(c) jie paveikia arba gali paveikti daugiau nei vieną valstybę narę.

2. Išankstinio perspėjimo pranešimuose kompetentingos institucijos ir Komisija perduoda bet kokią turimą informaciją, kuri gali būti naudinga vertinant riziką ar incidentą.

3. Valstybės narės prašymu arba savo iniciatyva Komisija gali pareikalauti, kad valstybė narė pateiktų bet kokią informaciją, susijusią su konkrečia rizika ar incidentu.

4. Jei įtariama, kad rizika ar incidentas, apie kurį būtina pateikti išankstinį perspėjimą, yra nusikalstamo pobūdžio, kompetentingos Komisijos institucijos apie tai informuoja Europolo Europos kovos su elektroniniu nusikalstamumu centrą.

5. Komisija įgaliojama pagal 18 straipsnį priimti deleguotuosius aktus dėl tolesnio rizikos ir incidentų, dėl kurių pagal 1 dalį pateikiamas išankstinis perspėjimas, sąrašo tikslinimo.

11 straipsnis

Koordinuoti atsakomieji veiksmai

1. Gavusi 10 straipsnyje nurodytą išankstinį perspėjimą kompetentinga institucija, įvertinusi aktualią informaciją, susitaria dėl koordinuotų atsakomųjų veiksmų pagal 12 straipsnyje nurodytą Sąjungos TIS bendradarbiavimo planą.

2. Įvairios priemonės, priimtos nacionaliniu lygmeniu remiantis koordinuotais atsakomaisiais veiksmais, yra perduodamos į bendradarbiavimo tinklą.

12 straipsnis

Sąjungos TIS bendradarbiavimo planas

1. Komisija įgaliojama įgyvendinimo aktais priimti Sąjungos TIS bendradarbiavimo planą. Tokie įgyvendinimo aktai priimami pagal 19 straipsnio 3 dalyje nurodytą nagrinėjimo procedūrą.

2. Sąjungos TIS bendradarbiavimo plane numatoma:

   (a) taikant 10 straipsnį:

      – formato ir procedūrų, kuriomis vadovaudamosi kompetentingos institucijos renka ir dalijasi suderinama ir palyginama informacija apie riziką ir incidentus, apibrėžtis,

      – procedūrų ir kriterijų, kuriais vadovaudamasis bendradarbiavimo tinklas vertina riziką ir incidentus, apibrėžtis;

   (b) procesai, kuriais būtina vadovautis norint užtikrinti koordinuotus atsakomuosius veiksmus pagal 11 straipsnį, įskaitant vaidmenų, atsakomybės ir bendradarbiavimo procedūrų nustatymą;

   (c) planui stiprinti, tvirtinti ir išbandyti skirtų TIS pratybų ir mokymo gairės;

   (d) su gebėjimų stiprinimu ir savitarpio mokymusi susijusio žinių perdavimo tarp valstybių narių programa;

   (e) informuotumo didinimo ir mokymo valstybėse narėse programa.

3. Sąjungos TIS bendradarbiavimo planas priimamas ne vėliau kaip praėjus vieneriems metams po šios direktyvos įsigaliojimo ir yra reguliariai persvarstomas.

13 straipsnis

Tarptautinis bendradarbiavimas

Neapribojant bendradarbiavimo tinklo galimybių užtikrinti neformalų tarptautinį bendradarbiavimą, Sąjunga gali sudaryti tarptautinius susitarimus su trečiosiomis šalimis ar tarptautinėmis organizacijomis, pagal kuriuos joms būtų leidžiama dalyvauti tam tikroje bendradarbiavimo tinklo veikloje ir toks dalyvavimas būtų organizuojamas. Tokiame

susitarime atsižvelgiama į poreikį užtikrinti tinkamą bendradarbiavimo tinkle cirkuliuojančių asmens duomenų apsaugą.

IV SKYRIUS

VIEŠOJO ADMINISTRAVIMO INSTITUCIJŲ IR RINKOS DALYVIŲ TINKLŲ IR INFORMACIJOS SISTEMŲ SAUGUMAS

14 straipsnis

Saugumo reikalavimai ir pranešimas apie incidentus

1. Valstybės narės užtikrina, kad viešojo administravimo institucijos ir rinkos dalyviai imtųsi reikiamų techninių ir organizacinių priemonių, kad galėtų valdyti riziką, kylančią tinklų ir informacinių sistemų, kurias jie kontroliuoja ir kuriomis naudojasi savo veikloje, saugumui. Atsižvelgiant į naujausius technikos laimėjimus, šiomis priemonėmis užtikrinamas kilusią riziką atitinkantis saugumo lygis. Visų pirma priemonių imamasi siekiant užkirsti kelią incidentams, kurie paveikia jų tinklų ir informacines sistemas, kiek įmanoma sumažinti jų poveikį ir tuo būdu užtikrinti paslaugų, kurios grindžiamos tokiomis tinklų ir informacinėmis sistemomis, tęstinumą.
2. Valstybės narės užtikrina, kad viešojo administravimo institucijos ir rinkos dalyviai praneštų kompetentingoms institucijoms apie incidentus, kurie turi didelį poveikį pagrindinių jų teikiamų paslaugų saugumui.
3. Reikalavimai pagal 1 ir 2 dalis taikomi visiems rinkos dalyviams, teikiantiems paslaugas Europos Sąjungoje.
4. Kompetentinga institucija gali informuoti visuomenę (arba reikalauti, kad tai darytų viešojo administravimo institucijos ir rinkos dalyviai), kai ji nustato, kad pranešimas apie incidentą atitinka viešuosius interesus. Kartą per metus kompetentinga institucija bendradarbiavimo tinklui pateikia apibendrintą pagal šią dalį gautų pranešimų ir atliktų veiksmų ataskaitą.
5. Komisija yra įgaliojama pagal 18 straipsnį priimti deleguotuosius aktus dėl aplinkybių, kuriomis viešojo administravimo institucijos ir rinkos dalyviai turi pranešti apie incidentus, apibrėžties.
6. Atsižvelgdamos į bet kokius pagal 5 dalį priimtus deleguotuosius aktus kompetentingos institucijos priima gaires ir prireikus pateikia nurodymus dėl aplinkybių, kuriomis viešojo administravimo institucijos ir rinkos dalyviai privalo pranešti apie incidentus.
7. Komisija įgaliojama įgyvendinimo aktais apibrėžti pagal 2 dalį taikytinus formatus ir procedūras. Tokie įgyvendinimo aktai priimami pagal 19 straipsnio 3 dalyje nurodytą nagrinėjimo procedūrą.
8. 1 ir 2 dalys netaikomos labai mažoms įmonėms, mažosioms arba vidutinėms įmonėms, kaip apibrėžta 2003 m. gegužės 6 d. Komisijos rekomendacijoje 2003/361/EB dėl mikroįmonių, mažųjų ir vidutinio dydžio įmonių apibrėžimo[12];

15 straipsnis

Įgyvendinimas ir vykdymo užtikrinimas

[12] OL L 124, 2003 5 20, p. 36.

1. Valstybės narės užtikrina, kad kompetentingos institucijos turėtų visus įgaliojimus, kurių reikia norint nagrinėti atvejus, kai viešojo administravimo institucijos ar rinkos dalyviai nesilaiko savo įsipareigojimų pagal 14 straipsnį, ir tokių atvejų poveikį tinklų ir informacinių sistemų saugumui.

2. Valstybės narės užtikrina, kad kompetentingos institucijos turėtų įgaliojimus reikalauti, kad rinkos dalyviai ir viešojo administravimo institucijos:

   (a) pateiktų informaciją (įskaitant saugumo politikos dokumentus), kuri yra būtina norint įvertinti jų tinklų ir informacinių sistemų saugumą;

   (b) sutiktų, kad kvalifikuota nepriklausoma įstaiga ar nacionalinė institucija atliktų saugumo auditą, ir audito rezultatus pateiktų kompetentingai institucijai.

3. Valstybės narės užtikrina, kad kompetentingos institucijos turėtų įgaliojimus rinkos dalyviams ir viešojo administravimo institucijoms pateikti privalomus nurodymus.

4. Kompetentingos institucijos apie įtariamus kriminalinius nusikaltimus praneša teisėsaugos institucijoms.

5. Kompetentingos institucijos, nagrinėdamos su asmens duomenų saugumo pažeidimu susijusius incidentus, glaudžiai bendradarbiauja su asmens duomenų apsaugos institucijomis.

6. Valstybės narės užtikrinta, kad pagal šį skyrių nustatytiems viešojo administravimo institucijų ir rinkos dalyvių įsipareigojimams gali būti taikoma teisminė kontrolė.

16 straipsnis

Standartizavimas

1. Siekdamos užtikrinti 14 straipsnio 1 dalies vienodą įgyvendinimą, valstybės narės skatina naudotis standartais ir (arba) specifikacijomis, kurios yra svarbios tinklų ir informacijos saugumui.

2. Komisija įgyvendinimo aktais priima 1 dalyje nurodytų standartų sąrašą. Sąrašas skelbiamas *Europos Sąjungos oficialiajame leidinyje*.

V SKYRIUS.

BAIGIAMOSIOS NUOSTATOS

17 straipsnis

Sankcijos

1. Valstybės narės sankcijoms, taikytinoms už nacionalinių nuostatų, priimtų pagal šią direktyvą, pažeidimus nustato taisykles ir imasi visų priemonių, būtinų tų taisyklių taikymui užtikrinti. Sankcijos turi būti veiksmingos, proporcingos ir atgrasančios. Valstybės narės informuoja Komisiją apie tokias nuostatas ne vėliau kaip iki direktyvos perkėlimo į nacionalinę teisę datos ir nedelsdamos praneša jai apie vėlesnius tokių nuostatų pakeitimus.

2. Valstybės narės užtikrinta, kad, kai saugumo incidentas yra susijęs su asmens duomenimis, numatytosios sankcijos atitiktų sankcijas, numatytas Europos

Parlamento ir Tarybos reglamentu dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo[13].

18 straipsnis

Delegavimas

1. Įgaliojimai priimti deleguotuosius aktus Komisijai suteikiami šiame straipsnyje nustatytomis sąlygomis.

2. Komisijai suteikiami 9 straipsnio 2 dalyje, 10 straipsnio 5 dalyje ir 14 straipsnio 5 dalyje nurodyti įgaliojimai priimti deleguotuosius aktus. Komisija parengia ataskaitą dėl įgaliojimų suteikimo likus ne mažiau kaip devyniems mėnesiams iki penkerių metų laikotarpio pabaigos. Įgaliojimų suteikimas automatiškai pratęsiamas tokios pačios trukmės laikotarpiams, išskyrus atvejus, kai Europos Parlamentas arba Taryba pareiškia prieštaravimų dėl tokio pratęsimo likus ne mažiau kaip trims mėnesiams iki kiekvieno tokio laikotarpio pabaigos.

3. Europos Parlamentas arba Taryba gali bet kada atšaukti 9 straipsnio 2 dalyje, 10 straipsnio 5 dalyje ir 14 straipsnio 5 dalyje nurodytų įgaliojimų suteikimą. Sprendimu dėl atšaukimo nutraukiamas tame sprendime nurodytų įgaliojimų suteikimas. Sprendimas įsigalioja kitą dieną po jo paskelbimo *Europos Sąjungos oficialiajame leidinyje* arba vėlesnę jame nurodytą dieną. Jis neturi poveikio jokiam jau įsigaliojusiam deleguotajam teisės aktui.

4. Kai tik Komisija priima deleguotąjį aktą, apie tai ji tuo pačiu metu praneša Europos Parlamentui ir Tarybai.

5. Pagal 9 straipsnio 2 dalį, 10 straipsnio 5 dalį ir 14 straipsnio 5 dalį priimtas deleguotasis aktas įsigalioja tik jeigu per du mėnesius nuo pranešimo apie jį Europos Parlamentui ir Tarybai dienos nei Europos Parlamentas, nei Taryba nepareiškė prieštaravimų arba jeigu iki to laikotarpio pabaigos ir Europos Parlamentas, ir Taryba pranešė Komisijai, kad jie nepareikš prieštaravimų. Europos Parlamento arba Tarybos iniciatyva tas laikotarpis pratęsiamas dviem mėnesiams.

19 straipsnis

Komitetų procedūra

1. Komisijai padeda komitetas („Tinklų ir informacijos saugumo komitetas“). Tai komitetas, apibrėžtas Reglamente (ES) Nr. 182/2011.

2. Kai daroma nuoroda į šią dalį, taikomas Reglamento (ES) Nr. 182/2011 4 straipsnis.

3. Kai daroma nuoroda į šią dalį, taikomas Reglamento (ES) Nr. 182/2011 5 straipsnis.

20 straipsnis

Įvertinimas

Komisija periodiškai peržiūri šios direktyvos taikymą ir pranešimą apie tai pateikia Europos Parlamentui ir Tarybai. Pirmoji ataskaita pateikiama ne vėliau kaip praėjus trejiems metams po perkėlimo į nacionalinę teisę datos, nurodytos 21 straipsnyje. Tuo tikslu Komisija gali pareikalauti, kad valstybės narės nevilkindamos pateiktų informaciją.

[13] SEC(2012) 72 galutinis.

21 straipsnis

Perkėlimas į nacionalinę teisę

1. Ne vėliau kaip [vieneri su puse metų nuo priėmimo dienos] valstybės narės priima ir paskelbia įstatymus ir kitus teisės aktus, būtinus siekiant laikytis šios direktyvos. Jos nedelsdamos pateikia Komisijai tų nuostatų tekstus.

   Jos pradeda tas priemones taikyti nuo [vieneri su puse metų nuo priėmimo dienos].

   Valstybės narės, tvirtindamos tas priemones, daro jose nuorodą į šią direktyvą arba tokia nuoroda daroma jas oficialiai skelbiant. Nuorodos darymo būdą nustato valstybės narės.

2. Valstybės narės pateikia Komisijai šios direktyvos taikymo srityje priimtų vidaus teisės aktų pagrindinių nuostatų tekstus.

22 straipsnis

Įsigaliojimas

Ši direktyva įsigalioja [dvidešimtą] dieną po jos paskelbimo *Europos Sąjungos oficialiajame leidinyje*.

23 straipsnis

Adresatai

Ši direktyva skirta valstybėms narėms.

Priimta Briuselyje

Europos Parlamento vardu	*Tarybos vardu*
Pirmininkas	*Pirmininkas*

I PRIEDAS

Kompiuterinių incidentų tyrimo tarnybai (CERT) keliami reikalavimai ir jos užduotys

CERT keliami reikalavimai ir jos užduotys yra tinkamai ir aiškiai apibrėžti ir grindžiami nacionaline politika ir (arba) taisyklėmis. Juos sudaro:

(1) CERT taikomi reikalavimai

(a) CERT užtikrina, kad jos ryšio paslaugos būtų lengvai prieinamos ir kad nesusidarytų silpnų didelės svarbos grandžių, taip pat nustato keletą būdų, kaip susisiekti su ja ir kitais. Be to, ryšio kanalai yra aiškiai apibrėžti ir gerai žinomi susijusioms šalims ir bendradarbiavimo partneriams.

(b) CERT įgyvendina ir valdo saugumo priemones, siekdama užtikrinti jos gaunamos ir tvarkomos informacijos konfidencialumą, vientisumą, prieinamumą ir autentiškumą.

(c) CERT biurai yra įkurti ir pagalbinės informacinės sistemos įrengtos saugiose vietose.

(d) Tarnybos valdymo kokybės sistema sukuriama remiantis CERT veiklos rodikliais, taip užtikrinant nuoseklų tobulinimo procesą. Ji grindžiama aiškiai apibrėžtomis matavimo priemonėmis, kurios apima oficialius paslaugų lygmenis ir pagrindinius veiklos rodiklius.

(e) Veiklos tęstinumas

- CERT aprūpinama tinkama prašymų valdymo ir nukreipimo sistema, siekiant palengvinti perdavimą,
- CERT turi pakankamai darbuotojų, kad būtų prieinama bet kuriuo metu,
- CERT remiasi infrastruktūra, kurios tęstinumas yra užtikrintas. Tuo tikslu sukuriamos CERT atsarginės sistemos ir rezervinė darbo erdvė, siekiant užtikrinti pastovią prieigą prie ryšio priemonių.

(2) CERT užduotys

(a) CERT užduotys yra bent tokios:

- stebėti incidentus nacionaliniu lygmeniu,
- teikti su rizika ir incidentais susijusius išankstinius perspėjimus, įspėjimus, skelbimus ir informaciją atitinkamoms suinteresuotosioms šalims,
- reaguoti į incidentus,
- užtikrinti dinaminę rizikos bei incidentų analizę ir informuotumą apie susiklosčiusią padėtį,
- didinti visuomenės informuotumą apie riziką, susijusią su veikla internete,
- organizuoti su TIS susijusias kampanijas;

(b) CERT užmezga bendradarbiavimo santykius su privačiuoju sektoriumi.

(c) Siekdama palengvinti bendradarbiavimą, CERT skatina priimti ir naudoti bendrus ar standartizuotus metodus tokiose srityse:

- incidentų ir rizikos valdymo procedūrų,
- incidentų, rizikos ir informacijos klasifikavimo sistemų,
- matavimo priemonių taksonomijos sistemų,

– keitimosi informacija apie riziką ir incidentus formatų ir sistemų įvardijimo susitarimų.

II PRIEDAS

Rinkos dalyvių sąrašas

Nurodyti 3 straipsnio 8 dalies a punkte

1. E. prekybos platformos

2. Interneto mokėjimo vartai

3. Socialiniai tinklai

4. Paieškos sistemos

5. Nuotolinių išteklių paslaugos

6. Taikomųjų programų parduotuvės

Nurodyti 3 straipsnio 8 dalies b punkte

1. Energetika

- Elektros ir dujų tiekėjai
- Elektros energijos ir (arba) dujų paskirstymo sistemų operatoriai ir mažmenininkai, teikiantis prekes galutiniams vartotojams
- Gamtinių dujų perdavimo sistemų operatoriai, saugyklų operatoriai ir SGD operatoriai
- Elektros energijos perdavimo sistemų operatoriai
- Naftotiekiai ir naftos saugyklos
- Elektros energijos ir dujų rinkų dalyviai
- Naftos ir gamtinių dujų gamybos, perdirbimo ir apdorojimo įrengimų įmonės

2. Transportas

- Oro vežėjai (krovinių ir keleivių vežimas oro transportu)
- Jūrų vežėjai (jūrų ir pakrančių keleivių vežimo vandens transportu bendrovės ir jūrų bei pakrančių krovinių vežimo vandens transportu bendrovės)
- Geležinkeliai (infrastruktūros valdytojai, integruotos bendrovės ir geležinkelių vežėjai)
- Oro uostai
- Uostai
- Eismo valdymo kontrolės operatoriai
- Papildomos logistinės paslaugos: a) sandėliavimo ir saugojimo, b) krovinių tvarkymo ir c) kitos transporto pagalbinės veiklos.

3. Bankininkystė – kredito įstaigos pagal Direktyvos 2006/48/EB 4 straipsnio 1 dalį.

4. Finansų rinkų infrastruktūra – vertybinių popierių biržos ir pagrindinės sutarties šalies tarpuskaitos namai.

5. Sveikatos sektorius – sveikatos priežiūros vietos (įskaitant ligonines ir privačias klinikas) ir kiti sveikatos priežiūros paslaugų teikimo subjektai.

FINANSINĖ TEISĖS AKTO PASIŪLYMO PAŽYMA

1. PASIŪLYMO (INICIATYVOS) STRUKTŪRA

1.1. Pasiūlymo (iniciatyvos) pavadinimas

1.2. Atitinkama (-os) politikos sritis (-ys) VGV / VGB sistemoje

1.3. Pasiūlymo (iniciatyvos) pobūdis

1.4. Tikslai

1.5. Pasiūlymo (iniciatyvos) pagrindas

1.6. Trukmė ir finansinis poveikis

1.7. Numatomas (-i) valdymo metodas (-ai)

2. VALDYMO PRIEMONĖS

2.1. Priežiūros ir atskaitomybės taisyklės

2.2. Valdymo ir kontrolės sistema

2.3. Sukčiavimo ir pažeidimų prevencijos priemonės

3. NUMATOMAS PASIŪLYMO (INICIATYVOS) FINANSINIS POVEIKIS

3.1. Atitinkama (-os) daugiametės finansinės programos išlaidų kategorija (-os) ir biudžeto išlaidų eilutė (-ės)

3.2. Numatomas poveikis išlaidoms

3.2.1. Numatomo poveikio išlaidoms suvestinė

3.2.2. Numatomas poveikis veiklos asignavimams

3.2.3. Numatomas poveikis administracinio pobūdžio asignavimams

3.2.4. Suderinamumas su dabartine daugiamete finansine programa

3.2.5. Trečiųjų šalių įnašai

3.3. Numatomas poveikis įplaukoms

FINANSINĖ TEISĖS AKTO PASIŪLYMO PAŽYMA

1. PASIŪLYMO (INICIATYVOS) STRUKTŪRA

1.1. Pasiūlymo (iniciatyvos) pavadinimas

Europos Parlamento ir Tarybos direktyvos dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti pasiūlymas.

1.2. Atitinkama politikos sritis VGV / VGB sistemoje[37]

- 09 – Ryšių tinklai, turinys ir technologijos

1.3. Pasiūlymo (iniciatyvos) pobūdis

☒ Pasiūlymas (iniciatyva) susijęs (-usi) su **nauja priemone**

☐ Pasiūlymas (iniciatyva) susijęs (-usi) **su nauja priemone, kuri bus priimta įgyvendinus bandomąjį projektą ir (arba) atlikus parengiamuosius veiksmus**[38]

☐ Pasiūlymas (iniciatyva) susijęs (-usi) su **esamos priemonės galiojimo pratęsimu**

☐ Pasiūlymas (iniciatyva) susijęs (-usi) su **priemone, perorientuota į naują priemonę**

1.4. Tikslai

1.4.1. Komisijos daugiametis (-čiai) strateginis (-iai) tikslas (-ai), kurio (-ių) siekiama šiuo pasiūlymu (šia iniciatyva)

Siūlomos direktyvos tikslas – užtikrinti **aukštą bendrą** tinklų ir informacijos saugumo **(TIS) lygį visoje ES.**

1.4.2. Konkretūs tikslai ir atitinkama VGV / VGB veikla

Pasiūlyme nustatytos priemonės aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti.

Konkretūs tikslai:

1. Nustatyti minimalų TIS lygmenį valstybėse narėse ir taip apskritai pagerinti bendrą parengtį ir atsakomuosius veiksmus.

2. Gerinti TIS bendradarbiavimą ES lygmeniu siekiant veiksmingai tarpvalstybiniu lygmeniu kovoti su incidentais ir grėsmėmis. Bus sukurta saugi dalijimosi informacija infrastruktūra, kuri leistų kompetentingoms institucijoms keistis slapta ir konfidencialia informacija.

3. Suformuoti rizikos valdymo kultūrą ir pagerinti privačiojo ir viešojo sektorių keitimąsi informacija.

Atitinkama VGV / VGB veikla

Direktyva taikoma tam tikrų sektorių (energetikos, transporto, kredito institucijų ir vertybinių popierių biržų, sveikatos priežiūros ir pagrindinių interneto paslaugų teikimą užtikrinančių priemonių) subjektams (bendrovėms, organizacijoms, įskaitant kai kurias MVĮ), taip pat viešojo administravimo institucijoms. Joje pristatomos sąsajos tarp teisėsaugos ir duomenų apsaugos, taip pat išorės santykių TIS aspektai.

- 09 – Ryšių tinklai, turinys ir technologijos

- 02 – Verslas

[37] VGV – veikla grindžiamas valdymas, VGB – veikla grindžiamas biudžeto sudarymas.

[38] Kaip nurodyta Finansinio reglamento 49 straipsnio 6 dalies a arba b punktuose.

- 32 – Energetika
- 06 – Judumas ir transportas
- 17– Sveikatos ir vartotojų apsauga
- 18 – Vidaus reikalai
- 19 – Išorės santykiai
- 33 – Teisingumas
- 12 – Vidaus rinka

1.4.3. Numatomas (-i) rezultatas (-ai) ir poveikis

Nurodyti poveikį, kurį pasiūlymas (iniciatyva) turėtų turėti tiksliniams gavėjams (grupėms)

Labai padidėtų ES vartotojų, verslo įmonių ir valdžios institucijų apsauga nuo TIS incidentų, grėsmių ir rizikos.

Daugiau informacijos galima rasti prie šio teisės akto pasiūlymo pridedamo Komisijos tarnybų darbinio dokumento „Poveikio vertinimas“ 8.2 skirsnyje (2 varianto „Reguliavimas“ poveikis).

1.4.4. Rezultatų ir poveikio rodikliai

Nurodyti pasiūlymo (iniciatyvos) įgyvendinimo stebėjimo rodiklius.

Stebėsenos ir vertinimo rodikliai pateikiami Poveikio vertinimo 10 skirsnyje.

1.5. Pasiūlymo (iniciatyvos) pagrindas

1.5.1. Trumpalaikiai arba ilgalaikiai poreikiai

Būtų reikalaujama, kad kiekviena valstybė narė turėtų:

- nacionalinę TIS strategiją;
- TIS bendradarbiavimo planą;
- TIS kompetentingą nacionalinę instituciją; taip pat
- Kompiuterinių incidentų tyrimo tarnybą (CERT)

ES lygmeniu būtų reikalaujama, kad valstybės narės bendradarbiautų tinkle.

Būtų reikalaujama, kad viešojo administravimo institucijos ir pagrindiniai privačiojo sektoriaus atstovai užtikrintų TIS rizikos valdymą ir praneštų kompetentingoms institucijoms apie didelį poveikį turinčius TIS incidentus.

1.5.2. Papildoma ES dalyvavimo nauda

Atsižvelgiant į tarpvalstybinį TIS pobūdį, atitinkamų teisės aktų ir politikos skirtumai yra kliūtis bendrovėms veikti daugelyje šalių ir užtikrinti visuotinę masto ekonomiją. Jei nebus veikiama ES lygmeniu, gali susidaryti padėtis, kai kiekviena valstybė narė veiktų atskirai, nepaisydama sąsajų tarp tinklų ir informacinių sistemų.

Tad nustatyti tikslai gali būti geriau pasiekti imantis ES lygmens, o ne valstybių narių lygmens veiksmų.

1.5.3. Panašios patirties išvados

Pasiūlymas grindžiamas analizės išvadomis, jog būtini reguliavimo srities įpareigojimai, kad būtų sudarytos vienodos veiklos sąlygos ir panaikintos tam tikros teisės aktų leidybos spragos. Atsižvelgiant į visiško savanoriškumo principą bendradarbiavimas šioje srityje vyksta tik tarp mažumos didelius pajėgumus turinčių valstybių narių.

1.5.4. Suderinamumas ir galima sąveika su kitomis atitinkamomis priemonėmis

Pasiūlymas visiškai atitinka Europos skaitmeninę darbotvarkę, o todėl – ir strategiją „ES 2020“. Jis atitinka ES elektroninių ryšių reguliavimo sistemą, ES direktyvą dėl ypatingos svarbos Europos infrastruktūros objektų ir ES duomenų apsaugos direktyvą ir juo šie teisės aktai papildomi.

Šis pasiūlymas teikiamas kartu su bendru Komisijos ir Sąjungos vyriausiosios įgaliotinės užsienio reikalams ir saugumo politikai komunikatu dėl Europos kibernetinio saugumo strategijos ir yra jos svarbi dalis.

1.6. Trukmė ir finansinis poveikis

– ☐ Pasiūlymo (iniciatyvos) trukmė ribota

– ☐ Pasiūlymo (iniciatyvos) trukmė – MMMM [mm dd] – MMMM [mm dd].

– ☐ Finansinis poveikis nuo MMMM iki MMMM.

– ☒ Pasiūlymo (iniciatyvos) trukmė neribota

– Perkėlimo į nacionalinę teisę laikotarpis pradedamas skaičiuoti po priėmimo (numatoma 2015 m.) ir trunka 18 mėnesių. Tačiau direktyvos įgyvendinimas prasidės nuo priėmimo; ją įgyvendinant bus sukurta saugi infrastruktūra, kuri padės paremti valstybių narių bendradarbiavimą.

– vėliau – visavertis taikymas.

1.7. Numatyti valdymo būdai[39]

– ☒ Komisijos vykdomas tiesioginis centralizuotas valdymas

– ☒ Netiesioginis centralizuotas valdymas, vykdymo užduotis perduodant:

– ☐vykdomosioms įstaigoms

– ☒ Bendrijų įsteigtoms įstaigoms[40]

– ☐ nacionalinėms viešojo sektoriaus arba viešąsias paslaugas teikiančioms įstaigoms

– ☐ asmenims, atsakingiems už konkrečių veiksmų vykdymą pagal Europos Sąjungos sutarties V antraštinę dalį ir nurodytiems atitinkamame pagrindiniame teisės akte, apibrėžtame Finansinio reglamento 49 straipsnyje

– ☐ Pasidalijamasis valdymas kartu su valstybėmis narėmis

– ☐ Decentralizuotas valdymas kartu su trečiosiomis šalimis

– ☐ Bendras valdymas su tarptautinėmis organizacijomis, įskaitant Europos kosmoso agentūrą

Jei nurodomas daugiau kaip vienas valdymo būdas, papildomą išsamią informaciją pateikti šio punkto pastabų skiltyje.

Pastabos
Decentralizuota Bendrijų įkurta agentūra ENISA gali padėti valstybėms narėms ir Komisijai įgyvendinti direktyvą pagal jos įgaliojimus, perskirsčius šiai agentūra pagal 2014–2020 m. daugiametę finansinę programą numatytus išteklius.

[39] Informacija apie valdymo būdus ir nuorodos į Finansinį reglamentą pateikiamos svetainėje „BudgWeb“ http://www.cc.cec/budg/man/budgmanag/budgmanag_en.htmlhttp://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

[40] Kaip nurodyta Finansinio reglamento 185 straipsnyje.

2. VALDYMO PRIEMONĖS

2.1. Priežiūros ir atskaitomybės nuostatos

Nurodyti dažnumą ir sąlygas.

Komisija periodiškai peržiūrės direktyvos taikymą ir pateiks apie tai pranešimą Europos Parlamentui ir Tarybai.

Be to, Komisija įvertins, ar direktyva į nacionalinę teisę teisingai perkelta visose valstybėse narėse.

EITP pasiūlyme taip pat numatyta galimybė vertinti projektų įgyvendinimo metodus ir jų įgyvendinimo poveikį siekiant įvertinti, ar yra pasiekti tikslai, įskaitant su aplinkos apsauga susijusius tikslus.

2.2. Valdymo ir kontrolės sistema

2.2.1. Nustatyta rizika

- vėlavimas įgyvendinant projektą kurti saugią infrastruktūrą

2.2.2. Numatomi kontrolės metodai

Pagal EITP vykdomų veiksmų įgyvendinimo susitarimuose ir sprendimuose bus numatyta Komisijos arba bet kokio Komisijos įgalioto atstovo vykdoma priežiūra ir finansinė kontrolė, taip pat Audito Rūmų auditas ir Europos kovos su sukčiavimu tarnybos (OLAF) vykdomi patikrinimai vietoje.

2.2.3. Kontrolės priemonių taikymo išlaidos ir nauda ir galimas nesilaikymo lygis

Rizika grindžiamos *ex ante* ir *ex post* kontrolės priemonės ir audito vietoje galimybė leis užtikrinti, kad kontrolės priemonių taikymo Išlaidos būtų pagrįstos.

2.3. Sukčiavimo ir pažeidimų prevencijos priemonės

Nurodyti dabartines arba numatytas prevencijos ir apsaugos priemones.

Komisija tinkamomis priemonėmis užtikrina, kad, vykdant pagal šią direktyvą finansuojamą veiksmą, finansiniai Sąjungos interesai būtų ginami taikant prevencines kovos su sukčiavimu, korupcija ir kitokia neteisėta veika priemones, atliekant veiksmingas patikras ir, jei nustatoma pažeidimų, susigrąžinant nepagrįstai sumokėtas sumas ir prireikus skiriant veiksmingas, proporcingas ir atgrasomąsias sankcijas.

Komisijai arba jos atstovams ir Audito Rūmams suteikiami įgaliojimai atlikti visų dotacijų gavėjų, rangovų ir subrangovų, gavusių Sąjungos lėšų pagal programą, dokumentų auditą ir auditą vietoje.

Europos kovos su sukčiavimu tarnyba (OLAF) gali, laikydamasi Reglamente (Euratomas, EB) Nr. 2185/96 nustatytų procedūrų, atlikti ūkinės veiklos vykdytojų, tiesiogiai arba netiesiogiai susijusių su tokiu finansavimu, patikrinimus ir patikras vietoje, siekdama nustatyti, ar vykdant dotacijos susitarimą, dotacijos sprendimą ar sutartį dėl Sąjungos lėšų skyrimo nebūta Sąjungos finansiniams interesams kenkiančių sukčiavimo, korupcijos ar kitos neteisėtos veikos atvejų.

Nepažeidžiant ankstesnių pastraipų nuostatų, bendradarbiavimo susitarimuose su trečiosiomis šalimis bei tarptautinėmis organizacijomis ir dotacijų susitarimuose, dotacijų sprendimuose ir sutartyse, sudaromose įgyvendinant šį reglamentą,

Komisijai, Audito Rūmams ir OLAF aiškiai suteikiami įgaliojimai atlikti tokį auditą, patikrinimus ir patikras vietoje.

EITP numatytos subsidijų ir viešojo pirkimo sutartys, kurios bus pagrįstos standartiniais modeliais, kuriuose bus nustatytos bendrai taikytinos kovos su sukčiavimu priemonės.

3. NUMATOMAS PASIŪLYMO (INICIATYVOS) FINANSINIS POVEIKIS

3.1. Atitinkama (-os) daugiametės finansinės programos išlaidų kategorija (-os) ir biudžeto išlaidų eilutė (-ės)

- Dabartinės biudžeto eilutės

Daugiametės finansinės programos išlaidų kategorijas ir biudžeto eilutes nurodyti eilės tvarka.

Daugiametės finansinės programos išlaidų kategorija	Biudžeto eilutė	Išlaidų rūšis	Įnašas			
	Rezultatų [Aprašymas….....]	DA / NDA (41)	ELPA šalių[42]	šalių kandidačių [43]	trečiųjų šalių	pagal Finansinio reglamento 18 straipsnio 1 dalies aa punktą
	09 03 02 skatinti nacionalinių internetu teikiamų viešųjų paslaugų sujungimą bei sąveiką ir prieigą prie tokių tinklų	DIF	NE	NE	NE	NE

- Prašomos sukurti naujos biudžeto eilutės (netaikoma)

Daugiametės finansinės programos kategorijos ir biudžeto eilutės nurodytos eilės tvarka.

Daugiametės finansinės programos išlaidų kategorija	Biudžeto eilutė	Išlaidų rūšis	Įnašas			
	Rezultatų [Išlaidų kategorija…]	DA / NDA	ELPA šalių	šalių kandidačių	trečiųjų šalių	pagal Finansinio reglamento 18 straipsnio 1 dalies aa punktą
	[XX.YY.YY.YY]		TAIP / NE	TAIP / NE	TAIP / NE	TAIP / NE

41 DA – diferencijuotieji asignavimai / NDA – nediferencijuotieji asignavimai.

42 ELPA: Europos laisvosios prekybos asociacija.

43 Šalių kandidačių ir, kai taikoma, Vakarų Balkanų potencialių šalių kandidačių.

3.2. Numatomas poveikis išlaidoms

3.2.1. Numatomo poveikio išlaidoms suvestinė

mln. EUR (tūkstantųjų tikslumu)

Daugiametės finansinės programos išlaidų kategorija	1	Tvarus ir integracinis augimas

DG: <…….>			2015 m.*[44]	**2016** metai	**2017** metai	**2018** metai	Vėlesni metai (2019-2021) ir vėliau			**IŠ VISO**
• Veiklos asignavimai										
09 03 02	Įsipareigojimai	(1)	1,250**	0,000						**1,250**
	Mokėjimai	(2)	0,750	0,250	0,250					**1,250**
Administracinio pobūdžio asignavimai, finansuojami konkrečių programų rinkinio[45] lėšomis			**0,000**							**0,000**
Biudžeto eilutės numeris		(3)	**0,000**							**0,000**
IŠ VISO asignavimų <….> GD	Įsipareigojimai	=1+1a +3	1,250	0,000						**1,250**
	Mokėjimai	=2+2a +3	0,750	0,250	0,250					**1,250**

• IŠ VISO veiklos asignavimų	Įsipareigojimai	(4)	1,250	0,000						**1,250**
	Mokėjimai	(5)	0,750	0,250	0,250					**1,250**

[44] Metai N yra metai, kuriais prasideda pasiūlymo ar iniciatyvos įgyvendinimas.

[45] Techninė ir (arba) administracinė pagalba ir išlaidos ES programų ir (arba) priemonių įgyvendinimui (buvusios BA eilutės), netiesioginiams moksliniams tyrimams, tiesioginiams moksliniams tyrimams remti.

• IŠ VISO administracinio pobūdžio asignavimų, finansuojamų konkrečių programų rinkinio lėšomis		(6)	**0,000**							
IŠ VISO asignavimų pagal daugiametės finansinės programos 1 IŠLAIDŲ KATEGORIJĄ	Įsipareigojimai	=4+ 6	1,250	0,000						**1,250**
	Mokėjimai	=5+ 6	0,750	0,250	0,250					**1,250**

* Tikslus laikas priklausys nuo datos, kai pasiūlymą priims teisės aktų leidybos institucija (t. y. jei direktyva bus patvirtinta 2014 m., esamos infrastruktūros pritaikymas prasidės 2015 m.; kitu atveju – po metų).

** Jeigu valstybės narės nusprendžia pasinaudoti esama infrastruktūra ir padengti vienkartines pritaikymo išlaidas iš ES biudžeto, kaip paaiškinta 1.4.3 ir 1.7 punktuose, apskaičiuota, kad, remiantis direktyvos III skyriumi (išankstinis perspėjimas, koordinuoti atsakomieji veiksmai ir t. t.), tinklo pritaikymo valstybių narių bendradarbiavimui paremti išlaidos būtų 1 250 000 EUR. Ši suma šiek tiek didesnė nei paminėtoji poveikio vertinime (apie 1 mln. EUR), nes ji pagrįsta tikslesniu reikiamų tokios infrastruktūros sudedamųjų dalių apskaičiavimu. Reikiamos sudedamosios dalys ir su jomis susijusios išlaidos yra pagrįstos JRC apskaičiavimu, pagrįstu sistemų kūrimo kitose srityse (tokiose kaip visuomenės sveikatos), ir būtų tokios: TIS ankstyvojo perspėjimo ir pranešimo sistema (275 000 EUR), keitimosi informacija platforma (400 000 EUR); išankstinio perspėjimo ir atsakomųjų veiksmų sistema (275 000 EUR); operatyvinio valdymo centras (300 000 EUR) – iš viso 1 250 000 EUR. Tikimasi, kad išsamesnis įgyvendinimo planas bus pateiktas būsimame galimybių tyrime pagal konkrečią sutartį SMART 2012/0010 „Europos išankstinio perspėjimo ir atsakomųjų veiksmų sistemos kovai su kibernetiniais išpuoliais ir elektroninių ryšių tinklo veiklos sutrikdymu įgyvendinimo galimybių tyrimas ir parengiamoji veikla“.

Jei pasiūlymas (iniciatyva) daro poveikį kelioms išlaidų kategorijoms:

• IŠ VISO veiklos asignavimų	Įsipareigojimai	(4)	0,000	0,000						
	Mokėjimai	(5)	0,000	0,000						
• IŠ VISO administracinio pobūdžio asignavimų, finansuojamų konkrečių programų rinkinio lėšomis		(6)	**0,000**	**0,000**						
IŠ VISO asignavimų pagal daugiametės finansinės programos 1–4 IŠLAIDŲ KATEGORIJAS (Orientacinė suma)	Įsipareigojimai	=4+ 6	1,250	0,000						1.250
	Mokėjimai	=5+ 6	0,750	0,250	0,250					1.250

Daugiametės finansinės programos išlaidų kategorija	**5**	Administracinės išlaidos

mln. EUR (tūkstantųjų tikslumu)

		2015 metai	**2016** metai	**2017** metai	**2018** metai	Vėlesni metai (2019-2021) ir vėliau			**IŠ VISO**
GD: CNECT									
• Žmogiškieji ištekliai		0,572	0,572	0,572	0,572	0,572	0,572	**0,572**	**4,004**
• Kitos administracinės išlaidos		0,318	0,118	0,318	0,118	0,318	0,118	**0,118**	**1,426**
IŠ VISO CNECT generalinio direktorato	Asignavimai	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**

IŠ VISO asignavimų Daugiametės finansinės programos **5 IŠLAIDŲ KATEGORIJA**	(Iš viso įsipareigojimų = Iš viso mokėjimų)	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**

mln. EUR (tūkstantųjų tikslumu)

		2015 metai[46]	**2016** metai	**2017** metai	**2018** metai	Vėlesni metai (2019-2021) ir vėliau			**IŠ VISO**
IŠ VISO asignavimų pagal daugiametės finansinės programos **1–5 IŠLAIDŲ KATEGORIJOS**	Įsipareigojimai	2,140	0,690	0,890	0,690	0,890	0,690	0,690	**6,680**
	Mokėjimai	1,640	0,940	1,140	0,690	0,890	0,690	0,690	**6,680**

[46] N metai yra pasiūlymo (iniciatyvos) įgyvendinimo pradžios metai.

3.2.2. Numatomas poveikis veiklos asignavimams

– ☐ Pasiūlymui (iniciatyvai) įgyvendinti veiklos asignavimai nenaudojami

– ☑ Pasiūlymui (iniciatyvai) įgyvendinti veiklos asignavimai naudojami taip:

– Įsipareigojimų asignavimai mln. EUR (tūkstantųjų tikslumu)

Nurodyti tikslus ir rezultatus ⇩			**2015*** metai		**2016** metai		**2017** metai		**2018** metai		Vėlesni metai (2019-2021) ir vėliau						**IŠ VISO**	
	REZULTATAI																	
	Tipas[47]	Vidutinės išlaidos	Skaičius	Išlaidos	Skaičius	Išlaidos	Skaičius	Išlaidos	Skaičius	Išlaidos	Skaičius	Išlaidos	Skaičius	Išlaidos	Skaičius	Išlaidos	Visas skaičius	Iš viso sąnaudų
2 KONKRETUS TIKSLAS[48] Saugi dalijimosi informacija infrastruktūra																		
- Rezultatas	Pritaikyta infrastruktūra																	
Iš viso 2 konkretaus tikslo			1	1,250**													1	1,250
VISOS IŠLAIDOS				1,250														1,250

[47] Rezultatai yra numatomi tiekti produktai ir paslaugos(pvz., finansuotų studentų mainų skaičius, km nutiestų kelių ir kt.)

[48] Kaip apibūdinta 1.4.2 dalyje. „Konkretus (ūs) tikslas (-ai)...“

* Tikslus laikas priklausys nuo datos, kai pasiūlymą priims teisės aktų leidybos institucija (t. y. jei direktyva bus patvirtinta 2014 m., esamos infrastruktūros pritaikymas prasidės 2015 m.; kitu atveju – po metų).

** Žr. 3.2.1 punktą.

3.2.3. Numatomas poveikis administracinio pobūdžio asignavimams

3.2.3.1. Santrauka

– ☐ Pasiūlymui (iniciatyvai) įgyvendinti administraciniai asignavimai nenaudojami

– ☑ Pasiūlymui (iniciatyvai) įgyvendinti administraciniai asignavimai naudojami taip:

mln. EUR (tūkstantųjų tikslumu)

	2015 metai[49]	**2016** metai	**2017** metai	**2018** metai	Vėlesni metai (2019-2021) ir vėliau			**IŠ VISO**
Daugiametės finansinės programos 5 IŠLAIDŲ KATEGORIJA								
Žmogiškieji ištekliai	0,572	0,572	0,572	0,572	0,572	0,572	0,572	**4,004**
Kitos administracinės išlaidos	0,318	0,118	0,318	0,118	0,318	0,118	0,118	**1,426**
Tarpinė suma pagal daugiametės finansinės programos 5 IŠLAIDŲ KATEGORIJĄ	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**
Neįtraukta į daugiametės finansinės programos 5 IŠLAIDŲ KATEGORIJĄ[50]								
Žmogiškieji ištekliai	0,000	0,000						**0,000**
Kitos administracinio pobūdžio išlaidos								
Tarpinė suma, neįtraukta pagal daugiametės finansinės perspektyvos 5 IŠLAIDŲ KATEGORIJĄ	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**
IŠ VISO	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**

[49] N metai yra pasiūlymo (iniciatyvos) įgyvendinimo pradžios metai.

[50] Techninė ir (arba) administracinė pagalba ir išlaidos ES programų ir (arba) priemonių įgyvendinimui (buvusios BA eilutės), netiesioginiams moksliniams tyrimams, tiesioginiams moksliniams tyrimams remti.

Administracinių CNECT generalinio direktorato asignavimų poreikiai bus tenkinami panaudojant asignavimus, kurie jau paskirti priemonei valdyti ir (arba) kurie buvo perskirstyti generaliniame direktorate, ir prireikus finansuojami iš papildomų lėšų, kurios atsakingam generaliniam direktoratui gali būti skiriamos valdančiajam generaliniam direktoratui pagal metinę asignavimų skyrimo procedūrą ir atsižvelgiant į biudžeto apribojimus.

Europos tinklų ir informacijos apsaugos agentūra (ENISA) gali padėti valstybėms narėms ir Komisijai įgyvendinti direktyvą remdamasi savo įgaliojimais, perskirsčius šiai agentūrai pagal 2014–2020 m. daugiametę finansinę programą skirtus išteklius, t. y. be jokių papildomų biudžeto ar žmogiškųjų išteklių asignavimų.

3.2.3.2. Numatomi žmogiškųjų išteklių poreikiai

– ☐ Pasiūlymui (iniciatyvai) įgyvendinti žmogiškieji ištekliai nenaudojami

– ☑ Pasiūlymui (iniciatyvai) įgyvendinti žmogiškieji ištekliai naudojami taip:

Iš esmės papildomų darbuotojų neprireiks. Žmogiškųjų išteklių reikės labai mažai, jų poreikiai bus patenkinti pasitelkiant generalinio direktorato darbuotojus, kurie jau paskirti vykdyti veiksmo valdymo užduotį.

Sąmatą nurodyti sveikaisiais skaičiais (arba ne smulkiau nei dešimtųjų tikslumu)

		2015 metai	**2016** metai	**2017** metai	**2018** metai	Vėlesni metai (2019-2021) ir vėliau		
• Etatų plano pareigybės (pareigūnai ir laikinieji darbuotojai)								
09 01 01 01 (Komisijos būstinė ir atstovybės)		4	4	4	4	4	4	4
XX 01 01 02 (Delegacijos)								
XX 01 05 01 (Netiesioginiai moksliniai tyrimai)								
10 01 05 01 (Tiesioginiai moksliniai tyrimai)								
• Išorės personalas (visos darbo dienos ekvivalentas: FTE)[51]								
09 01 02 01 (CA, INT, SNE finansuojami iš bendrojo biudžeto)		1	1	1	1	1	1	1
XX 01 02 02 (CA, INT, JED, LA ir SNE delegacijose)								
XX 01 04 yy[52]	būstinėje[53]							
	delegacijose							
XX 01 05 02 (CA, INT, SNE – netiesioginiai moksliniai tyrimai)								
10 01 05 02 (CA, INT, SNE – tiesioginiai moksliniai tyrimai)								
Kitos biudžeto eilutės (nurodyti)								
IŠ VISO		**5**	**5**	**5**	**5**	**5**	**5**	**5**

XX yra atitinkama politikos sritis arba biudžeto antraštinė dalis.

Žmogiškųjų išteklių poreikiai bus tenkinami panaudojant CNECT GD darbuotojus, jau paskirtus priemonei valdyti ir (arba) perskirstytus generaliniame direktorate, ir prireikus finansuojami iš papildomų lėšų, kurios atsakingam GD gali būti skiriamos pagal metinę asignavimų skyrimo procedūrą ir atsižvelgiant į biudžeto apribojimus.

51 CA – sutartininkas („Contract Agent“); INT – per agentūrą įdarbintas darbuotojas („Intérimaire“); JED – „Jeune Expert en Délégation“ (jaunesnysis ekspertas delegacijoje); LA – vietinis darbuotojas; SNE – deleguotasis nacionalinis ekspertas („Seconded National Expert“).

52 Neviršijant viršutinės ribos, nustatytos išorės personalui, finansuojamam iš veiklos asignavimų (buvusių BA eilučių).

53 Būtina struktūriniams fondams, Europos žemės ūkio fondui kaimo plėtrai (EŽŪFKP) ir Europos žuvininkystės fondui (EŽF).

Europos tinklų ir informacijos apsaugos agentūra (ENISA) gali padėti valstybėms narėms ir Komisijai įgyvendinti direktyvą remdamasi savo dabartiniais įgaliojimais, perskirsčius šiai agentūrai skirtus išteklius pagal 2014–2020 m. daugiametę finansinę programą, t. y. be jokių papildomų biudžeto ar žmogiškųjų išteklių asignavimų.

Vykdytinų užduočių aprašas:

Pareigūnai ir laikinieji darbuotojai	- Deleguotųjų aktų parengimas pagal 14 straipsnio 3 dalį - Įgyvendinimo aktų parengimas pagal 8 straipsnį, 9 straipsnio 2 dalį, 12 straipsnį, 14 straipsnio 5 dalį ir 16 straipsnį - Indėlis į bendradarbiavimą per tinklą politikos ir veiklos lygmenimis. - Dalyvavimas tarptautinėse derybose ir galimas tarptautinių susitarimų sudarymas.
Išorės personalas	Prireikus parama įgyvendinant visas pirmiau minėta užduotis.

3.2.4. Suderinamumas su dabartine daugiamete finansine programa

– ☑ Pasiūlymas (iniciatyva) atitinka dabartinę daugiametę finansinę programą

– ☐ Atsižvelgiant į pasiūlymą (iniciatyvą), reikės pakeisti daugiametės finansinės programos atitinkamos išlaidų kategorijos programavimą

Numatytas finansinis poveikis pasiūlymo veiklos išlaidoms bus, jei valstybės narės nuspręs pritaikyti esamą infrastruktūrą ir paves Komisijai pritaikymus įgyvendinti pagal 2014–2020 m. daugiametę finansinę programą. Susijusios vienkartinės Išlaidos pagal EITP bus padengtos su sąlyga, kad bus pakankamai lėšų. Priešingu atveju valstybės narės gali pasidalyti infrastruktūros pritaikymo sąnaudas arba naujos infrastruktūros kūrimo sąnaudas.

– ☐ Įgyvendinant pasiūlymą (iniciatyvą) būtina taikyti lankstumo priemonę arba patikslinti daugiametę finansinę programą[54]

Netaikoma.

3.2.5. Trečiųjų šalių įnašai

– Pasiūlyme (iniciatyvoje) nenumatyta bendro su trečiosiomis šalimis finansavimo.

3.3. Numatomas poveikis įplaukoms

– ☑ Pasiūlymas (iniciatyva) neturi finansinio poveikio įplaukoms

[54] Žr. Tarpinstitucinio susitarimo 19 ir 24 punktus.